SECURITY SERVICES

Consulting, Managed Services, Education

October 2023

Blue River Experts

Member of the **Art of Innovation** Network

Table of Contents

1 Executive Summary

Blue River Experts is managed by veterans in the industry with more than 30 years of experience in nearly all areas of information technology. Our consulting system engineers have vast experience regarding real life design, deployment, and troubleshooting of all sorts of customer installations.

We consider ourselves trusted advisors in the realm of Cyber Security and our role extends beyond traditional consulting; it encompasses a commitment of understanding and navigating the complex landscape of digital threats and solutions. We offer strategic advice and tailored solutions, enabling businesses to make informed decisions to safeguard their digital assets. Our focus lies in delivering proactive, forward-thinking strategies that foster a secure environment, ensuring resilience in the face of evolving cyber threats.

Our services include a variety of Cyber Security areas and tasks including:

- Risk Management & Risk Assessment
- Network & Infrastructure Security
- Security Operations
- Incident Handling, Incident Response, Threat Intelligence
- Security (PEN) Testing
- Securing Critical Infrastructure
- Application Security
- Cloud Security
- Data Protection, Data Security & Data Loss Prevention
- Endpoint Protection
- Identity & Access Management
- Security Awareness & Education

Many of our services are also available as Managed Security Services, providing 24x7x365 availability of highly skilled and experienced experts allowing you to completely outsource various complex Cyber Security tasks including:

- SOC as a Service (SaaS)
- Managed Detection and Response (MDR)
- CISO as a Service
- Security Testing as a Service
- Bug Bounty as a Service
- Application Security as a Service
- Data Loss Prevention as a Service

This document gives a comprehensive overview of all our security services. If you need information about just one service, we also have short brochures covering every individual service.

2 Risk Management & Risk Assessment

Everything related to Cyber Security starts with Risk Assessment and Risk Management. You can't implement Cyber Security strategies if you don't know what to protect.

Cyber-attacks are typically not spontaneous events. With proper knowledge, signs of a planned attack against an organization can often be detected. Indicators of an imminent attack include references to the organization on the dark web, registration of similar domain names for phishing attacks, and confidential information, such as user account credentials, being offered for sale.

After conducting an initial Cyber Security Risk Assessment, many organizations fail to maintain an ongoing review process of their Cyber Security risk. This creates a false sense of security due to the initial assessment and any security measures taken. However, the threat landscape and attack surface are constantly evolving, necessitating continuous Cyber Security Risk Management to maintain protection.

In addition to changing threat landscapes, other factors also impact existing Cyber Security risk planning. Regulations are often modified or introduced, and the associated risks must be analyzed. Cyber Security policies and procedures must be updated to ensure compliance with new regulations.

2.1 Risk Assessment

The objective is to gain a comprehensive understanding of potential threats and vulnerabilities that constitute a risk specific to your organization's operations, assets, and industry.

Risk Assessment allows you to achieve the following:

Identify and prioritize risks based on their likelihood and potential impact. This helps you focus your attention and allocate resources to address the most critical risks.

Provide valuable insights that enable informed decision-making. It allows you to consider risks and potential consequences when setting objectives, making strategic decisions, and allocating resources.

With a clear understanding of risks, you can allocate resources more effectively. This ensures that resources are directed to areas where they are most needed to implement controls and mitigation measures.

Identify vulnerabilities and areas of weakness within your organization. By addressing these vulnerabilities, you enhance your resilience and ability to withstand and recover from adverse events.

Ensure that you comply with relevant regulations and industry standards. It helps you identify any compliance gaps and guides you in implementing controls to meet regulatory requirements.

However, as mentioned above, conducting a Risk Assessment should be just the starting point of continuous Cyber Security Risk Management.

2.2 Risk Management Process

The risk management process involves several steps, including:

Risk Identification. To effectively manage and secure your assets, it's crucial to have a comprehensive understanding of what you have and how it's being used. Simply creating an inventory of your assets is not enough; you need to dig deeper. This involves understanding the business processes, data flow, system usage, and the importance of each asset to the organization. Categorizing assets based on criticality and other factors is also important. Without proper categorization, it's difficult to prioritize and allocate resources effectively. For example, simply creating an inventory of assets without defining their function, purpose, and criticality is insufficient. Categorizing assets will help ensure that your limited resources, including time, people, and money, are focused on the highest priority assets.

Risk Assessment. Once you have categorized your assets, the next crucial step is to assess the risk associated with each asset. This includes identifying the potential vulnerabilities and threats to each asset. Afterward, you need to evaluate the likelihood of the identified threats exploiting these vulnerabilities.

This analysis will enable you to determine the areas with the highest likelihood and potential impact if a threat were to materialize. By focusing your resources and remediation efforts on the most critical areas, you can respond more effectively and mitigate the risks that pose the highest impact and criticality to your organization.

Risk Mitigation. Once risks are assessed, the next step is to respond to each risk and bring them down to an acceptable level. Organizations have four potential responses to a risk: accept, transfer, mitigate, or avoid. The response chosen will depend on the organization's overall risk appetite. It is important to focus on the risks that pose the highest threat and allocate resources to implement controls that will reduce the risk to an acceptable level.

Acceptance means not fixing the risk. This is appropriate in cases where the risk is clearly low and the time and effort it takes to fix the risk costs more than the costs that would be incurred if the risk were to be realized. Transfer means transferring the risk to another entity so your organization can recover from incurred costs of the risk being realized. Mitigation means lessening the likelihood and/or impact of the risk, but not fixing it entirely and avoidance means removing all exposure to an identified risk.

Risk Monitoring. Risk management is an ongoing process, and risks should be regularly monitored and evaluated to ensure that the risk management plan remains effective. Risk monitoring involves several sub-tasks like risk tracking, risk measurement, risk reporting, and risk communication.

Related tasks are:

- Risk Identification
- Risk Analysis and Evaluation
- Risk Treatment and Mitigation
- Risk Monitoring and Review
- Risk Reporting and Communication
- Compliance and Regulatory Alignment

2.3 Vendor / Third Party Risk Management

Third-party risks are simply the risks that arise from doing business with a supplier. Some examples include additional risk related to exposure of your data if you have a supplier who is handling, processing, or storing your data. Another risk scenario could be an outage risk – if you are hosting your infrastructure at a third-party data center, you would certainly want to validate whether they have the appropriate physical and environmental security controls in place. This protects your infrastructure in the event of a disaster.

As part of your overall risk assessment policy and process, vendor risks should be noted within the overall risk register, which is a list of all your organization’s risks with outlined details on when and how they are being addressed. A vendor/third-party risk management process is one that would guide and allow an organization to conduct appropriate due diligence during the vendor selection process while also ensuring the selected and current vendors are then monitored on an ongoing basis.

Please note that compliance with certain standards and regulations – in particular regulations covering critical infrastructure - includes proper vendor / third party risk management.

2.4 Risk Management Best Practices

No matter what framework or methodology you choose to adopt for your company, there are some steps and considerations that are constant across all environments. In general, risk management starts with gathering and analyzing information about your business, your company, your assets, your IT environment, your users, etc. From there you can identify potential threats and establish appropriate responses.

Best practices include:

- Integrate Risk Management into your Business Culture
- Risk Assessment and Analysis
- Security Policies and Procedures
- Secure Configuration and Hardening
- Access Management
- Security Awareness and Training
- Incident Response Planning
- Data Backup and Recovery
- Vendor and Third-Party Risk Management
- Continuous Monitoring and Auditing
- Regular Updates and Patch Management
- Encryption and Data Protection

2.5 Risk Management Services

We offer a comprehensive set of services around Risk Assessment, Risk Management, and Compliance including:

- Risk Assessment, Risk Identification
- Risk Management Strategy
- Risk Management Process
- Compliance Assessment & Advisory
- Vendor / Third-Party Risk Management
- Security Architecture Review
- Security Program Review
- M&A Security Services

In addition, we have special programs for important European compliance frameworks:

- DORA Services
- NIS2 Services

3 Network & Infrastructure Security

Network Security is a subset of Cyber Security, which specifically focuses on securing the network infrastructure and its components, such as routers, switches, firewalls, and other network devices.

Legacy networks were traditionally designed from the outside in, with a focus on classifying users as either "trusted" or "untrusted". The network design process began at the outer edge, where the carrier handed off the network circuit to the data center. The necessary routers were then identified and connected to multiple types of networks. The infrastructure was then built and once the network was in place, users were free to connect wherever they wished.

Therefore, perimeter-based security is based on the concept of a trusted perimeter around the network. The model assumes that all devices and users within the network are trusted, and that the perimeter can be secured using Firewalls, Intrusion Detection and Prevention Systems, and other security controls.

Micro-Segmentation introduces an advanced network security model that offers greater control and protection by logically dividing network resources into distinct security segments, even down to individual workloads. Unlike traditional network segmentation, which focuses on creating sub-networks within the overall network, Micro-Segmentation provides granular security at the level of Virtual Machines (VMs) and individual hosts.

By leveraging network virtualization technology, Micro-Segmentation enables the creation of secure zones within data centers and cloud deployments. This approach isolates each workload and applies specific security controls tailored to its needs. The use of fine-grained security policies tied to individual workloads helps prevent attacks and limits an attacker's ability to move laterally within the data center, even if they breach perimeter defenses.

The Zero Trust model flips the traditional network design approach by starting from the inside out instead of the outside in. This means that instead of classifying users as "trusted" and "untrusted," the focus is on protecting the data or assets that require safeguarding, and the network is built around them. By eliminating the trust model from the network, Zero Trust provides sophisticated and detailed protection against data breaches and other network threats.

In a Zero Trust Architecture, every user, device, and application are assumed to be untrusted, and access is granted on a need-to-know basis, based on continuous authentication and authorization.

Our services include:

- Network (IT) Security Policy
- Network Security Assessment
- Network Security Design & Implementation
- Platform Specific Services (services related to products and vendors)
- Next-Generation Firewalls
- Zero Trust Architecture Consulting
- Zero Trust Deployment Support

3.1 Network (IT) Security Policy

An IT Security Policy defines the rules and requirements for ensuring the confidentiality, integrity, and availability your organization's IT assets, and provide a framework for implementing and enforcing security controls. Such a policy typically includes:

- Access Control
- Authentication and Authorization
- Data Protection
- Incident Response
- Network Security
- Physical Security
- Third-Party Access

It also includes another important component being “Enforcement”. Once your organization has established multiple layers of protection, including firewalls, intrusion detection/prevention systems, access controls, and other security technologies, enforcement mechanisms are necessary to ensure that these security measures are being applied correctly and are effective.

Enforcement involves establishing policies, procedures, and guidelines that dictate how network security technologies and controls should be configured, monitored, and managed. It also involves assigning responsibilities to specific individuals or teams for maintaining the security of the network and enforcing compliance with security policies and procedures. This can include the regular testing of security systems, analyzing security logs for potential threats, and promptly addressing any security incidents or violations.

3.2 Network Security Assessment

To establish a baseline, we can perform various audits to assess the status and effectiveness of your network security measures. Auditing involves the examination and evaluation of network infrastructure, systems, and applications to ensure they comply with your organization's security policies and standards. The main goal of auditing is to identify security gaps or vulnerabilities in the network and ensure that appropriate measures are taken to mitigate those risks.

There are different types of audits in network security, including network audits, system audits, application audits, and compliance audits.

Network Audits focus on examining the network architecture, infrastructure, and topology, as well as network devices such as routers, switches, and firewalls.

System Audits involve the examination of operating systems, servers, workstations, and other devices that are part of the network.

Application Audits focus on examining the security of software applications running on the network, including web applications, mobile apps, and desktop applications.

Compliance Audits are performed to ensure that the network is following regulatory and industry standards such as PCI DSS, HIPAA, and ISO 27001.

3.3 Network Security Design & Implementation

There are many important components involved in designing and implementing a network security architecture, for example:

- Various Firewall implementations
- Intrusion Detection and Prevention Systems (IDPS)
- Virtual Private Networks (VPNs)
- Network Access Control (NAC)
- Security Information and Event Management (SIEM), Encryption
- Patch Management
- Data Loss Prevention (DLP)
- Antivirus and Anti-Malware software
- Application Security
- Email Security

Designing, implementing and fine-tuning your network security architecture is not an easy task and can be overwhelming for an internal team. Hiring, educating and maintaining a full staff covering all your network security needs is time consuming and expensive.

Our team of experts can help as much or as little as you like. We can perform various design and deployment tasks, but we also can cover complete job roles as part of our “Expert on Demand” program.

3.4 Platform Specific Services

We have a large team of experts covering many different vendors, solutions and products. This means we can help you with specific products and solutions in case your internal team does not have the required expertise. This includes architectures, solutions, and products from the following vendors:

- Amazon Web Services
- Aruba
- Cisco Systems / Splunk
- Fortinet
- Google Cloud Platform
- Microsoft
- Palot Alto Networks
- VMware

Please get in touch with us and let us know your specific needs as we can’t list everything we can cover.

