SECPOINT®

www.secpoint.com

SecPoint® Penetrator™ Vulnerability Scanning Profiles

NCC-DK
DENMARK CYBERSECURITY COORDINATION CENTRE

INTERFORCE

CenSec
CENTER FOR DEFENCE, SPACE & SECURITY

CYBERSECURITY™ MADE IN EUROPE

SC MAGAZINE

Web App PENTESTING

network SECURITY

HIPAA COMPLIANT

Trustpilot
TrustScore 4.9 | 121 reviews

Defense Network North

NEW VULNERABILITY SCAN - PROFILES

You can choose between 33 different vulnerability scanning profiles.

Our scanning profiles enable quick and comprehensive scans to provide an overview of potential vulnerabilities.

You can opt for the recommended 'Normal Scan' or the more intensive 'Full Firewall Scan,' both of which are safe for production environments. To rigorously test the resilience of your firewall and systems, the 'Aggressive Scan' profile is available.

We also offer a range of compliance scanning profiles for specific needs.

If you're uncertain about the most suitable profile for your network security environment, don't hesitate to reach out to us for guidance.

Profile 1 - Best Scan - Popular Ports	**Profile 9 – SSL Security Checks**
Profile 2 – Lethal HTTPS Web Attack Scan	**Profile 10 – VoIP Devices**
Profile 3 – SSL & CMS Web Scan – Wordpress – Joomla	**Profile 11 – Cloud Infrastructure and Services Security Scan**
Profile 4 – Wordpress Web Scan	**Profile 12 – OWASP 10 2021 Compliance**
Profile 5 – Quick Scan – Most Common Ports	**Profile 13 – PCI-DSS Preparation for Web Applications**
Profile 6 – Full Scan – All 65.535 Ports	**Profile 14 – HIPAA Policy Scan for Compliance**
Profile 7 – Firewall Scan – Stealth Scan	**Profile 15 – SCADA ICS PLC IoT**
Profile 8 – Aggressive Scan – Exploits & DoS Attacks	**Profile 16 – CWE 2011 Compliance**

NEW VULNERABILITY SCAN - PROFILES

You can choose between 33 different vulnerability scanning profiles.

Using these vulnerability scanning profiles ensures comprehensive compliance across key regulatory frameworks, including GLBA, FFIEC, SOX, and more. Each scan is tailored to meet specific legal and cybersecurity standards, helping organizations maintain integrity, minimize risks, and ensure adherence to stringent protocols such as NSA and CERT guidelines.

This helps streamline audits, mitigate compliance violations, and safeguard critical assets, all while meeting the highest industry requirements. Regular scanning enhances overall cybersecurity posture, giving you peace of mind and better control over regulatory obligations.

Profile 17 – ISO 27001 Compliance	**Profile 26 – SCAP Compliance Scan**
Profile 18 – NIST 800-53/FISMA Compliance	**Profile 27 – SOX Compliance Scan**
Profile 19 – CIS Controls v8.0 Compliance	**Profile 28 – CERT Compliance Scan**
Profile 20 – CMMC Level 1 ComplianceScan	**Profile 29 – COBIT/ITIL Compliance Scan**
Profile 21 – DORA Compliance scan	**Profile 30 – DISA STIGs Compliance Scan**
Profile 22 – GLBA Integrity Compliance	**Profile 31 – FDCC Compliance Scan**
Profile 23 – FFIEC Compliance Scan	**Profile 32 – NSA Compliance Scan**
Profile 24 – CyberScope Compliance Scan	**Profile 33 – NIS2 Compliance Scan**
Profile 25 – NERC Compliance Scan	**Profile 34 – CRA Compliance Scan**

NEW VULNERABILITY SCAN - PROFILES

Profile 1 - Best Scan - Popular Ports	Profile 2 – Lethal HTTPS Web Attack Scan
• Will do a non harmful scan with recommended ports. • Scans 8000 among the most common ports. • Performs 146.000+ checks. • Web application vulnerability scanner WAS. • Automatic Service Identification. • SQL Injection - XSS Cross Site Scripting - Remote Code Execution. • Web Crawler - Joomla Security Scan - Google Safe Browsing. • 50+ Blacklist Checks. Wordpress Security Scan. • Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS and much more. • Scans Windows, Mac OS X, Linux, *Nix and other operating systems. • Duration can be several hours depending on how many services are found during the scan. • The normal scan will scan for all areas only limited to most common ports. • It is designed to be non-disruptive and avoids overwhelming the services by simulating human behavior.	• SQL Injection (SQLi). • Blind SQL Injection (Blind SQLi). • Cross Site Scripting (XSS). • Attack String Reflection (Reflected XSS). • Command Code Execution (RCE). • Web Crawler. • Remote File Inclusion. • Directory Traversal. • Scans Web portals. • CMS, Web pages. • Web Interfaces. • Nix and other operating systems. • Duration can be several hours depending on how many services are found during the scan. • It is designed to be non-disruptive and avoids overwhelming the services by simulating human behavior.

