Expert Services Essentials

Fortify your defenses and identify and mitigate cyber threats with the help of CYE's experts.

- Security Maturity Assessment
- Security Risk Assessment
- External Assessment
- Cloud Assessments
- OT Environment Assessment
- Secure Software Development Lifecycle Gap Analysis
- Application Security Assessment
- Secure-SDLC and Secure Coding Training for Developers
- Mitigation Workshop
- Incident Response and Digital Forensics

April
2025

Security Maturity Assessment

Description

The Security Maturity Assessment led by CYE's architecture team is a fundamental building block in evaluating and increasing the cybersecurity maturity level of an organization. The assessment focuses on the organization's various cyber defense aspects to determine the current maturity level by identifying gaps in the overall security program from a technical and procedural perspective. Moreover, the assessment is intelligence-driven; i.e., it considers the possible attackers and their motivation as an anchor point for the assessment. Finally, the team will provide recommendations for rectifying the identified gaps to increase the organizational maturity score.

The assessment includes the following activities:

- Interviews of relevant personnel to gain in-depth knowledge about the organization's procedures, infrastructure, and security controls
- Configuration reviews of critical infrastructure according to the organization's tech stack
- Analysis of current gaps in security based on NIST CSF

Relevant standards

The proprietary methodology is derived from the following sources:

- NIST Cybersecurity Framework
- ISO/IEC 27001

Deliverables

The following are the deliverables:

- All discovered findings are shown in Hyver, CYE's exposure management platform.
- The maturity level indicative of the organization's security posture is determined.
- The maturity level is derived using the NIST Cybersecurity Framework with discovered findings and organizational insights.

Security Risk Assessment

Description

The Security Risk Assessment conducted by CYE is an extensive, hands-on evaluation aimed at gauging an organization's security risk comprehensively. Its purpose is to assess the organization's current security status through the lens of a potential attacker. In subsequent assessments, we also emphasize the examination of previously identified vulnerabilities and the implementation of mitigation measures. The assessment includes the following phases, which are described as follows:

External reconnaissance

This phase involves discovering and collecting public information that can be used in attacks. Typically, it includes the following tasks:

- Passive information gathering from public resources and social networks.
- Identification of Public IP ranges, and enumeration.
- Finding publicly available vulnerabilities in hacker forums, IRCs, darknet, and so on.
- Identification of information assets, and their prioritization.
- Identification of potential threat sources, and their prioritization.
- Defining the main threat scenarios that are relevant to the company.

Internet perimeter breach

Depending on the goals, a perimeter breach is the initial entry vector into a network. If the perimeter breach is unsuccessful, an "assume breach" scenario is used, whereby the team is provided with a domain user account that is equivalent to a user account of a regular employee. This starts a scenario much further into the attack timeline.

Typically, the following activities are included:

- Identification of the client's exposed IP addresses and interfaces.
- Scanning and enumerating the exposed interfaces to identify open ports and services, which are used to determine the internet attack surface.
- Vulnerability assessment of internet-accessible services and interfaces.
- Internet connectivity for corporate network entities assessment.

Internal assessment and lateral movement

This attack stage starts within the internal network, where further reconnaissance of the network and user behavior is conducted to identify systems that are key to achieving the predetermined goals.

A command-and-control infrastructure (C2) would typically be established for redundant and persistent communications into the network. In some cases, achieving the goals will include compromising a Microsoft Active Directory domain. However, critical business systems can often be accessed via other means, negating the need to target a potentially highly monitored target such as Active Directory. Activities typically include the following:

- Scans and enumeration of various network segments and entities.
- Active Directory enumeration.
- Vulnerability assessment of servers and network equipment that may enable lateral movement.
- Active directory features and configuration abuse to perform privilege escalation and lateral movement.