3.5 Next-Generation Firewalls

NGFWs offer a more comprehensive and sophisticated approach to network security by combining traditional firewall capabilities with additional features including:

- Application Awareness
- Intrusion Prevention System (IPS)
- User and Group-Based Policies
- Identity Awareness
- SSL Inspection
- Application Control and Visualization
- Advanced Threat Protection
- Quality of Service (QoS) Capabilities
- Integration with the Security Ecosystem
- Cloud and Virtualization Support
- Centralized Management and Reporting

A lot of additional features usually means additional challenges like:

- Specialized Skill and Training
- Configuration Complexity
- Policy Management
- Performance Impact
- Integration with Existing Infrastructure
- SSL/TLS Inspection
- Regulatory Compliance
- Scalability

We can help you with a comprehensive range of solutions for implementing, optimizing, and managing Next-Generation Firewalls (NGFWs) tailored to your organization's specific needs. Our services cover initial assessment and design to ensure an optimal NGFW architecture, considering your network's unique demands. We provide robust implementation strategies, configuring the NGFWs with advanced security features and policies while prioritizing performance. We also ensure seamless integration with your existing network infrastructure, enabling you to harness the full potential of advanced security features. In addition, our team offers ongoing support and management, including regular updates, maintenance, and fine-tuning.

We also can help you to develop the skills of your team using various education methods.

3.6 Zero Trust Architecture Consulting

Over the past few years, the networking and security landscape has experienced a significant shift where work is no longer confined to a physical location but is instead an activity that can be performed from anywhere. As a result, hybrid work has become the new norm, causing your applications and users to be scattered everywhere, which has led to a significant expansion of your attack surface. In conjunction, we also have seen a surge in the level of sophistication and frequency of cyber-attacks aimed at exploiting this expanded attack surface.

Therefore, the traditional network security model is no longer sufficient and is being replaced by a new model that assumes every user, device, and application to be untrusted, and access is granted on a need-to-know basis, based on continuous authentication and authorization – the **Zero Trust Model**.

A Zero Trust Architecture is based on the following:

- Identity-Centric Security
- Micro Segmentation
- Least Privilege Access
- Continuous Monitoring and Analytics
- Encryption and Data Protection
- Adaptive Security Controls
- Secure Access Everywhere

This results in three main areas:

- Trust and Identity
- Policy Enforcement
- Visibility and Monitoring

A typical Zero Trust Architecture might include the following components:

- Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Device Identity and Management
- Network Segmentation
- Micro-Segmentation
- Policy-Based Access Controls
- Continuous Monitoring and Analytics
- Encryption
- API Security
- Cloud Security
- Endpoint Security
- Remote Access Security
- User Behavior Analytics (UBA)
- Threat Intelligence Integration
- Automated Security Orchestration

In most cases, moving to a Zero Trust Architecture without re-architecting the entire network is not a simple thing and requires a lot of expertise and experience. We can help you to accelerate your Zero Trust adoption by identifying and reviewing your business assets, optimize and automate your policies, and designing your Zero Trust architecture.

3.7 Zero Trust Deployment Support

In addition to Zero Trust Architecture Consulting, we offer complete day 0 to day 2 Zero Trust life-cycle services. Those services follow our proven model of ideation, innovation, transformation, execution, and optimization.

3.7.1 Discovery & Assessment

This phase of our services involves a series of activities aimed at understanding your organization's current security posture, identifying existing challenges, and defining the requirements and goals for implementing a Zero Trust model. These activities include:

- Current Infrastructure Assessment
- Risk Assessment
- Identifying Assets and Data
- Mapping User and Device Access
- Policy Review
- Gap Analysis
- Stakeholder Identification and Interviews
- Compliance and Regulations Review

This phase serves as a foundational step in preparing for the implementation of a Zero Trust framework by providing a comprehensive understanding of your organization's security landscape and paving the way for a tailored Zero Trust strategy.

3.7.2 Innovation & Design

This phase involves crafting a tailored strategy for the implementation of a Zero Trust security model. This includes:

- Architecture Planning
- Segmentation Strategy
- Identity Management Design
- Access Control Policies
- Data Classification and Protection
- Security Controls Integration
- Policy and Governance Framework
- Testing and Validation Strategy

This phase focuses on shaping a comprehensive and tailored Zero Trust strategy that aligns with your organization's specific needs, infrastructure, and security requirements, ensuring a smooth transition toward a more secure and resilient security architecture.

3.7.3 Build

During this phase activities center around the actual implementation and construction of the Zero Trust security architecture. These activities include:

- Configuration and Deployment
- Identity and Access Management (IAM)
- Encryption and Data Protection
- Integration of Security Solutions
- Policy Enforcement
- Testing and Validation
- Security Awareness Training
- Continuous Monitoring and Evaluation
- Incident Response Preparation

The build phase is a critical stage where the theoretical plans formulated in the design phase are put into practice. It involves implementing the foundational elements of the Zero Trust model, configuring security measures, and establishing the infrastructure required to support the Zero Trust architecture within your organization.

3.7.4 Optimize

The optimize phase involves refining, fine-tuning, and continually improving the Zero Trust security model. Activities in this phase include:

- Performance Evaluation
- Security Monitoring and Analysis
- Threat Intelligence Integration
- Policy Review and Refinement
- User and Device Authentication Enhancement
- Incident Response Drills
- Training and Awareness
- Compliance Assurance
- Risk Assessment and Mitigation
- Documentation and Reporting

The optimize phase aims to continuously improve and adapt the Zero Trust model to meet the evolving security landscape and organizational needs. It involves iterative refinements and adjustments to ensure the Zero Trust security framework remains effective, proactive, and robust against emerging threats.

4 Security Operations

Security Operations refers to the ongoing activities and processes that organizations implement to detect, respond to, and mitigate Cyber Security threats and incidents.

4.1 Security Operations Center (SOC)

Security Operations is usually performed within a Security Operations Center (SOC) and involves various areas and tasks including:

Security Monitoring and Threat Detection. Security operations teams employ advanced technologies, such as Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), and threat intelligence platforms, to monitor your organization's networks, systems, and applications for suspicious activities or known threats. These tools generate alerts and notifications when potential threats are detected.

Incident Management and Response is another important part of SOC operations. Security operations teams are supposed to have well-defined incident response plans and procedures in place and when an incident occurs, they coordinate and execute the necessary steps to contain and mitigate the impact. This includes investigating the incident, identifying the root cause, implementing necessary remediation measures, and documenting lessons learned for future improvement.

Incident Monitoring and Reporting. SOC teams are supposed to generate reports and provide regular updates on security incidents, vulnerabilities, and threat landscape to executives and other stakeholders. These reports include information about the types of threats, your organization's response, and the effectiveness of existing security controls.

Security Tools and Technologies. SOC teams are responsible for managing and maintaining your organization's security tools and technologies. This includes implementing patches and updates, configuring the tools to align with your organization's security policies, and ensuring the tools are operating effectively to provide accurate and timely information.

Security Incident Coordination. SOC teams work closely with other internal teams, such as IT, legal, and human resources, as well as external partners, to coordinate and respond to security incidents effectively. This collaboration ensures a cohesive and unified response, minimizing disruptions and facilitating swift recovery.

Threat Intelligence and Proactive Defense. Security operations teams continuously monitor the threat landscape, gathering intelligence about emerging threats, vulnerabilities, and attack techniques. This information is used to proactively strengthen defenses, update security controls, and enhance your organization's overall security posture.

We can help you with the deployment and maintenance of your own Security Operations Center (SOC) or you may implement Security Operations by outsourcing various components and tasks.

4.2 SOC as a Service

We offer different flavors of SOC as a Service (co-managed, fully managed), and, if desired, can also include **Managed Detection & Response (MDR)** services. Our MDR services are more proactive, and threat focused than traditional MSSP services, and involve security analysts with specialized skills in threat hunting, incident response, and forensic analysis.

If you decide to implement your own SOC, we can assist you defining your SOC process, hire and educate your SOC team, and build your SOC using various sophisticated tools like:

- Security Information & Event Management (SIEM)
- Intrusion Detection and Prevention Systems (IDPS)
- Extended Endpoint Detection and Response (XDR)
- User and Entity Behavior Analytics (UEBA)
- Network Traffic Analysis (NTA)
- Network Detection and Response (NDR)

However, there are several significant benefits of a SOC as a Service setup:

Cost Savings. Setting up an in-house SOC requires a significant investment in personnel, infrastructure, and training. By outsourcing SOC operations to an expert company your organization can save costs related to staffing, training, and infrastructure.

Access to Expertise. We have highly skilled security professionals who specialize in managing and monitoring security incidents. These experts have the latest knowledge and expertise to detect and respond to security incidents quickly.

Advanced Security Technologies. We also have access to the latest security technologies and tools that are expensive for organizations to purchase and maintain. By outsourcing your SOC operations your organizations can leverage these technologies without the need for related expertise and investment.

24/7 Monitoring. Security incidents can happen anytime, day or night. We offer 24/7 monitoring, providing your organization with round-the-clock protection against threats.

Faster Incident Response. We can quickly respond to security incidents and provide remediation guidance, helping your organization minimize the impact of a breach.

Reduced Complexity. Managing a SOC in-house requires significant investment in infrastructure, staff, and tools. By outsourcing SOC services to an expert company, your organization can reduce the complexity of maintaining and managing your own SOC, freeing up resources to focus on core business activities.

Lower Cyber Risk. An expert company like us has a larger team of security experts with a wider range of expertise and experience in detecting and responding to threats. This leads to quicker threat detection and response times, which reduces the impact of a cyber-attack on your organization's operations and reputation. Additionally, we always use the latest security technologies and best practices, which helps reduce the overall cyber risk for your organization.

Scalability. As a specialized expert company, we can scale our services to meet the changing needs of our clients. This allows your organization to adjust your security services as your business grows or as new threats emerge.

Compliance. Many companies are subject to industry-specific compliance regulations. As an external provider we can help you to meet these compliance requirements by providing regular reports and audit documentation that demonstrate your adherence to these regulations.

4.3 Security Analytics

Security Analytics is an advanced service and refers to the automated analysis of collected and aggregated critical data sources for threat detection and security monitoring. It provides security operations center (SOC) teams with better visibility into the unique environments of organizations, improving threat detection, investigations, and response. As an evolution of SIEM, Security Analytics synthesizes raw data collection and makes it actionable, managing infrastructure complexity, increasing data volumes, and quickly identifying evolving threats. Security Analytics platforms converge logs from network, identity, endpoint, application, and other security-relevant sources to generate high-fidelity behavioral alerts and facilitate rapid incident analysis, investigation, and response.

While Security Analytics platforms have been around for decades, the market continues to evolve as modern security operations teams seek tool consolidation and demand more automation to drive better security outcomes. The MITRE ATT&CK framework has been widely adopted by SecOps teams, and most vendors now map their solutions to the framework for detection, investigations, and response. The ability to granularly map to ATT&CK indicates the quality of the analytics because it shows that the analytics engine can interpret the observed or collected data.

We can either help you to select and deploy the right tool(s) if you are operating your own SOC or we can include this service into our SOC as a Service engagement.

4.4 Threat Hunting

Threat Hunting is a proactive approach that involves actively searching for cyber threats that may have gone undetected by existing security measures. It's an iterative process that involves analyzing data, identifying potential indicators of compromise, and investigating them to determine if they represent actual security threats.

Threat Hunting is typically performed by a dedicated team of security analysts who use a variety of tools and techniques to identify potential threats. These tools may include network and endpoint monitoring tools, data analysis platforms, and machine learning algorithms that can help identify anomalies and potential indicators of compromise.

The goal of Threat Hunting is to identify and neutralize potential security threats before they can cause damage or disrupt business operations. This is achieved by identifying and mitigating vulnerabilities, stopping cyber-attacks before they can succeed, and responding quickly and effectively to security incidents when they do occur.

We provide Threat Hunting as part of our Managed Detection & Response (MDR) services

4.5 CISO as a Service

A Chief Information Security Officer is an essential job role when it comes to Cyber Security as he / she is responsible for defining, implementing, and maintaining your organization’s security policy and measures. A CISO is also the highest level of hierarchy in a Security Operations Center.

However, many organizations are not that large to justify hiring a full-time, experienced CISO. Therefore, we offer to perform all the responsibilities of a CISO as a service, so your organization can benefit from the expertise and experience of a seasoned CISO while not being required to hire such a person.

5 Incident Handling, Incident Response, Threat Intelligence

You may choose to handle incidents on your own as part of your Security Operations Center. In this case we can help you to build and educate your incident response team.