Attack capability phase
When the team has the appropriate access and understanding of the relevant infrastructure, the attack capability phase is the technical execution of a predetermined goal to demonstrate the ability to exploit and show the associated risks of a complete attack chain leading up to an attack. Typically, the following activities are included:

- Cross-domain lateral movement.
- Identifying and demonstrating control over the defined critical business assets, including access to sensitive information and standard critical services.
- Performing domain-level persistence attacks.

Prerequisites

The assessment team requires the following information from the customer before the start of the assessment:

- List of organizational crown jewels. This will be the target list for the assessment's impact on the organizational risk.
- Relevant access as the potential threat actor. For example, for internal employee threat, the team will need regular domain user and machine in the network.
- Direct channel with the technical point of contact for any urgent communication during the activity.

Deliverables

When the assessment is completed:

- All discovered findings are shown in Hyver, which is CYE's exposure management platform.
- Attack routes from the threat sources to the organization's business-critical assets are shown on the mitigation graph and indicate risk.
- The maturity level that is indicative of the organization's security posture is determined for the organization. The maturity level is derived using the NIST Cybersecurity Framework with discovered findings and organizational insights.
- By incorporating risk and maturity evaluations, the customer can create optimized mitigation plans, which they can design independently and manage by configuring timelines, ownership, and cost and effort settings.

Relevant standards

The proprietary methodology is derived from the following sources:

- MITRE ATT&CK Framework: Adversary tactics and techniques knowledge base
- NIST Cybersecurity Framework
- Center for Internet Security (CIS) Critical Security Controls

External Assessment

Description

CYE's External Security Risk Assessment is a practical, hands-on evaluation designed to determine an organization's external security posture from the viewpoint of a potential attacker. The assessment aims to highlight vulnerabilities, evaluate security readiness, and support ongoing security improvements by monitoring previously identified weaknesses and corresponding mitigation actions.

Assessment phases

1. External reconnaissance

This phase focuses on identifying publicly accessible information that could be exploited by attackers. Activities typically include:

- Passive collection of information from public sources and social networks.
- Identification and enumeration of public IP address ranges.
- Discovery of publicly disclosed vulnerabilities from hacker forums, IRC channels, and the darknet.
- Identification and prioritization of information assets.

2. Internet perimeter breach

Based on defined objectives, this phase evaluates the initial entry vectors into the organization's network through external interfaces. Typical activities involve:

- Identification of externally exposed IP addresses and interfaces.
- Scanning and enumeration to identify open ports and active services, outlining the organization's attack surface.
- Comprehensive vulnerability assessments of internet-facing services and interfaces.
- Evaluation of internet connectivity security for corporate network components.

Relevant standards

Our proprietary methodology aligns with industry-leading frameworks, including:

- MITRE ATT&CK Framework: Adversary tactics and techniques knowledge base
- NIST Cybersecurity Framework
- Center for Internet Security (CIS) Critical Security Controls

Prerequisites

Before initiating the assessment, the following information is required:

- Detailed list of organizational assets.
- Domain names.
- IP addresses targeted for assessment.
- Names of relevant personnel, technologies, or suppliers, depending on assessment scope.
- Target asset lists to be finalized prior to commencement.

A scoping meeting (typically 1–2 hours) with organizational representatives may be necessary. Additionally, a one-hour meeting with a network architect after the assessment helps clarify specifics regarding the network environment, hosted assets, and user groups.

Deliverables

Upon conclusion of the assessment, deliverables include:

- Comprehensive findings integrated within Hyver, CYE's exposure management platform.
- Visualized attack paths highlighting threats to business-critical assets, displayed on a detailed mitigation graph.
- Determination of the organization's security maturity level, calculated according to the NIST Cybersecurity Framework, factoring in identified vulnerabilities and organizational context.

With these insights, clients can effectively prioritize risks, devise targeted mitigation strategies, and manage remediation timelines, responsibilities, and resource allocation independently.

Cloud Assessments

Description

The cloud assessment is a process that involves the collection of data to discover possible attack routes, misconfigurations, and weaknesses within the clients Azure, AWS, or GCP cloud environments. This is accomplished by filtering the noise and highlighting the “critical to block” actions that must be mitigated to prevent live attack paths.

The following are the main goals of the assessment:

- Estimate the security level of the cloud organization
- Identify high-risk vulnerabilities
- Map possible attack routes in the environment
- Recommend the initial remediation steps required for the assessed entities

The cloud security assessment is a a hands-on, manual penetration test using a proprietary and organized methodology of the representative platforms and systems and corresponding interviews. Specifically, the infrastructure assessment is based on the NIST Cybersecurity Framework, and the risk rating method is based on the CVSS 3.1 standard.

CYE’s cloud infrastructure assessment comprehensively evaluates cloud management resources and different components. The assessment uses a white box method to evaluate and provide the most comprehensive results possible.

This activity includes, but is not limited to, the following:

- Identity and roles management
- Deep assessment of permission allocation to identities in an environment, identifying possible privilege escalation vectors and excessive permissions allocations, and testing security features related to the subject, for example, permission boundaries and "SCP" in AWS
- Examine different levels of access to an environment and identify cross-context vectors. For example, attempt to achieve "developer" context from the "QA" context
- Potential access points to the environment
- Network-level access points, such as web interfaces that are managed in the cloud and exposed to the internet or DBs and VMs that have excessive network access
- Identity-level access points, such as roles with a broad trust policy, third party vendors that can access the environment, API gateways that can be used unauthenticated, and so on
- Key and secret access/management
- Assessing the secrets management in the environment. In addition, scanning the environment (resources configurations, environment variables, and more) for cleartext secrets

- Hardening assessments according to the best practices
- Testing the environment for CIS best practice gaps
    - Access level of third parties that are integrated into the cloud infrastructure
    - Testing the level of access of third parties that can access the cloud environment. Access of third parties to an environment poses a security risk because there is no way to know how the access is managed and what security policies the vendor uses when accessing the organization's cloud environment.
    - As a result, part of the assessment is dedicated to testing third parties' level of access to the environment. This includes testing if they can achieve a stronger context in the environment, access sensitive data, and whether they are granted unnecessary privileges.
- Segmentation/segregation between cloud resources
- Testing the level of isolation between the different environments

Relevant standards

The proprietary methodology is derived from the following sources:

- MITRE ATT&CK's knowledge base of adversary tactics and techniques
- NIST Cybersecurity Framework
- Center for Internet Security (CIS) Critical Security Controls

Deliverables

When the assessment is completed:

- All discovered findings are shown in Hyver, which is CYE's exposure management platform.
- Attack routes from the threat sources to the organization’s business-critical assets are shown on the mitigation graph and indicate risk.
- The maturity level that is indicative of the organization's security posture is determined for the organization. The maturity level is derived using the NIST Cybersecurity Framework with discovered findings and organizational insights.

By incorporating risk and maturity evaluations, the customer can create optimized mitigation plans, which they can design independently and manage by configuring timelines, ownership, and cost and effort settings.

OT Environment Assessment

Description
Operational Technology (OT) is one of the most critical components of a company's ecosystem. Strengthening its cyber resilience requires the same proactive approach as any other IT system. This is achieved by assessing the OT environment's security maturity level, identifying high-risk vulnerabilities, and recommending initial remediation steps for the assessed entities.

To adhere to the "do no harm" principle, CYE has developed a secure and safe methodology for OT assessments. This assessment is conducted in two phases:

1. Passive Data Gathering – The team collects various artifacts to understand the environment's architecture, processes, and potential vulnerabilities. This phase primarily involves reviewing firewall configurations, policies, procedures, and third-party support agreements.
2. Interviews – The objective is to gain a comprehensive understanding of the organization's cybersecurity maturity based on the NIST Cybersecurity Framework (NIST SP 800-82 Rev. 3). Conducted over several days, the interviews cover key aspects of the OT environment, including risk management, vendor management, authentication and authorization models, Purdue model implementation, iDMZ-OT connectivity, OT Wi-Fi, security controls, detection capabilities, and response and recovery measures.