You may also choose to outsource some tasks or job roles to an expert company like us. We offer:

- Incident Response Planning
- Incident Response Readiness Assessment
- Incident Response Retainer
- Incident Response Investigation
- Incident Response Remediation
- Digital Forensics Services

Using our services can bring several benefits to your organization including:

- Access to Expertise
- Reduced Response Time
- Reduced Costs
- Improved Risk Management

5.1 The Incident Response Team

An incident response team is responsible for identifying, containing, eradicating, and recovering from security incidents. The primary goal of the team is to minimize the impact of the incident on the organization's operations, assets, and reputation.

The team is responsible for developing and implementing an incident response plan that outlines the processes and procedures to be followed in the event of a security incident.

There are several essential roles within an incident response team that are necessary to ensure a well-coordinated and effective response to security incidents. These roles include:

- Incident Response Manager
- Incident Responder
- Threat Intelligence Analyst
- Forensic Analyst
- Communication Specialist
- Legal Advisor
- Public Relations Specialist

5.2 The Incident Response Life Cycle

The National Institute of Standards and Technology (NIST) has developed a four-step process for incident response. These four steps are:

Preparation. Preparation is the key to effective incident response. Even the best incident response team cannot effectively address an incident without predetermined guidelines. It involves identifying assets, establishing policies and procedures, and implementing security controls that are designed to detect, prevent, and respond to incidents. Preparation includes:

- Asset Identification
- Policies and Procedures
- Security Controls
- Incident Response Plan
- Training and Awareness

Detection and Analysis. The detection and analysis step involves identifying potential incidents, analyzing the situation, and determining the scope of the incident. The primary goal of this step is to detect incidents as early as possible and determine their severity and impact. This step includes the following:

- Alert and Notification
- Initial Assessment
- Containment
- Investigation and Analysis
- Risk Assessment
- Prioritization and Escalation
- Reporting

Containment, Eradication, and Recovery. This step involves containing the incident to prevent further damage, eradicating the threat, and recovering any lost or damaged data. It may involve isolating affected systems or networks, disabling user accounts or network access, and restoring data from backups. As the name suggests, it involves:

- Containment
- Eradication
- Recovery

Post-Incident Activity. This is the final phase of the incident response process. It involves activities that occur after an incident has been successfully resolved. The main goal of this phase is to identify and implement measures that can help prevent similar incidents from occurring in the future. Activities include:

- Lessons Learned
- Post-Incident Analysis
- Follow-up Actions

5.3 Incident Response Plan

Having an incident response plan is an essential element for responding effectively to security breaches or crises. A well-defined plan empowers teams to take immediate action and minimize the damage caused. Just like emergency responders who undergo regular training and process checks to respond quickly, information security teams should follow their lead. In the event of a security incident, there is no time to waste figuring out response procedures. Having a pre-planned and rehearsed incident response plan becomes crucial.

There's a great deal of groundwork that can be done ahead of time to reduce complexity and risk during an emergency. A robust incident response plan should include the following elements:

- Roles and Responsibilities
- Preparation and Readiness
- Incident Identification and Categorization
- Incident Response Procedures
- Training and Awareness
- Testing, Updating, and Continuous Improvement

5.4 Threat Detection & Hunting

These days organizations understand the importance of safeguarding their valuable data and invest in smart technologies and people to create a defensive shield against potential attacks. However, security is an ongoing process, and there is no guarantee of foolproof protection against breaches. In this context, speed is critical in detecting and neutralizing threats. A strong security program must have the capability to identify threats quickly and efficiently, preventing attackers from accessing sensitive information. Typically, defensive programs can detect and eliminate most known threats, as they have been encountered before and can be addressed using known tactics. However, organizations must also be equipped to detect unknown threats that may arise from novel techniques or technologies employed by attackers.

Threat Detection involves the use of tools, techniques, and processes to identify potential security incidents in an organization's network or systems.

Threat Hunting is a proactive approach to identifying security threats that may have gone undetected by traditional security measures. It involves actively searching for signs of compromise within an organization's network or systems.

5.5 Threat Intelligence

Threat intelligence is the process of gathering, analyzing, and sharing information about potential or actual cyber threats, threat actors, and their tactics, techniques, and procedures (TTPs) to help organizations proactively defend against them. It involves collecting data from various sources such as open-source intelligence, social media, dark web, and other threat feeds, analyzing it to identify patterns and trends, and turning it into actionable intelligence.

The main goal of threat intelligence is to help organizations improve their security posture by identifying and mitigating potential threats before they cause harm. By leveraging threat intelligence, organizations can gain a better understanding of the threat landscape, detect new and emerging threats, and prioritize their response to potential threats.

There are two main types of threat intelligence: strategic and operational. Strategic threat intelligence focuses on high-level, long-term trends and provides organizations with a broader understanding of the overall threat landscape. Operational threat intelligence, on the other hand, focuses on the specific tactics, techniques, and procedures used by threat actors and provides organizations with more granular information about specific threats.

6 Security (PEN) Testing

Penetration (PEN) Testing is a process that utilizes a combination of manual and automated techniques to replicate a real-world attack on an organization's information security measures, whether from malicious external actors or internal employees. Conducting a series of penetration tests aids in evaluating an organization's security measures and identifying areas that require improvement. When executed and documented correctly, a penetration test can offer insight into almost all technical security vulnerabilities and furnish the necessary information and assistance to remedy or mitigate those weaknesses.

While penetration testing will identify vulnerabilities and provide valuable insights into your organization's security arrangements, it is not a simple process, nor is it a universal solution. There are several challenges your organization may face when conducting penetration tests, such as determining the extent of the test's coverage, deciding which type of penetration test to use, managing risks associated with system failure and data exposure, agreeing on the targets and frequency of tests, and if fixing the vulnerabilities found during the test will make your systems "secure" without further measures.

A penetration test is best performed by an independent and qualified expert company who also qualifies as ethical security testers. The objective of a penetration test is to exploit known vulnerabilities, as well as to utilize the tester's expertise to identify specific weaknesses that may be unknown to your organization.

We offer many different types of penetration testing, and we also can help you determining a penetration testing program suitable for your organization. And our services don't stop identifying vulnerabilities, we also will fix them and suggest measures to avoid such vulnerabilities in the future.

6.1 Penetration Testing Programs

Penetration testing is driven by several factors, including a growing need for compliance, increased concern about the impact of security breaches on similar organizations, the use of a larger number and variety of outsourced services, significant changes to business processes, and a heightened awareness of the potential for cyber-attacks.

Establishing and managing a suitable penetration testing program can be a challenging task, even for advanced organizations. Some organizations adopt an ad hoc or piecemeal approach when performing penetration tests, depending on the needs of a particular region, business unit, or the IT department. Although this approach can fulfill a specific requirement, it is unlikely to provide real assurance about the overall security condition of enterprise-wide systems.

It is advisable to adopt a more systematic, structured approach to penetration testing as part of an overall testing program, ensuring that:

- Business requirements are met
- Major system vulnerabilities are identified and addressed quickly and effectively
- Risks are kept within acceptable business parameters

Your penetration testing program should also cover key activities required to prepare for penetration testing. Any program must include an appropriate set of tests, delivered in a consistent, well-managed way and measures to ensure the tests are followed up effectively.

Also, to ensure the effectiveness of your penetration testing program, it should be integrated with an approved technical security assurance framework that is designed to safeguard your critical information and systems.

Finally, it is advisable to incorporate one or more of the most popular penetration testing standards like:

The Penetration Testing Execution Standard (PTES) which is a framework that provides guidelines and best practices for conducting penetration testing engagements. It outlines a standardized approach to ensure consistent and thorough testing of systems, applications, and networks.

Open Web Application Security Project (OWASP) which includes the OWASP Mobile Application Security Verification Standard, the OWASP Mobile Application Security Testing Guide, the OWASP Application Security Verification Standard and the OWASP Web Security Testing Guide.

NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. The National Institute of Standards and Technology (NIST) special publication 800-115 aims to offer organizations guidelines for effective planning and execution of technical information security testing and assessments, as well as analyzing findings and developing appropriate mitigation strategies. It provides practical recommendations for designing, implementing, and maintaining processes and procedures related to technical information security testing.

6.2 Penetration Testing Methods

There are different methods of PEN testing depending on your requirements. They are called black box, grey box, or white box tests.

A **black box** test is a complete assault testing where you do not provide any information about your infrastructure. You may provide no more than a URL or even just the company name. Our testers would behave like real hackers and will test IT systems, the behavior of employees (social engineering) and physical security (building security, data center security, etc.).

In contrast, in a **white box** test we will receive extensive information about the target (e.g., network maps, source codes or internal information that is available to every employee) to focus on certain areas to identify specific weak points and design protection measures.

A **grey box** test is obviously a combination of the two opposite methods. In this scenario, we will have access to partial information (e.g., user information of a conventional user) and are checking what can be done with this piece of information. For example, circumvent security measures and gain higher rights to steal valuable information.

The white box test is ideal for initial testing as it allows us to get a holistic overview of your systems and infrastructure and therefore makes sure that most if not all existing vulnerabilities will be found and can be fixed.

It is important to recognize that a PEN test is always just a snapshot in time. If a new release or just a software update goes live after our testers have left, new problems might be introduced that were not covered in the previous test. And we all know it will happen, just look at how many problems a simple operating system update introduces to your computer.

Therefore, an initial test needs to be followed by supporting measures like a comprehensive penetration testing program that may include additional services like for example a bug bounty program.

6.3 Penetration Testing Steps

6.3.1 Planning and Reconnaissance

This is the first phase of a penetration testing engagement, which involves gathering information about the target system or network to identify potential vulnerabilities and attack vectors. It is the process of actively searching for and collecting information including identifying the target's IP address range, network topology, operating systems, applications, services, and users that can be used to identify security weaknesses.

Reconnaissance can be done through various methods, such as social engineering, online searches, and network scanning.

6.3.2 Enumeration

This is the process of collecting information about a system or network, which can then be used by the attacker to exploit vulnerabilities and gain unauthorized access. In the context of penetration testing, enumeration involves actively probing the target system to identify key pieces of information, such as usernames, passwords, system architecture, network topology, running services and applications, open ports, and other system attributes.

Enumeration is typically carried out after the initial reconnaissance phase of penetration testing, where the tester collects as much information as possible about the target network and its components. The enumeration process uses a range of techniques to extract information about the system, including port scanning, banner grabbing, service and user enumeration, and network mapping.

The results of the enumeration phase are typically used to identify potential attack vectors, but the information can also be used to develop recommendations for improving the security posture of the system, such as patching known vulnerabilities, tightening access controls, and improving network segmentation.

6.3.3 Scanning

In this phase, our experts scan the target system or network for vulnerabilities. This can be done through automated tools or manual methods, such as fuzzing or vulnerability scanning.

The scanning phase usually involves port scanning which means scanning the target system for open ports and identifying the services running on those ports. Banner grabbing is the process of retrieving information about the running service, such as its version number and operating system. Service enumeration involves identifying the types of services running on the target system and their configuration, while user enumeration involves identifying the user accounts on the system and their access levels.

6.3.4 Gaining Access

Once vulnerabilities are identified, our experts will try to exploit them to gain access to the target system or network. There are several ways testers can gain access, including:

Exploiting Vulnerabilities. Testers can use automated tools or manually identify vulnerabilities in the target system or network and exploit them to gain access. This can include exploiting unpatched software or misconfigured services.

Social Engineering. Testers can use social engineering techniques to trick users into revealing their credentials or providing access to the target system or network. This can include phishing attacks, baiting, pretexting, or other techniques.

Password Cracking. Testers can use password cracking tools to attempt to gain access to the target system or network by cracking weak or easy-to-guess passwords.

Brute Force Attacks. Testers can use automated tools to attempt to guess login credentials by systematically trying different username and password combinations until a match is found.

Physical Access. In some cases, testers may be able to gain physical access to the target system or network, such as by gaining entry to a server room or by stealing a device that contains sensitive data.

6.3.5 Maintaining Access

Once a tester has gained access to a target system or network, maintaining that access is important to continue to gather information, perform further exploitation, and test the effectiveness of any implemented security controls. To maintain access, a tester can utilize various techniques such as:

Backdoors. Creating a hidden or undocumented means of accessing the target system or network, such as a hidden user account, a Trojan horse program, or a persistent command and control channel.

Rootkits. A rootkit is a type of malware that is designed to hide its presence on a system by modifying the operating system to remove all traces of the malicious software. This can allow the attacker to maintain access to the system undetected.

Persistence Mechanisms. A persistence mechanism is a technique used to ensure that an attacker's access to a system or network is maintained over time. This can include creating a service or scheduled task that automatically executes the attacker's code, or modifying the registry to ensure that the attacker's code is executed each time the system is booted.

Covert Channels. A covert channel is a method of communicating between two parties in a way that is hidden from detection. This can include using steganography to hide messages within legitimate files or data streams, or using a protocol or port that is normally unused or uncommonly used to avoid detection.

6.3.6 Analysis and Reporting

During this stage, the results of the penetration test are compiled into a comprehensive report that provides an overview of the security posture of the target system, including any vulnerabilities that were discovered, their impact, and recommendations for remediation. The analysis and reporting stage typically includes the following steps:

Vulnerability Analysis. The results of the penetration test are analyzed to identify the vulnerabilities that were discovered and their impact on the target system.

Risk Assessment. The vulnerabilities are assessed in terms of their risk to the target system, considering factors such as the likelihood of exploitation, the impact of a successful attack, and the cost of remediation.

Prioritization. The vulnerabilities are prioritized based on their level of risk, allowing your organization to focus on the most critical vulnerabilities first.

Remediation Recommendations. The report includes recommendations for remediation of the vulnerabilities, including technical details on how to fix them and any associated risks.

Reporting. The results of the analysis are documented in a comprehensive report that is provided to your organization. The report typically includes an executive summary, technical details on the vulnerabilities, and recommendations for remediation.

6.3.7 Remediation

The final phase involves addressing the vulnerabilities found during the penetration testing engagement. The remediation phase typically includes the following steps:

Planning. A plan needs to be developed to address all the identified and prioritized vulnerabilities. This plan may include implementing security patches, changing configuration settings, updating security policies, or improving security awareness training.

Execution. The plan is executed to address the vulnerabilities. This may involve deploying security updates, reconfiguring systems, or implementing new security controls.

Validation. Once the vulnerabilities have been addressed, the systems are retested to validate that the remediation efforts have been successful. This ensures that the vulnerabilities have been properly addressed and the system is no longer vulnerable to attack.

Reporting. A final report is generated that documents the vulnerabilities that were identified, the remediation efforts that were undertaken, and the validation results. This report is used to communicate the results of the testing to management and to ensure that your organization is aware of the vulnerabilities and the steps taken to address them.

6.4 Vulnerability Assessment

Vulnerability Assessment is a process of identifying, quantifying, and prioritizing vulnerabilities in an information system, network, or application. It involves the use of automated tools to scan systems for known vulnerabilities and configuration issues. The output of a vulnerability assessment is typically a report listing the identified vulnerabilities along with recommendations for remediation.

Penetration Testing, on the other hand, is an authorized simulated attack on your system, network, or application with the goal of identifying and exploiting vulnerabilities to gain access or steal sensitive data. Penetration Testing is typically conducted manually by experienced security professionals who use a combination of tools and techniques to try to circumvent security controls and gain access to systems and data. The output of a penetration test is a report detailing the vulnerabilities found and the success of attempts to exploit them.

There is a lot of similarity, however, Vulnerability Assessment is a more automated and passive approach that provides a broad overview of your security posture, while Penetration Testing is a more manual and active approach that attempts to simulate a real-world attack scenario to identify and exploit vulnerabilities.

6.5 Types of Penetration Testing

6.5.1 Network Penetration Testing

As the name implies, this type of penetration testing is performed on the network infrastructure of an organization. There are two different types of tests:

6.5.1.1 External Network Penetration Testing

This type of penetration testing is performed on the external-facing network infrastructure of an organization. It involves identifying and exploiting vulnerabilities in the network that could potentially be exploited by attackers to gain unauthorized access to the network or steal sensitive information.

The external network infrastructure includes all the systems that are accessible from the internet, such as web servers, email servers, DNS servers, firewalls, routers, switches, and other network devices. The objective of external network penetration testing is to identify vulnerabilities in these systems and provide recommendations to mitigate or remediate the identified vulnerabilities.

6.5.1.2 Internal Network Penetration Testing

Internal network penetration testing is performed from within the organization's network, with the aim of identifying vulnerabilities that could be exploited by insiders or external attackers who have already gained access to the network. This type of testing is usually performed by security professionals who have been granted access to the organization's internal network, and who have knowledge of the network architecture and configuration. The focus is on identifying vulnerabilities in systems that are accessible only from within the organization's network, such as internal servers, databases, and applications.

Such testing usually includes privilege escalation which means that the testing team will attempt to escalate privileges to gain access to sensitive data or systems once access to a system is obtained and lateral movement where the testing team will attempt to move laterally across the network to gain access to additional systems and sensitive data.

6.5.2 Web Application Penetration Testing

Web applications are a popular target for hackers due to their accessibility and potential for quick spread of malicious code. Vulnerabilities in web apps can arise from various issues such as incorrect coding, misconfigured web servers, application design flaws, and failure to validate forms. These vulnerabilities can provide easy access for attackers to valuable databases containing financial or personal data. Additionally, cloud containers that package application software are particularly vulnerable if not properly secured, and the use of open source and APIs can further exacerbate security concerns.

One of the most important guidelines for web application security is OWASP Top 10. As a nonprofit foundation, the Open Worldwide Application Security Project (OWASP) strives to improve software security by sharing knowledge, tools, and best practices to prevent software vulnerabilities and mitigate security risks.

OWASP Top 10 outlines the most critical security risks to web applications and promotes a broad consensus about these risks. Companies are encouraged to adopt this document and take steps to minimize these risks in their web applications. Consequently, our web application testing includes a comprehensive check for all vulnerabilities described in OWASP Top 10 and our report will detail recommendations to mitigate all identified vulnerabilities.

6.5.3 Wireless Security Audits

As wireless networks and smartphones have become ubiquitous, wireless networks have become a prime target for cybercriminals. While the goal of a wireless network is to provide easy access to users, it can also serve as an open door for attackers. Unfortunately, many wireless routers are rarely, if ever, updated, leaving them vulnerable to known exploits.

There are several types of attacks that are specific for wireless networks including:

Wireless Access Control Attacks. Such attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. The attacks can take place through anything from rouge access points, MAC spoofing, ad-hoc associations, promiscuous clients, etc.

Wireless Integrity Attacks. In integrity attacks, the attacker sends forged control, data, and management frames over the wireless network to misdirect the wireless devices to perform DOS attack. This can happen through a range of methods such as data frame injections, WEP injections, data replay, etc.

Wireless Confidentiality Attacks. Confidentiality attacks attempts to intercept confidential information sent over the wireless associations, whether sent in clear text or encrypted by Wi-Fi protocols. This can be caused through eavesdropping, session hijacking, honey-pot access points, masquerading, evil twin access points, cracking WEP key or traffic analysis.

Wireless Availability Attacks. Such attacks aim to prevent legitimate users from accessing resources in a wireless network via various methods including beacon flood, authentication flood, routing attacks, etc.

Wireless Authentication Attacks. The objective of this kind of attacks is to steal the identity of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources which can happen over time through various methods including application login theft, PSK cracking, domain login cracking, VPN login cracking, etc.

To prevent such attacks from happening, wireless security audits are assessments conducted on wireless networks to identify vulnerabilities and risks to the confidentiality, integrity, and availability of wireless data and systems. The primary goal is to identify potential security threats and weaknesses in the wireless network infrastructure, access points, and wireless devices that could be exploited by attackers.

Our audit involves a comprehensive evaluation of the wireless network architecture, including wireless access points, routers, switches, and other components, to identify vulnerabilities in the configuration, deployment, and management of these devices. This also includes examining the security policies, access controls, encryption protocols, and authentication mechanisms in place to protect the wireless network.

6.5.4 IOT / ICS Penetration Testing

Embedded devices have been a part of technology for many decades, even before the term "IoT" was invented by MIT in 1999. However, the distinction between "traditional" embedded devices and the new IoT devices is the legacy of design decisions and configurations that were not intended to be connected to the public internet. This lack of foresight from manufacturers has led to the widespread exploitation of IoT devices, resulting in some of the largest Distributed Denial of Service (DDoS) attacks in the world.

In recent years, IoT devices have received significant attention due to their widespread deployment, convenience, ease of use, and potential security risks. With the increasing popularity of IoT devices, concerns regarding safety, privacy, and security have also risen. The proliferation of these devices across various industry verticals, including consumer, entertainment, commercial, medical, industrial, energy, and manufacturing, has made it evident that both consumers and technology operators/owners are unable to adequately ensure the security of these devices. Additionally, relying on device manufacturers to provide security-by-design assurance is heavily reliant on the industry for which the device was intended.

As a result, it's important to perform security testing on these devices to identify potential vulnerabilities and prevent them from being exploited by attackers. IoT penetration testing involves testing the security of IoT devices and networks, including the protocols and applications used by these devices.

There are some very specific areas of focus during IoT penetration testing including:

Device Firmware. This obviously means the testing of firmware on IoT devices.

Network Communication. This involves the testing of the communication between IoT devices and their servers.

Cloud-Based Platforms. Many IoT devices rely on cloud-based platforms for storage and processing of data. These platforms need to be tested to ensure that they're secure and that there are no vulnerabilities that could be exploited by attackers.

Mobile Applications. Also, many IoT devices are controlled via mobile applications. These applications are as secure as any other mobile application and need to be tested according to current software testing standards.

Data Privacy. IoT devices often collect sensitive data, such as personal information and usage data. Consequently, applicable data privacy standards need to be implemented and verified.

IoT penetration testing is closely related to Cloud Penetration Testing and Mobile Application Penetration Testing. Also, please note that IoT penetration testing is an essential part of securing **Critical Infrastructure**, which is discussed in chapter 7 of this document.

6.5.5 Cloud Penetration Testing

Conventional penetration testing approaches are not designed for cloud-native environments and concentrate on procedures applicable to on-premise settings. Cloud penetration testing demands expertise that varies from standard penetration testing as it involves evaluating cloud-specific settings, passwords, applications, encryption, APIs, database, and storage access. Moreover, cloud penetration testing is influenced by the Shared Responsibility Model, which clarifies the responsibility for components within a cloud infrastructure, platform, or software.

During a Cloud penetration test, security controls that are the complete responsibility of the Cloud Service Provider (CSP) are typically excluded from the scope of the test. It is important to note that when it comes to cloud security, the focus is on testing the security **within** the cloud, rather than the security **of the** cloud itself. In an Infrastructure as a Service (IaaS) environment, security testing covers the User Access/Identity, Data, Application, and Operating System layers, while other components are managed and controlled by the Cloud Service Provider (CSP) and are considered out of scope. The scope of the penetration test is determined by the service model, and the extent and coverage of the testing will vary based on the services offered by the CSP.

6.5.5.1 Scope

The application of test cases and the scope of testing vary depending on the service model. SaaS applications have a relatively small scope, focusing on data and user access/identity controls. PaaS has a larger scope that includes the application layer and some platform configuration, with all lower layers excluded. IaaS has an even broader scope, including client responsibility and potential security testing. However, certain aspects such as virtualization, hardware, and sometimes the operating system are still under the control of the CSP. Moving workloads to the cloud changes the scope of potential security testing and introduces additional areas of testing, such as the cloud management plane. If authorized by the CSP, you can expand the scope of the cloud penetration testing service to include components under the control and management of the CSP, which introduces additional complexity to the scoping process.

Depending on the service model, client-side application testing is in scope when conducting Cloud penetration testing. Please refer to Web Application Penetration Testing and Mobile Application Penetration Testing for details. In addition, the following domains are relevant:

- Account Security as it relates to User Identity and Access
- Cloud Service Security as it relates to Data Structures and Cloud Infrastructure that can be configured by the Cloud Customer
- Application / Business Logic that is under the control of the End User

It is important to consider all three domains when scoping a penetration test, even if any of them are excluded from the test's scope, as they can significantly impact each other. For instance, a misconfigured user account can increase the severity and probability of an application breach. An application that is poorly designed, implemented, or configured with elevated cloud privileges can result in a complete compromise if breached. Neglecting service use at the account level, billing thresholds, and controls can leave the application highly vulnerable to denial-of-service attacks, resource starvation, or billing abuse.

6.5.5.2 Objectives

The widely known STRIDE model can be used to look at Cloud specific testing objectives. The STRIDE model is a threat modeling framework used in software development and information security to identify and categorize potential threats to a system. The STRIDE model consists of six threat categories that represent different types of attacks that can be launched against a system:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

When applied to Cloud penetration testing, the STRIDE model helps identify potential security weaknesses and vulnerabilities including virtual machines, containers, and cloud infrastructure.

Keep in mind that the cloud is a versatile platform with a multitude of potential deployments and applications, such as workloads, storage, and containers. As a result, vulnerabilities and security weaknesses can vary depending on what is being hosted and how it is implemented. Therefore, it is important to have specific testing guidelines for each of these components.

To conclude, please note that performing penetration testing involving Cloud deployments no matter the service model is considerably different than penetration testing of legacy systems. All stages of penetration testing – preparation, threat modelling, reconnaissance and research, testing, and reporting – involve many additional items to be considered when dealing with Cloud deployments.

We have the knowledge and expertise required in such an environment. This can't be said about all companies offering such services.