Additionally, the team may perform a physical review of data centers and OT endpoints such as PLCs, HMIs, network switches, and control rooms. This inspection helps identify security gaps, such as exposed credentials, unsecured MFA devices, and alarm panels with written codes.

Prerequisites
The following prerequisites must be met before the assessment:
- Detailed OT facility and ICS architecture, including a list of OT network segments.
- List of vendors and security solutions deployed on the OT network.
- Export of OT firewall configurations.
- Various privileged credentials, depending on the assessed environment.

Deliverables
- All identified findings are documented in Hyver, CYE's exposure management platform.
- The organization's security maturity level is determined based on the NIST Cybersecurity Framework, incorporating both discovered findings and organizational insights.

Requirements from the customer
The customer is responsible for:
- Providing all relevant data, materials, and required access.
- Assisting the assessment team during onsite testing.
- Ensuring the availability of relevant stakeholders for interviews, including network personnel, key component engineers (ESD, DCS, SCADA), and OT security personnel.

Relevant standards
NIST SP800-82 rev.3, NIST CSF

Secure Software Development Lifecycle Gap Analysis

Description
Secure-SDLC gap analysis aims to find gaps in the secure software development lifecycle of product development. The main goals of this assessment are to estimate the current security status of the software development lifecycle and the DevOps chain, identify major gaps, and recommend the initial remediation steps necessary to reduce the overall risk of systems.

The assessment process is based on interviews with key organizational personnel to provide a high-level report. Upon activity finalization, CYE will communicate with the designated personnel on the client side to discuss additional recommended Secure-SDLC dive-in activities.

Prerequisites
Secure SDLC procedures and supporting documentation (if available).

Deliverables
Secure-SDLC Gap Analysis Report:
- Executive Summary: A high-level overview of the activity and results.
- Methodology.
- Detailed Description of Identified Security Gaps: An in-depth account of the security gaps discovered during the analysis.
- Follow-up Recommended Activities and Mitigation Plan: Suggested actions and plans to address the identified gaps.

Secure-SDLC Policy:
- A formal policy document outlining the practices and guidelines to be followed to ensure a secure software development lifecycle.
- Incorporating Security Gaps: The policy will incorporate and address all the security gaps identified in the Secure-SDLC Gap Analysis.

Requirements from the customer
2-3 hours of interview, email comments, and availability for potential follow-up interviews

Relevant standards
A proprietary methodology based partially on:
- Microsoft SDL
- OWASP SAMM

Application Security Assessment

Description

The main goals of this assessment are to estimate the security level of an application, to identify high-risk vulnerabilities, and to recommend the initial remediation steps necessary for the assessed entities. This security assessment is conducted based on a hands-on, manual penetration test according to an organized methodology. In particular, the application-level assessment is based on the OWASP TOP-10 standard, and the risk rating method is based on the CVSS 3.1 standard.

CYE performs testing from the perspective of an anonymous user as well as from the privileges of the various authenticated user roles in the application. This assessment is relevant to all kinds of software products: web systems, APIs, desktop application, mobile application and more.

This assessment includes:

- Scan the application servers to identify infrastructure-level vulnerabilities
- Use application scanners to identify common application vulnerabilities
- Perform manual pentesting to find additional vulnerabilities including one that cannot be identified using automated tools, such as business logic and authorization flaws
- Identify session management issues such as OAuth and JWT misconfiguration
- Identify injections and other implementation errors, including, among other XSS attacks, SQL Injection, NoSQL Injection and more
- Attempt to exploit the identified application vulnerabilities
- Perform other exploits such as cookie poisoning, business logic exploits, flooding proof-of-concept and more

At the conclusion of the application review, CYE evaluates the identified areas of weakness and rates the findings based on the risk each possess to the Company.