6.5.6 Mobile Application Penetration Testing

This type of penetration testing is very similar to security testing during initial software development or during a software development life cycle. You can also find a lot of details in chapter 8 of this document.

As mentioned above, mobile app security testing can be viewed in two contexts. The first is the traditional security test conducted towards the end of the development cycle. In this scenario, we will evaluate a nearly finished or production-ready version of the app, detect security vulnerabilities, and produce a comprehensive report. The second context involves the implementation of security requirements and automated testing from the beginning of the software development life cycle. Although the same fundamental requirements and test cases apply to both contexts, the testing methodology and level of client involvement differ.

Whenever performing such a test, we strongly advise that we have access to source code so that testing time can be used as efficiently as possible. Code access obviously doesn't simulate an external attack, but it simplifies the identification of vulnerabilities by allowing us to verify every identified anomaly or suspicious behavior at the code level. A white-box test is the way to go if the app hasn't been tested before.

There are two primary methods for analyzing mobile apps for security vulnerabilities: static analysis and dynamic analysis. As described above, **Static Application Security Testing (SAST)** involves reviewing the source code of the app to identify potential security issues related to the implementation of security controls. Typically, a combination of automated and manual testing is used to maximize coverage. Automated scans are useful for identifying common vulnerabilities, while our expert testers can use specific usage scenarios to explore the code base more deeply.

Dynamic Application Security Testing (DAST) aims to test and evaluate mobile apps in real-time during their execution. The main goal is to identify security vulnerabilities or weaknesses in a program while it's running. This method of testing is performed on both the mobile platform layer and the backend services and APIs. By analyzing the mobile app's request and response patterns, security weaknesses can be identified and remediated.

DAST is commonly used to verify if security mechanisms are providing adequate protection against the most common types of attacks, such as data disclosure during transit, authentication and authorization issues, and server configuration errors.

By applying best practices, we follow the traditional method which entails comprehensive security testing of the mobile app's final or almost final build, such as the build that is accessible at the end of the development phase. Our testing process also employs the **OWASP MASVS (Mobile Application Security Verification Standard)** being the industry standard for mobile app security.

6.6 Social Engineering Audits

Social Engineering refers to manipulating or deceiving individuals or groups of people into divulging confidential information or performing actions that may compromise the security of an organization's information systems or physical security. It is a form of psychological manipulation that exploits human trust, gullibility, and natural curiosity.

Social Engineering attacks can take various forms and may involve the use of electronic communication channels, such as email, instant messaging, or social media platforms, as well as in-person interaction, such as impersonation, pretexting, or tailgating. The goal of Social Engineering is to obtain unauthorized access to sensitive data, such as login credentials, financial information, or personal data, or to gain physical access to restricted areas or resources.

The purpose of performing Social Engineering Audits is to identify vulnerabilities in your organization's human element. The goal is to assess the effectiveness of your organization's security controls, policies, and procedures regarding Social Engineering attacks. Social Engineering audits help your organization identify weaknesses in your security measures and provide insights into the effectiveness of your security awareness training programs. The audit results can be used to implement improvements in employee education and awareness training programs, and to enhance the overall security posture of your organization.

The first steps are always working with your organization to understand the scope of the audit and the types of Social Engineering attacks that will be simulated and gather information about your organization, your employees, and your security policies and procedures.

Next, our auditors will simulate social engineering attacks such as:

Phishing. Using emails, websites, or other electronic communication methods to trick users into disclosing confidential information, such as login credentials, credit card numbers, or social security numbers.

Pretexting. Creating a false pretext or scenario to persuade an individual to disclose sensitive information or perform an action that may compromise security.

Baiting. Using enticing offers or promises to lure individuals into disclosing sensitive information or downloading malware-infected files.

Tailgating. Following authorized personnel into restricted areas without proper authorization or credentials.

Impersonation. Posing as someone else to gain access to sensitive information or resources.

Finally, our auditors will analyze the results of the Social Engineering attack and identify areas where your organization's security policies and procedures should be improved. All our findings will be summarized in a report which also includes recommendations for improving your policies and / or employee training programs.

6.7 Active Directory Security Audits

Active Directory (AD) is a Microsoft technology used for managing computers and other resources on a network. It is a centralized authentication and authorization service that enables users to log in to multiple computers and applications using a single set of credentials. Therefore, Active Directory deployments are a main target for cyber criminals as whoever gains control of your AD (and that's easier than most people think) gains full control over your environment.

Why is getting control over your AD not that hard? Because deployment, migration, configuration, or operation of MS Active Directory is not that simple due to the many configuration options and its complexity. And this very often leads to misconfigurations that are causing vulnerabilities. Examples for AD security issues include:

Weak Passwords. Weak passwords are one of the most common vulnerabilities in AD security. Attackers can use tools to crack passwords, or they can simply guess them if they are easy to guess.

Privilege Escalation. Once an attacker gains access to a system, they can use various methods to escalate their privileges to gain greater access to systems and data.

Lack of Monitoring. AD security can be compromised if there is no monitoring in place to detect unauthorized access or suspicious activity.

Misconfigured Settings. Misconfigured AD settings can leave systems open to attack. For example, if user permissions are not properly configured, attackers may be able to gain unauthorized access.

Poorly Designed Group Policy Objects (GPOs). GPOs are used to enforce policies across an organization. Poorly designed GPOs can leave systems open to attack, as they may not provide adequate security.

Insider Threats. Insider threats can pose a significant risk to AD security, as employees with access to sensitive data may be tempted to abuse their access for personal gain.

Unpatched Systems. Unpatched systems can leave AD vulnerable to known exploits. Attackers can use these vulnerabilities to gain unauthorized access to systems and data.

It's highly recommended to perform regular AD Security Audits covering the following key aspects:

Domain Controllers. They are the backbone of the Active Directory infrastructure. Hence, it is crucial to review domain controller configurations, security policies, and logs to ensure they are configured correctly and adequately protected against threats.

Group Policies. Such policies are used to enforce security settings on domain-joined machines. Our experts will review the group policy configurations to ensure that they are aligned with your organization's security policies and best practices.

User Accounts. User accounts are the primary way users access resources in the domain. Our experts will review user account configurations to ensure that they are correctly configured.

Privileged Accounts. Such accounts have access to critical systems and data and are hence highly targeted by attackers. Our experts will review privileged account configurations to ensure that they are adequately protected and monitored.

Group Memberships. Group memberships control access to resources in the domain. Our experts will review group membership configurations to ensure that only authorized users have access to resources.

Password Policies. They dictate the strength and complexity of passwords used by users in the domain. Our experts will review password policy configurations to ensure that they are aligned with your organization's security policies and best practices.

Auditing and Monitoring. These are critical components to detect and respond to security incidents. Our experts will review the auditing and monitoring configurations to ensure that they are adequately configured.

Authentication and Authorization. Our experts will review authentication and authorization mechanisms in the domain to ensure that they are adequately protected.

A common approach is to collect all necessary information in cooperation with your team and agree a course of action. Then, our experts either may deploy several analysis tools within your infrastructure or may provide you with such analysis tools that need to be executed by your team. In both cases, the tools will generate data that will be analyzed by our experts and then you will receive comprehensive documentation of the results and recommendations for eliminating identified vulnerabilities.

Next, either your team or our experts will use the results of the first audit to harden your system. Once this has been done, another test will be performed including a corresponding analysis and evaluation. Using the results of the second test we will perform a final review where the results of the second tests will be discussed and compared with the results of the first test. If necessary, we will provide additional recommendations regarding further measures to harden the Active Directory.

6.8 Bug Bounty Programs

Traditional testing methods like the penetration testing described above are only testing your systems and environment selectively at a certain point in time. But in today's rapidly changing environment this is no longer appropriate. Also, vulnerabilities are discovered daily, so a one-time penetration test is already obsolete when you are reading the results.

Also, the result of a penetration test is often a long list of problems because such tests focus on all aspects including theoretical threats that currently are no problem but could become problems in the future. In practice this means that only some of the findings are easily actionable. A white box test is ideal for initial testing as it allows testers to get a holistic overview of your systems and infrastructure and therefore makes sure that most if not all existing vulnerabilities will be found and can be fixed.

But this is just a snapshot in time. If a new release or just a software update goes live after the test has been performed, new problems might be introduced that were not covered in the previous test. And we all know it will happen, just look at how many problems a simple operating system update introduces to your computer.

Adding a bug bounty program to them mix, your systems are tested continuously and therefore there is a very high probability that all vulnerabilities and threats are being identified.

6.8.1 What is a bug bounty program?

When hearing the term "bounty hunter" people usually think of the wild west where gunfighters received a bounty for hunting down "wanted" persons. A bug bounty program is similar but in the virtual world and instead of "wanted" persons bounty hunters are hunting bugs (errors, malfunctions). Here, hackers are receiving a bounty for identifying a software error as in reality all security issues are either software misconfigurations or software errors. And the more severe the error, the more generous the bounty.

Already many years ago Internet pioneers like Netscape (the de-facto web browser standard at the time) launched internal bug bounty programs inviting their employees to report any bug they could find and receive a reward for doing so. It took a while until such programs gained momentum but today many companies consider bug bounty programs as an effective addition to their security measures. The crowd intelligence of registered ethical (friendly) hackers is constantly attacking your systems abiding pre-defined rules and hackers will be rewarded with a bounty (payment) for identifying verified security issues.

In contrast to penetration testing, such a program is an **outside-in, black box approach**. Testers (hackers) don't have access to source information or other company resources. They approach your systems the way criminals would do.

Therefore, the ongoing result of a bug bounty program is a much shorter list of vulnerabilities compared to a white-box penetration test, but this is a list of actual issues that could be used right now by criminals. As the list only contains actual issues it allows you to take immediate action.

Another key difference of bug bounty programs is that there is continuous checking of your systems and applications, so updates and new releases are included in the process. Organizations are sometimes hesitant to allow hackers to attack their applications but let's be realistic – this happens in an uncontrolled way all the time so better get it done in a controlled way and discover issues before they can be exploited.

6.8.2 Advantages of Bug Bounty programs

They solve the "snapshot in time" issue of traditional penetration tests. With a bug bounty program, security tests take place on an ongoing basis and therefore provide continuous information about the security situation of systems and infrastructure. Therefore, you will gain uninterrupted insight into any security issues and can immediately take action to solve the problem(s).

The above usually also means faster response. A bug bounty service can provide faster and more efficient identification and resolution of security vulnerabilities since the researchers are incentivized to find and report any issues as quickly as possible.

Another advantage is the usage of collective knowledge. Bug bounty services provide you with the swarm intelligence of a large community of trusted friendly hackers. And this combined expertise will always be superior to the expertise of one or a few penetration testers. With such a service, you will be served by a community of hundreds of security researchers worldwide and gain access to a much broader range of expertise, knowledge, and backgrounds. This ensures that the risk of a cyberattack is minimized and your own experts and developers will learn from our ongoing reports and thus automatically expand their cyber security knowledge.

A bug bounty program is often more cost-effective than traditional security testing methods since it provides a way to pay for results instead of paying for time spent testing. We offer such programs to all company sizes, and they pay only for the identification of verified vulnerabilities and impactful flaws. Furthermore, we can also run such a program on a pre-defined budget and can trigger an alarm once the payment for verified vulnerabilities has reached a pre-defined threshold.

Also, running a bug bounty program can be seen as a sign of a proactive and responsible approach to security, which can be a valuable marketing and public relations tool.

Another interesting side effect is that bug bounty programs increase the internal awareness of cyber security. Neither software developers nor vendors want to be confronted with ongoing issues caused by either of them.

7 Securing Critical Infrastructure

Critical infrastructure refers to the collection of assets, systems, and networks that are vital for the proper functioning of a society. It encompasses both physical and virtual components and is essential for various aspects of a nation, including its economy, national security, public health, and safety. Examples of critical infrastructure include sectors such as food and agriculture, transportation systems, water supply, internet and mobile networks, public health services, energy utilities, financial services, telecommunications, and defense. The specific infrastructure considered critical can vary depending on a nation's unique needs, available resources, and level of development. Safeguarding critical infrastructure is crucial to ensure the stability and resilience of essential services and the overall well-being of a society.

Industrial control systems (ICS) are a key component of critical infrastructure, particularly in sectors such as transportation, oil and gas, electricity, and water management. These systems, including supervisory control and data acquisition (SCADA) systems, play a vital role in automating and controlling industrial processes. However, the increasing threat of attacks targeting SCADA and other ICS poses significant risks.

This infrastructure is hugely different from common IT structures that are normally found in companies. On the one hand, older protocols and systems can be found quite often due to the complexity of updating hard- and software. On the other hand, this is the area where we are facing some of the newest technologies collectively referred to as the Internet of Things (IOT). A very different world of new protocols and an enormous amount of data that needs to be collected, analyzed, and transmitted.

Operators of ICS are challenged to keep pace with the ever-evolving trend of gathering and ingesting reliable, quickly obtained data from both interior and exterior sources or risk losing market share. The need for reliable and fast access to data representing what's happening in one's own system, as well as the competitive market, can make the difference between record profit margins or bankruptcy. Now that these serial networks have been modified to operate in IP networks using commercial off-the-shelf (COTS) products, most of which do not provide any additional security, these once serial, air gapped systems face the same advanced persistent threats, malware, and insider threats as their enterprise counterparts' systems. These day-to-day threats are of concern to the enterprise IT, but even more so to the operational technology systems, because unlike enterprise systems, OT systems cannot be easily updated and retooled to address the constantly changing threat landscape.

Designed to control physical processes with as close to 100 percent uptime as possible, these systems are difficult and costly to take offline due to the impact they could have on production and surrounding environments. Due to the functional requirements placed upon these systems, the equipment refresh cycle is greatly extended. It is not uncommon to find one that has been operating for close to 25 years on the original hardware and operating system.

Security experts with a computer science background are confronted with a very different world with a high attack potential and of course an enormous value for attackers as messing around with such systems has devastating effects. When it comes to securing critical infrastructure, you need to employ experts with a background in IT and OT technologies and ideally experience in one or more verticals like manufacturing, transportation, oil and gas, etc.

We can help with the following:

- ICS Risk Management
- ICS Risk Assessment
- ICS Security Program Development and Deployment
- ICS Security Architecture
- ICS Security Testing
- Cyber Security Platform Selection

7.1 ICS Risk Management

An ICS risk management process is considerably different, for example safety is a paramount concern for ICS operators and significantly influences the engineering and operational decisions made. When establishing a risk management process for an ICS organization, it is essential to consider how safety requirements interact with information security. In situations where safety requirements conflict with best security practices, the organization must make a clear decision on prioritization. In most cases, ICS operators would prioritize safety over security. The risk management process ensures that such assumptions are explicitly addressed, fostering agreement within the organization, and maintaining consistency throughout the process.

The availability of services is another significant concern for ICS operators. In critical infrastructure sectors like water or power systems, uninterrupted and dependable operations are vital. Therefore, ICS often have stringent requirements for availability and recovery. It is crucial to explicitly develop and state these assumptions in the risk management process. Failing to do so may lead the organization to make risk decisions that inadvertently impact the users and stakeholders who rely on the services provided by the ICS.

There are many more examples but discussing all of them would go far beyond the purpose of this document.

7.2 ICS Risk Assessment

When conducting a risk assessment for an ICS, there are unique considerations that differentiate it from a risk assessment for a traditional IT system. Due to the interaction of physical and digital aspects in an ICS, the impact of a cyber incident can extend beyond the digital realm and have physical consequences. As a result, risk assessments for ICS must consider these potential effects.

For example, assessing the potential physical impact of a cyber incident is crucial for an ICS. This involves evaluating how a disruption or compromise in the ICS could affect physical processes, equipment, infrastructure, and personnel safety.

Considerations should also be given to the potential operational consequences resulting from a cyber incident in an ICS. This includes assessing the impact on critical processes, production capabilities, delivery of services, and overall system availability. Operational disruptions can have significant financial, reputational, and safety implications.

Another important aspect are supply chain dependencies. ICS often rely on a complex network of suppliers and vendors. Assessing the risks associated with supply chain dependencies is crucial to ensure the resilience and security of the ICS. This involves evaluating the potential vulnerabilities and threats that may arise from third-party interactions and considering appropriate risk mitigation strategies.

As above, there are many more examples, but we can’t discuss all of them in this document.

7.3 ICS Security Program Development and Deployment

Effectively integrating security into an ICS requires defining and executing a comprehensive program that addresses all aspects of security, ranging from identifying objectives to day-to-day operation and ongoing auditing for compliance and improvement. This involves many aspects like:

- developing a business case for security
- establishing governance structures and defining roles and responsibilities
- conducting a comprehensive risk assessment
- developing and documenting security policies, procedures, and guidelines
- implementing security awareness and training programs
- defining and deploying appropriate security controls
- establishing an incident response plan
- implementing monitoring systems and security technologies to detect and respond to potential threats
- ensuring compliance with relevant industry-specific regulations, standards, and frameworks
- developing procedures for assessing the security posture of third-party vendors and contractors who have access to your systems

7.4 ICS Security Architecture

Designing and implementing a security architecture for critical infrastructure and industrial control systems involves a solid understanding of the corresponding industry vertical. Besides, various technical elements like the following need to be considered:

- Segmentation and Zoning
- Boundary Protection and Firewalls
- Logically separated Control Network
- Defense-In-Depth
- Access Controls
- Secure Remote Access
- Event Logging and Monitoring
- Man-In-The-Middle Attacks
- Incident Detection, Response, and System Recovery

If you are interested in more details, you may want to get hold of NIST special publication 800-82 which includes a lot of details on executing the Risk Management Framework tasks for Industrial Control Systems and gives in-depth guidance on the application of Security Controls to ICS.

7.5 ICS Security Testing

Due to the heightened sensitivity of many ICS environments, special care must be taken when conducting technical security tests. The type and nature of these tests need to be carefully considered, and analysts need to employ a diverse range of methods and alternative approaches as part of their testing methodology.

Unlike traditional IT environments, ICS environments prioritize "availability" over "integrity" or "confidentiality." This fundamental difference requires a distinct approach to technical security testing. Invasive tests or tests that strain the network can potentially lead to disruptive service outages and should be avoided in these environments.

Performing security tests in ICS environments requires analysts to have a deep understanding of the unique technologies and processes involved, as well as the most effective testing approaches. This places a greater emphasis on the skills, knowledge, and situational awareness of analysts, requiring specialized individuals supported by a robust methodology.

Also, when conducting testing in ICS environments, it is crucial to consider the various stakeholders involved and their different perspectives, motivations, and expectations regarding risk assessment. ICS environment owners, process engineers, safety specialists, and security practitioners may have distinct viewpoints on the risks associated with an ICS environment and the specific types of tests and assurances they require.

The actual engagement is like other established approaches; however, we pay special attention to demystifying technical security testing and facilitate effective communication throughout the engagement.

While the process is generic in nature, it includes activities tailored to address the unique characteristics of ICS environments. This involves adapting the testing approach to align with the sensitivity of business functions and processes specific to the ICS environment. Factors such as potential adverse consequences and the incident response capability are considered. Additionally, the process incorporates up-to-date threat intelligence and employs a well-balanced combination of offline and online tests that prioritize safety and process awareness, using methods like the check-test-check approach.

There are six characteristics that differentiate this approach from conventional security testing:

Business Process Sensitivity ensuring a clear understanding of the connection between ICS-related risks and the achievement of business goals

Focused Threat Intelligence leveraging relevant threat intelligence, tailored to the target company and industry sector

Integrated Risk Assessment incorporating the risk perspectives of various stakeholders, including process engineers, safety specialists, and IT and Cyber Security professionals

Proven Tools and Methods as special caution should be exercised when conducting online technical security testing in ICS environments

Highly Qualified Technical Security Testers with in-depth knowledge of ICS technologies and their integration with critical business processes

Combined Testing Teams ensuring domain knowledge, process expertise, and a deep understanding of the ICS environment

7.6 Cyber Security Platform Selection

Your organization can no longer rely on disjointed and ineffective legacy point solutions to defend critical infrastructure. You need a modern Cyber Security platform with a complete, tightly integrated set of capabilities to prevent threats while reducing the burden on your organization in deploying and maintaining security. Here are some of the areas to consider:

- Network and Endpoint Security
- Traffic Classification
- Network Segmentation
- Detection and Elimination
- Shared Threat Intelligence
- Zero -Day Attacks
- Centralized Management & Reporting
- Mobility & Virtualization Technologies
- APIs and Industry-Standard Management Interfaces
- Alignment with Industry Standards

8 Application Security

Security breaches affecting applications are among the most common types of security incidents. There are numerous statistics highlighting the importance of application security as a critical component of a comprehensive Cyber Security strategy.

Application Security refers to the process of identifying, fixing, and preventing security vulnerabilities in software applications. It involves incorporating security measures into the design, development, deployment, and maintenance of software applications to protect them from potential security threats and attacks. The goal of application security is to ensure that the application functions properly and securely, and that sensitive information is protected from unauthorized access, modification, or disclosure.

There are many security concerns related to application development including:

- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Insecure Configuration Management
- Insecure Third-Party Components

Based on the above it is critical to include Security into the **Software Development Life Cycle (SDLC)** by following these steps:

Design for Security. During the design phase, the development team should consider how to incorporate security into the design of the application. This includes selecting secure architecture patterns, secure coding practices, and security controls.

Implement Secure Coding Practices. Secure coding practices are a critical component of building secure applications. This involves training developers on secure coding practices, using secure coding guidelines, and conducting code reviews to identify and fix security vulnerabilities.

Perform Security Testing. Security testing should be performed throughout the SDLC to ensure that security requirements are met. There are various security testing techniques that can be used during the SDLC, including:

Static Application Security Testing (SAST). This involves analyzing the application's source code or binary code for security vulnerabilities. It is typically performed during the early stages of development.

Dynamic Application Security Testing (DAST). This involves testing the application's security by simulating attacks against a running instance of the application. It is typically performed during the later stages of development, when the application is closer to being deployed.

Interactive Application Security Testing (IAST). This involves combining the techniques of SAST and DAST to test the application's security in real-time. It provides a more comprehensive view of the application's security posture and is typically performed during the later stages of development.

Penetration Testing. This involves simulating an attack against the application to identify vulnerabilities that could be exploited by attackers. It is typically performed during the later stages of development or after the application has been deployed.

Threat Modeling. This involves identifying potential threats to the application and analyzing the potential impact of those threats. It is typically performed during the early stages of development and can help inform the development of security controls.

Implement Security Controls. Security controls should be implemented throughout the application to help mitigate security risks. This includes access controls, authentication and authorization, encryption, monitoring, and logging.

Maintain Security. Security is an ongoing process that requires maintenance and updates over time. This includes patching vulnerabilities, monitoring for security incidents, and conducting regular security assessments.

We offer many application security services like:

Assessing your current Application Security measures and coverage.

Designing and implementing a proper Software Development Life Cycle including all relevant aspects like designing for security, implementing secure coding practices, performing various security tests, and more.

Conducting ongoing security assessments and audits to ensure that configurations are secure and remain secure over time.

Designing and implementing appropriate user authentication methods and defining and establishing proper role-based access policies.

Defining and implementing appropriate data protection policies, procedures and mechanisms.

Performing data protection audits to ensure that you are following applicable laws and regulations.

Performing comprehensive code reviews.

Designing and delivering a comprehensive secure coding education program covering languages like C, C++, Java, and Python. Topics include:

- Web Application Security
- Desktop Application Security
- Cloud Application Security for Azure
- Cloud Application Security for AWS
- Machine Learning Security
- Security Testing

9 Cloud Security

9.1 Cloud Security

Cloud Security refers to the overarching discipline involving the practices, technologies, policies, and controls aimed at protecting cloud-based assets, data, and infrastructure from various threats, vulnerabilities, and risks. It encompasses a broad range of strategies and measures designed to ensure confidentiality, integrity, and availability of data and services hosted in the cloud.

Technologies for Cloud Security include:

- Cloud Access Security Broker (CASB)
- Cloud Security Posture Management (CSPM)
- Container Security
- Continuous Integration and Continuous Delivery/Deployment (CI/CD)
- Encryption
- Data Loss Prevention (DLP)
- (Virtual) Firewalls
- Identity and Access Management
- Security Information and Event Management (SIEM)
- Secure Web Gateways

The most important architectures related to Cloud Security are:

- Zero Trust Architecture (ZTA)

  As described in detail earlier in this document, Zero Trust is a security model that assumes that all networks, devices, and users are untrusted by default, and verifies and grants access based on specific parameters and conditions. In the context of Cloud Security, Zero Trust is important because traditional security models that rely on perimeter-based defenses are no longer sufficient to protect against modern cyber threats. With cloud environments, the perimeter is constantly shifting and expanding, making it difficult to monitor and secure all points of entry. Additionally, users and devices are increasingly mobile and remote, making it difficult to identify and authenticate legitimate access.

- Secure Access Service Edge (SASE)

  SASE combines various networking and security capabilities into a single platform to provide secure access to applications and data, regardless of the location of the user or application. The primary goal of SASE is to simplify the management and delivery of network and security services while providing a more comprehensive and flexible approach to security. SASE brings together key capabilities such as WAN (Wide Area Network), SD-WAN (Software Defined WAN), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS) into a single integrated platform.

9.2 Cloud Security Architecture

Cloud Security Architecture is a specific aspect within the realm of Cloud Security. It pertains to the structured design and implementation of security controls, frameworks, and strategies within a cloud environment. It focuses on creating a robust, well-architected framework that incorporates security measures at various layers of the cloud infrastructure, including network, data, applications, and access management. Cloud Security Architecture is essentially the blueprint or design framework that outlines the security measures necessary for a secure cloud environment.