Relevant standards

- OWASP Top 10
- OWASP Web Security Testing Guide (WSTG)
- Proprietary methodologies and tools

Deliverables

Upon assessment's finalization, all found findings will be seen on CYE's exposure management platform, Hyver. The found findings will also be analyzed according to NIST cybersecurity framework, and together with additional insights present a clear representation of the security maturity level of the organization.

Secure-SDLC and Secure Coding Training for Developers

Description
The Secure-SDLC and Secure coding workshop raises the security awareness of developers and other R&D members and gives them the knowledge and tools to write secure code and think about security by design. This workshop, together with the implementation of Secure-SDLC practices in the daily development process, are important steps towards creating secure products and maintaining enhanced cyber-hygiene environments.

Target Audience
Software developers, code writers, R&D researchers, system architects, QA personnel and all those who affect the development of the organizations' systems and applications.

Remote 2 half-days (5.5 hours each) course agenda

Half-day 1:
SDLC Basics | Attacks in the cyber world – latest trends; Application security overview and threats; Attack and threats (live demos); OWASP Top 10; Mitigations
Half-day 2:
Guided Hands-on Hacking Exercise | Implementing the attacks, as demonstrated in the sessions of the first session; fixing the code to prevent the attacks from being executed

Relevant standards
Proprietary methodology based partially on OWASP Top 10; Microsoft SDL.

Mitigation Workshop

Description
After completing CYE's security assessments, all identified vulnerabilities are documented on Hyver, our exposure management platform. These vulnerabilities connect various threat sources to the client's critical business assets, facilitating a systematic evaluation of the impact on the organization. By employing graph theory and algorithms, we can recommend mitigation strategies that prioritize both impact and cost-efficiency.

Following a comprehensive review of all security areas, including the attack graph, vulnerabilities, their severity, and likelihood, our team develops both short-term and long-term action plans. These plans include a range of measures aimed at enhancing the client's cybersecurity posture and maturity.

These plans are then reviewed and discussed with the client and their technical staff to delve into the root causes of the issues identified and to devise solutions utilizing the organization's current tools and within the client's budget constraints. In the mitigation workshop, the initial plan proposed by Hyver and our team is further refined to better align with the specific needs, challenges, and distinctiveness of the client's environment.

Relevant standards
- NIST Cyber Security Framework
- Common Vulnerability Scoring System (CVSS)

Deliverables
A detailed action plan that includes different workstreams relevant to each security domain or technical team in the organization.

Incident Response and Digital Forensics

Description
24/7 support for ensuring successful containment, remediation, and recovery of a breach, reducing response time and minimizing business operational impact, collecting forensic evidence, threat hunting, and reporting on the scope of damage.

Deliverables
Upon completion and incident closure, CYE will provide a detailed incident summary report, including the following:

- Executive summary
- Investigation findings (including methodology, investigation process summary – containment approach, IOCs gathering, forensic analysis methodology, etc.)
- Root causes, findings, and proposed remediations

Want to learn more about how CYE's expert services can bolster your organization's security? **Contact us.**

About CYE

CYE's exposure management platform transforms the way security teams protect their organizations. With CRQ at its core, the platform reveals enterprises' exposure in financial terms, visualizes the most exploitable attack routes to critical business assets, and creates mitigation plans tailored to each business. CYE's customized reporting enables the sharing of vital board-level metrics and validating exposure reduction over time. In addition, CYE improves cybersecurity maturity by mapping weaknesses and defining targets based on industry frameworks. Founded in 2012 in Israel with operations around the world, CYE has served hundreds of organizations across industries globally. Visit us at cyesec.com.

1000 North West Street, Suite 1410, Wilmington DE 19801, United States
1 Ballards Lane, London N3 1LQ, UK | Abba Eban 10, Herzliya 4615200, Israel