A Cloud Security Architecture depends a lot on the choice of Cloud Service Provider as every CSP like AWS, Google Cloud, Microsoft Azure, etc. has their own security model and architecture. It also depends on the choice of cloud service model - Infrastructure as a Service, Platform as a Service, Software as a Service - as this has an impact on the distribution of responsibilities between the CSP and your organization.

It is advisable that a Cloud Security Architecture should be designed to align with industry best practices, standards, and regulations, such as the Cloud Security Alliance (CSA) Cloud Controls Matrix, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the General Data Protection Regulation (GDPR).

9.3 The Shared Responsibility Model

One of the key challenges in securing cloud resources is the concept of shared responsibility. In a cloud environment, the responsibility for security is shared between the cloud service provider and the customer. The cloud service provider is responsible for the security of the cloud infrastructure, while the customer is responsible for securing their data, applications, and access to cloud services.

To address this challenge, a Cloud Security Architecture should include a range of security controls that are implemented by both the cloud service provider and the customer. For example, the cloud service provider may implement physical security measures to protect the cloud infrastructure, such as access controls, surveillance systems, and fire suppression systems. The customer, on the other hand, may implement access controls, data encryption, and vulnerability scanning to protect their applications and data.

9.4 Cloud Security Services

Designing and implementing Cloud Security can be a very complex and overwhelming challenge and many organizations that are more and more depending on cloud services to achieve their business goals are not equipped with the internal experts to deal with this challenge.

We have the experience and the experts to help you with many aspects and tasks like:

9.4.1 Cloud Security Strategy

Securing your organization's critical operations and data depends on robust cloud security solutions. To effectively deal with today’s threats and challenges, it's vital for your organization to adopt a holistic approach towards cloud security. A successful cloud security strategy extends beyond the adoption of the latest tools and technologies, integrating established cloud security frameworks and evolving architectures. Cloud security also needs to consider existing security measures deployed in your organization.

Your strategy also needs to emphasize strong identity and access management technology, well-defined security control configurations, data encryption practices, efficient operations management, and ongoing security and compliance monitoring.

When defining and implementing your cloud security strategy we will also help you to select, configure, and maintain the various security measures and solutions offered by cloud service providers, for example Amazon Web Services, Google Cloud Platform, or Microsoft Azure, etc. or even a combination of different providers.

9.4.2 Cloud Security Policies and Standards

This involves identifying the unique security requirements for your cloud environment and creating a set of rules, guidelines, and practices to safeguard cloud-based resources, data, and services. These policies typically outline authorized access controls, encryption standards, data protection measures, identity management protocols, and compliance requirements. They also cover incident response procedures, risk management strategies, and guidelines for securing various components within the cloud infrastructure.

9.4.3 Compliance Monitoring

What's the point of defining policies and standards if they are not being followed? The only way to ensure compliance is ongoing monitoring involving regular security assessments and audits that also lead to an ongoing improvement of your policies.

Compliance monitoring also means verifying compliance with applicable regulatory requirements and industry standards. You need to ensure that the chosen cloud service provider adheres to relevant compliance frameworks depending on the nature of your organization's data. This includes understanding the responsibilities of both the cloud provider and your organization in meeting compliance requirements.

9.4.4 Identity and Access Management

IAM provides you with tools used for controlling user access to systems, applications, and data. However, IAM in a cloud environment presents several challenges due to the dynamic and distributed nature of cloud systems. For example, managing identities, permissions, and access rights across diverse cloud services, multiple users, and various applications becomes increasingly complex.

One of the key challenges is managing the large number of users, groups, and access policies that need to be created and maintained. This can be a complex and time-consuming process, especially in a large environment. Therefore, user provisioning and de-provisioning needs to be automated to ensure timely access for new users and revoke access for departing employees promptly.

Additionally, IAM systems must be designed to be highly available and scalable, as they often need to handle millions of user requests per day.

Ensuring centralized control over distributed resources can be challenging. This is amplified when multiple cloud services or hybrid cloud environments are used, as different platforms often have varying IAM protocols.

Meeting regulatory standards and compliance requirements is very important, however, different regions have specific laws governing data protection and privacy, making it challenging to align IAM practices with these regulations.

Integrating IAM systems across multiple cloud providers and on-premises infrastructure while maintaining identity federation and single sign-on (SSO) capabilities can be very complex.

We can help you addressing these challenges by implementing robust IAM strategies tailored to your specific cloud environment, adopting automation for user provisioning, enforcing strong authentication measures, regularly auditing access controls, and stay updated on regulatory compliance standards.

9.4.5 Data Security & Integrity

Data Security and Integrity refers to measures put in place to ensure that data is kept safe from unauthorized access, modification, destruction, or other forms of interference. This includes protecting data from cyber-attacks, system malfunctions, and other threats. Data security and integrity also include measures to ensure the accuracy, completeness, and consistency of data.

In contrast to Data Protection, Data Security and Integrity focuses on the technical measures put in place to protect data, while Data Protection focuses on the policies and procedures in place to ensure that data is handled in accordance with legal and regulatory requirements.

We can help your organization to take several measures including:

- Encryption
- Access Controls
- Data Backups
- Data Classification
- Data Loss Prevention (DLP)
- Integrity Controls
- Vulnerability Management

9.4.6 Designing and Deploying a Zero Trust Architecture

We discussed Zero Trust at various places in this document and as outlined in chapter 3 we offer comprehensive Zero Trust life-cycle services. Those services are also applicable for a cloud environment and can help you to assess, design, build, and optimize your Zero Trust strategy and architecture.

Depending on your overall strategy this also includes integrating your Zero Trust strategy into your SASE framework (please see below).

9.4.7 Designing and Deploying a SASE Architecture

SASE (Secure Access Service Edge) is a cloud-based security framework that combines various networking and security capabilities into a single platform to provide secure access to applications and data, regardless of the location of the user or application. The primary goal of SASE is to simplify the management and delivery of network and security services while providing a more comprehensive and flexible approach to security.

SASE is designed to address the needs of organizations that are embracing digital transformation and are moving to cloud-based services, mobile devices, and remote workforces. SASE brings together key capabilities such as WAN (Wide Area Network), SD-WAN (Software Defined WAN), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS) into a single integrated platform.

SASE has a significant impact on traditional network and security architectures. With SASE, traditional perimeter-based security models are replaced with a model that is based on identity and context.

Challenges in implementing SASE include the complexity of integrating various networking and security capabilities into a single platform, the need to ensure compatibility with existing infrastructure, and the need to ensure compliance with regulations and standards.

9.4.8 SOC & SIEM Strategy & Operation

Cloud environments are usually more complex and dynamic than traditional on-premise environments, which makes it more difficult to monitor and detect security incidents. Consequently, your SOC team must have a deep understanding of the cloud environment they are monitoring, including the different services and configurations that are in use.

Second, in a cloud environment, security logs are dispersed across different services and regions. Your SIEM must be able to collect and aggregate logs from different sources and correlate them to provide a unified view of security incidents. This requires advanced integration capabilities between your SIEM and your cloud services.

Third, cloud environments can experience a high volume of events and logs, which can result in a high level of false positives. A SOC team must have the expertise to filter out the noise and focus on the most critical events that require action.

Finally, the SOC team must be aware of the shared responsibility model which means that the cloud service provider is responsible for security of the cloud infrastructure, while you as the customer are responsible for security of the applications and data that are hosted in the cloud. Every cloud service provider has their own security architecture including many security controls that can be configured by your team so your SOC team must have a very good understanding of the controls that are available and how to configure them.

9.4.9 Incident Handling & Response

There are some specific considerations in a cloud environment. Careful planning, collaboration with the cloud service provider, automation, and continuous monitoring and logging are required. This includes:

Cloud-Specific Incident Response Plan. A cloud-specific incident response plan should be developed, tested, and maintained. The plan should include procedures for detecting, investigating, containing, and recovering from cloud-related incidents.

Since cloud environments are highly dynamic and often involve multiple service providers, it is important to have clear communication and coordination between all parties involved in the incident response process.

Cloud environments often involve shared resources and multi-tenant architectures, so it is important to have appropriate measures in place to ensure that incident response activities do not inadvertently affect other tenants or users in the cloud.

Collaboration with the Cloud Service Provider. Incident response teams should collaborate closely with the cloud service provider to ensure that incidents are addressed in a timely and effective manner. The cloud provider should be able to provide logs and other data that may be necessary for the investigation and resolution of an incident.

Cloud Service Providers often have their own incident response procedures, which should be incorporated into an organization's incident response plan. It is important to understand the roles and responsibilities of both the cloud provider and the organization in responding to incidents.

Incident Response Automation. Automation can help streamline incident response in a cloud environment. Tools such as security orchestration, automation, and response (SOAR) can help automate routine tasks and improve incident response time.

Monitoring and Logging. Monitoring and logging are critical in a cloud environment. Logs should be generated for all cloud-related activity and stored in a central location for analysis. Real-time monitoring should be implemented to detect anomalies and suspicious activity.

Cloud-Specific Incident Response Training. Incident response teams should receive training on cloud-specific incident response procedures and technologies. This training should include topics such as cloud architecture, cloud security controls, and incident response in a multi-tenant environment.

9.4.10 Security Assessments and Testing

Conventional penetration testing approaches are not designed for cloud-native environments and concentrate on procedures applicable to on-premise settings. Cloud penetration testing demands expertise that varies from standard penetration testing as it involves evaluating cloud-specific settings, passwords, applications, encryption, APIs, database, and storage access. Moreover, cloud penetration testing is influenced by the Shared Responsibility Model, which clarifies the responsibility for components within a cloud infrastructure, platform, or software.

During a Cloud penetration test, security controls that are the complete responsibility of the Cloud Service Provider (CSP) are typically excluded from the scope of the test. It is important to note that when it comes to cloud security, the focus is on testing the security within the cloud, rather than the security of the cloud itself. In an Infrastructure as a Service (IaaS) environment, security testing covers the User Access/Identity, Data, Application, and Operating System layers, while other components are managed and controlled by the Cloud Service Provider (CSP) and are considered out of scope. The scope of the penetration test is determined by the service model, and the extent and coverage of the testing will vary based on the services offered by the CSP.

Please refer to chapter 6.5.5 for more information.

9.4.11 Introducing and enforcing Application Security and DevSecOps

There is another key element of Cloud Security, and this is to incorporate security as early as possible in an organization's software development lifecycle (SDLC). In other words, security issues should be evaluated as part of pre-deployment testing of code and treated like any other bug.

Not only does this ensure deployed code is free from security vulnerabilities, but by flagging security issues during testing, developers get the opportunity to learn what vulnerabilities exist in their code and how they can avoid them in the future. The types of modern web apps that are currently being deployed on cloud networks are generally pretty complex, so organizations looking for a way to test these sorts of apps should make sure that whatever SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), or IAST (Interactive Application Security Testing) solution they're considering can handle the codebase of their apps.

DevSecOps has evolved from traditional DevOps principles and is a practice that helps with the above by integrating security into the entire software development process, from planning to deployment, to building secure applications.

In a cloud environment, Application Security and DevSecOps play a crucial role in protecting against various cyber threats such as data breaches, malware, and cyber-attacks.

10 Data Protection, Data Security & Data Loss Prevention

Data Protection, Data Security, and Data Loss Prevention (DLP) are interrelated yet distinct concepts around safeguarding sensitive and valuable data within an organization. As an organization you should be aware of these concepts as they support you in ensuring the security, privacy, and compliance of your organization's data assets. This is especially important in case your organization is dealing with any kind of external data like customer data.

Data Protection

Data Protection encompasses a broad set of practices, policies, and measures designed to secure data against unauthorized access, use, disclosure, alteration, or destruction. It focuses on ensuring the confidentiality, integrity, and availability of data. Data Protection involves strategies like encryption, access control, data masking, and anonymization to prevent data from being compromised or misused. Data Protection is often governed by regulations, such as GDPR (General Data Protection Regulation) or HIPAA, to ensure that sensitive or personal data is handled appropriately.

Data Security

Data Security is a subset of Data Protection. It refers to the measures taken to safeguard data against threats, unauthorized access, and cyber threats. It concentrates on shielding data assets through technical, administrative, and physical controls. Data Security involves implementing security measures like firewalls, intrusion detection systems, antivirus software, secure authentication, and secure coding practices. With regards to compliance, it complements Data Protection by applying security measures that ensure data is protected from internal and external threats.

Data Loss Prevention (DLP)

DLP is a specific approach aimed at identifying, monitoring, and preventing potential data breaches or unauthorized exposure or exfiltration of sensitive data. It focuses on identifying and restricting the movement of sensitive data within an organization's network or through endpoints to prevent data leakage. DLP tools and strategies inspect and control data in motion, at rest, or in use to avoid data loss, ensuring it doesn't leave the organization inappropriately. With regards to compliance, it assists organizations in meeting regulatory requirements regarding data handling and confidentiality.

We can help you with selecting, designing, and implementing various technical measures like access controls, encryption mechanisms, backup and disaster recovery measures but also with defining and implementing a robust data governance framework and policy. Organizations need to ensure that data governance practices are in place, defining roles, responsibilities, and processes for data management, access, and protection.

We can also help you to select and deploy a **Data Loss Prevention (DLP)** solution that is right for your organization. As mentioned above, DLP is a set of strategies and tools designed to prevent unauthorized exposure, misuse, or theft of sensitive data. DLP typically involves a combination of policies, processes, and technology to protect data throughout its lifecycle, from creation to deletion.

DLP uses various techniques, such as content analysis, contextual analysis, and pattern recognition, to identify and prevent data loss. For example, DLP can monitor email traffic to ensure that sensitive information is not being sent outside of the organization or can scan files stored on endpoints to identify sensitive data and apply appropriate protections.

DLP policies are typically tailored to the specific needs of an organization, based on its industry, regulatory requirements, and internal security policies. These policies may define which types of data are considered sensitive, how sensitive data should be handled and protected, and what actions should be taken in the event of a data breach.

In general, there are three types of Data Loss Prevention: Network DLP, Endpoint DLP, and Cloud DLP.

Network Data Loss Prevention focuses on preventing the unauthorized transfer of sensitive data over a network. It involves monitoring and analyzing network traffic to detect and prevent data breaches or leaks, whether intentional or accidental.

Network DLP systems use a variety of techniques to inspect network traffic, including packet capture, deep packet inspection, and protocol analysis. The goal is to identify patterns or characteristics in the traffic that may indicate the presence of sensitive data. This can include data such as social security numbers, credit card information, or other confidential information.

Once the sensitive data is identified, network DLP systems can take several actions to prevent it from being transmitted outside the network. This can include blocking the transmission, encrypting the data, or alerting security personnel to take action.

Endpoint Data Loss Prevention protects sensitive data on end-user devices, such as laptops, desktops, and mobile devices. The solution monitors and controls data transfers on these devices to prevent sensitive data from being transmitted or stored in an unauthorized manner. It also provides the ability to encrypt sensitive data and track its usage.

Endpoint DLP works by monitoring and analyzing data in real-time on the endpoint device. It uses policies and rules to detect and prevent the unauthorized transfer or storage of sensitive data. Policies can be customized to match the specific data protection needs of the organization. For example, an organization might have policies that block the transfer of sensitive data to unauthorized USB devices or cloud storage platforms.

Endpoint DLP solutions typically provide the ability to encrypt sensitive data at rest on the endpoint device. This ensures that even if the data is stolen or lost, it remains protected. Additionally, endpoint DLP can track the usage of sensitive data on the device, providing insight into who is accessing and using the data.

Cloud Data Loss Prevention is a cloud-based service offered by various cloud providers, including Amazon Web Services, Google Cloud Platform, and Microsoft Azure. It is designed to help organizations protect sensitive data in the cloud by identifying, classifying, and securing the data in various cloud services and applications.

Cloud DLP provides a wide range of features, including scanning of data at rest and in transit, masking, redaction, and tokenization of sensitive information, and advanced machine learning algorithms that can identify sensitive information across a wide range of formats and languages.

The service can be configured to monitor and enforce data security policies across multiple cloud services and applications, including email, file storage, and database services. It also provides real-time alerts and audit logs to help organizations monitor and manage potential data breaches.

11 Endpoint Protection

For many years, organizations have relied heavily on antivirus software to protect their endpoints. However, traditional antivirus solutions are no longer sufficient to defend against the increasingly sophisticated threats of today. Also, mobility has changed the way people work and access corporate data. Users now access their applications on multiple devices from a variety of locations. As a result, traditional perimeter-based security measures are not applicable anymore.

Integrating network and endpoint security is a key component of extending a **Zero Trust Architecture** to the endpoint. This approach involves deploying a variety of security controls at both the network and endpoint levels, and then integrating them to enable better threat detection and response. Some of the specific measures that can be taken to integrate network and endpoint security include deploying advanced endpoint protection solutions, such as **Endpoint Detection and Response** (EDR) tools, which enable real-time threat detection and response across all endpoints.

Such endpoint security solutions take a behavior-centric approach, incorporating a wider range of capabilities, including antivirus, exploit protection, endpoint detection and response (EDR), analytics, and device control. To gain visibility into the growing number of unmanaged network-connected devices, such as Internet-of-Things (IoT) devices, enterprise endpoint security strategies often combine endpoint protection platforms (EPP) and EDR solutions with cloud and network security tools, such as network traffic analysis (NTA).

Advanced endpoint security solutions, often included in **Extended Detection and Response** (XDR) solutions, provide powerful and comprehensive security measures by gathering and correlating data centrally, in addition to performing local analysis on individual endpoints. These solutions can prevent both known and unknown malware and exploits, incorporating automation to alleviate security team workloads, and protecting and enabling users without impacting system performance.

XDR can be seen as the evolution of EDR, which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.

Open XDR represents an advanced form of extended detection and response (XDR) security solution or platform that supports seamless integration with third-party tools and technologies. This integration allows for the collection of specific telemetry from various data sources, enabling effective threat detection, hunting, investigation, and response.

Sometimes also called Hybrid XDR, Open XDR goes beyond traditional XDR solutions by integrating diverse tools within the organization's security stack. These tools can include endpoint detection and response (EDR), next-generation firewall (NGFW), identity and access management (IAM), cloud workload protection (CWP), cloud access security broker (CASB), and more. By breaking down the silos between these tools, Open XDR enables the generation of more accurate alerts, faster response times, improved threat hunting capabilities, and streamlined investigations.

We can help you with:

- Defining your Endpoint Security Strategy and Architecture
- Integrating it with your Zero Trust Strategy and Architecture
- Selecting and Deploying a suitable EDR or XDR Solution

12 Identity & Access Management

We already mentioned a few times that traditional security models were based on the concept of a trusted perimeter around the network. But state of the art security models are built on a completely different concept flipping the traditional network design approach by starting from the inside out instead of the outside in. This means that instead of classifying users as "trusted" and "untrusted," the focus is on protecting the data or assets that require safeguarding, and the network is built around them.

In a Zero Trust Architecture, every user, device, and application are assumed to be untrusted, and access is granted on a need-to-know basis, based on continuous authentication and authorization.

This is why **Identity & Access Management** has become a top priority for many organizations. As already discussed under “Cloud Security”, Identity and Access Management (IAM) provides companies with tools for controlling user access to systems, applications, and data. IAM is designed to ensure that only authorized personnel have access to critical resources while minimizing the risk of unauthorized access, theft, or misuse of sensitive data.

Least Privileged Access (LPA) is a key component of IAM. It sets the minimum amount of access that a person or machine will need to do the job. Solutions leveraging LPA will typically employ automation to tighten or loosen permissions based on the user's role.

IAM works by providing a centralized mechanism for managing user identities, roles, and access policies across an organization's systems and applications. This can include authentication mechanisms such as username and password, Two-Factor Authentication (2FA), and **Multi-Factor Authentication (MFA)** to ensure that only authorized users can access the system.

IAM also includes access control policies that specify who can access specific resources and under what conditions. **Access Control Policies** can be based on user roles, group membership, time of day, location, and other factors. These policies are enforced by access control mechanisms, such as Access Control Lists (ACLs) and **Role-Based Access Control (RBAC)**.

Challenges with IAM:

> One of the key challenges in implementing IAM is managing the large number of users, groups, and access policies that need to be created and maintained. This can be a complex and time-consuming process, especially in large organizations. Additionally, IAM systems must be designed to be highly available and scalable, as they often need to handle millions of user requests per day.
>
> Another challenge with IAM is ensuring that users are authenticated securely, with minimal risk of their credentials being stolen or compromised. This is where MFA comes in. MFA adds an additional layer of security to the authentication process, requiring users to provide additional proof of their identity, such as a code sent to their mobile device or a fingerprint scan.

There are several solutions on the market providing a range of features and functionality to help your organization manage your IAM needs, including user provisioning, access control policies, MFA, and auditing and reporting capabilities.

Our services include:

- Conducting a review of your environment
- Providing a roadmap for implementing and optimizing the main pillars of IAM - Identity Governance and Administration, Access Management, and Privileged Account Management
- Identify your unique use cases, roles, and policies to help you select and implement the best solutions that meet your business requirements

13 Security Awareness & Education

All employees of a company – from corporate management, customer support, IT support to staff running the reception - can and must do their part to ensure safety. But various groups within a company have a different level of knowledge of IT security issues, but also have a different view on importance and impact. As always, the chain is only as strong as the weakest link.

A workforce that is unaware of all the types of dangers lurking online are a serious security risk to any organization's network and mission. In short, today's workforce cannot be untrained in Cyber Security awareness.

Cybercriminals will aim their attacks on your employees because they consider them vulnerable and high-value targets that can be easily manipulated into clicking on links in a phishing email; unknowingly initiating an online drive-by download; or unwittingly granting a threat actor access to an office or facility.

One successful attack – maybe just the result of a single wrong click on hyperlink - can lead to millions of dollars for criminals and your organization becoming a repeat target of more attacks. The price paid by an organization - even one with cyber insurance - could be millions of dollars in compliance fines and in the loss of brand confidence, revenue, shareholder value, and more.

For a security awareness and training program to be effective, it should promote and nurture a culture of security within the organization. Merely treating it as a compliance checklist item will not cultivate awareness or adapt to the constantly evolving threat environment. Hence, it is crucial to integrate Cyber Security awareness into the organization's work culture continuously. Awareness should begin at the individual level, and every employee should take responsibility for safeguarding the organization's information and assets.

We can help you with the most important steps including the following:

13.1 Assessing and Understanding your Baseline

You should start by establishing a baseline of current security risks. This helps in developing a plan and evaluating the effectiveness of a training program in improving security habits over time. A Cyber Security framework comprising a set of standards, guidelines, and best practices used to manage digital risks can provide valuable assistance in this initial stage. The framework typically aligns security objectives with policies and procedures that define an organization's best practices for managing its Cyber Security risk. There are several frameworks available, and we can help you to select the one that's right for your organization when developing a security framework tailored to your specific needs.

Also, before designing a training plan and enrolling employees in training sessions, we recommend testing their security habits. This helps to establish a baseline, identify problem areas, and focus training and reinforcement efforts. Several techniques and tools can be deployed to understand the security habits of employees like:

- Phishing Simulations
- Social Engineering Simulations
- Monitoring Tailgating
- Performing Spot Checks

13.2 Designing and Developing your Training Plan

We will work with you to clearly define your goals and develop a training and awareness plan. In this context, several questions need to be answered:

- Training Cadence
- Rollout Strategy
- Target Audience
- Communication Plan
- Success Criteria
- Remediation

We recommend investigating professional employee security awareness solutions as it's close to impossible for any organization to create such a program on their own within a reasonable amount of time and at acceptable costs.

There are several solutions on the market that can help you to establish and roll out your program and we can help you to select, customize and implement the solution that is right for your organization. This includes defining and prioritizing your areas of concern like:

- Phishing Attacks
- Snowshoeing
- Ransomware
- Social Engineering
- Social Media Guidelines
- Internet an Email Use
- Mobile Device Security
- Removable Media and Devices
- Passwords and Authentication
- Physical Security
- Work from Home
- Public Wi-Fi
- Cloud Security

13.3 Rolling Out your Security Awareness Program

Once all questions have been answered and a suitable professional solution has been selected and customized, it's time to roll out and communicate the security awareness program to employees. We can help you with developing a roll out strategy that includes:

- Informing employees ahead of time about the upcoming security awareness training
- Defining deadlines and reminding employees to complete the training on time
- Communicating the importance of training, the training plan, and the training schedule to the entire organization
- Ensuring that everyone understands the importance of security awareness training and encourage them to participate
- Using various communication channels to reach employees
- Encouraging feedback from employees about the training program

13.4 Monitoring and Managing the Impact of your Program

To ensure the success of your security and awareness program, it is important to track employee progress and behavior. Some of the following actions should be supported by the training solution that has been selected for your organization. Therefore, it is important to include this when evaluating various products. We are looking for:

- Keeping track of who has taken the training and who hasn't, along with reasons for non-participation
- Identifying areas where people are performing poorly and looking for trends to increase adoption
- Establishing a cycle of initial baseline testing, training, retesting, and remediation training for noncompliant employees
- Evaluating if, and how, employee security behaviors improve over time
- Escalating gaps to management and acting on stragglers if necessary
- Increasing or decreasing the frequency of training module distribution as needed
- Making modifications to the training campaign to meet the success criteria