NEW VULNERABILITY SCAN - PROFILES

Profile 3 – SSL & CMS Web Scan	Profile 4 – Wordpress Web Scan
• Will do a non harmful scan with recommended ports. • Ports such as 80,443,3128,8000,8080,8843,9443,9997,9998. • Web application vulnerability scanner WAS. • Lethal Attack Crawler. • SQL Injection (SQLi). • Blind SQL Injection (Blind SQLi). • Cross Site Scripting (XSS). • Reflected Cross Site Scripting (Reflected XSS). • Checks for popular SSL Vulnerabilities such as: Heartbleed – Ticketbleed – BREACH. • Scans Windows, Mac OS X, Linux, *Nix and other operating systems. • Duration can be several hours depending on how many services are found during the scan. • The normal scan will scan for all areas only limited to most common ports. • It is designed to be non-disruptive and avoids overwhelming the services by simulating human behavior.	• Scans web ports such as Port 80, 443. • Quick Wordpress Scan. • Lethal Attack Crawler. • SQL Injection (SQLi). • Blind SQL Injection (Blind SQLi). • Cross Site Scripting (XSS). • Cross Site Scripting Attack String Reflection (Reflected XSS). • Remote Code Execution (RCE). • Remote File Inclusion. • Directory Traversal. • Nix and other operating systems. • Duration can be several hours depending on how many services are found during the scan. • It is designed to be non-disruptive and avoids overwhelming the services by simulating human behavior.

NEW VULNERABILITY SCAN - PROFILES

Profile 5 – Quick Scan – Most Common Ports	Profile 6 – Full Scan – All 65.535 Ports
• Scan Profile Quick Scan Top common popular ports for fast scan. • Same as best scan but faster scanning. • Lethal Attack Crawler. • SQL Injection (SQLi). • Blind SQL Injection (Blind SQLi). • Cross Site Scripting (XSS). • Reflected Cross Site Scripting (Reflected XSS). • Remote Code Execution (RCE). • Remote File Inclusion. • Directory Traversal. • Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS & much more. • Scans Windows, Mac OS X, Linux, Nix and other operating systems. • Duration can be several minutesdepending on how many services are found during the scan. • It is designed to be non-disruptive and avoids overwhelming the services by simulating human behavior.	• Will do a non harmful scan with 65.535 ports. • Scans the whole range of 65535 Ports. • Performs 146.000+ checks. • Web application vulnerability scanner. • WAS Automatic Service Identification. • SQL Injection(SQLi) Blind SQL Injection (Blind SQLi). • Cross Site Scripting (XSS) Reflected (Reflected XSS). • Remote Command Execution (RCE) Web Crawler. • Google Hack DB Joomla Security Scan. • Google Safe Browsing 50+ Blacklist Checks. • Wordpress Security Scan. • Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS and much more. • Scans Windows, Mac OS X, Linux, Nix and other operating systems. • Duration can be several hours depending on how many services are found during the scan. • It is designed to be non-disruptive and avoids overwhelming the services by simulating human behavior.

NEW VULNERABILITY SCAN - PROFILES

Profile 7 - Firewall Scan - Stealth Scan

- Will do a non harmful scan with 65535 ports.
- Scan Profile Full Firewall Scan The Full scan will force the ports to be scanned even if port scanning blocking is in place.
- Scans the whole range of **Common Firewall Ports**.
- Performs 146.000+ checks.
- Especially designed for firewalls, because tries to scan nodes even if they appear offline.
- Web application vulnerability scanner WAS.
- Automatic Service Identification.
- SQL Injection.
- XSS Cross Site Scripting.
- Command Execution.
- Web Crawler.
- Joomla Security Scan. Google Safe Browsing.
- 50+ Blacklist Checks. Wordpress Security Scan.
- Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS and much more.
- Scans Windows, Mac OS X, Linux, Nix and other operating systems.
- Duration can be several hours depending on how many services are found during the scan.
- It is designed to be non-disruptive and avoids overwhelming the services by simulating human behavior.

Profile 8 - Aggressive Scan - Full Scan, Exploits & DoS Attacks

- Will do a Full Port Scan, Overflow Attacks + DoS Attacks
- Scan Profile Aggressive Scan The Aggressive Profile will launch Denial of Service DoS attacks & Exploit attacks.
- This is only recommended on pre production systems since it can cause systems to crash.
- Scans the whole range of 65.535 Ports.
- Includes **Overflow** and **Denial of Service (DoS) attacks**.
- Performs 146.000+ checks.
- Web application vulnerability scanner WAS
- Automatic Service Identification
- SQL Injection
- XSS Cross Site Scripting
- Command Execution
- Web Crawler
- Joomla Security Scan, Wordpress Security Scan
- Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS and much more.
- Scans Windows, Mac OS X, Linux, Nix and other operating systems.
- **Duration can be several hours depending on how many services are found during the scan**.

The Aggressive profile is designed to apply rigorous testing methods, which could be harmful to pre-production systems.

Note: Always make sure users are adequately informed about the potential risks before running any kind of aggressive or potentially harmful tests.

NEW VULNERABILITY SCAN - PROFILES

Profile 9 – SSL Security Checks	Profile 10 – VoIP Devices
• This profile scans for common SSL checks. • Scans for missing security headers such as • X-Frame-Options, X-Xss-Protection, X-Content-Type-Options, Referrer-Policy • It is designed to be non-disruptive and avoids overwhelming the services by simulating human behavior	• This scan willl check if the audited target for vulnerable VoIP or exposing sensitive data. • It is designed to be non-disruptive and avoids overwhelming the services by simulating human behavior

NEW VULNERABILITY SCAN - PROFILES

Profile 11 – Cloud Infrastructure and Services Security Scan

- This profile focuses on identifying misconfigurations, vulnerabilities, and non-compliance with best practices in cloud environments.
- This scan includes checks for exposed data storage, unsecured cloud services, and adherence to cloud platform security guidelines. This scan is vital for organizations leveraging cloud computing to ensure their infrastructure remains secure and resilient against potential threats.
- Will do a non harmful scan on the most common ports.

Profile 12 – OWASP Top 10 Scan 2021 Scan

- Scan Profile OWASP Top 10 Scan.
- **This profile will carry out checks in the OWASP TOP 10. For each of these profiles, when every target IP in a scan is audited with the same profile.**
- Will perform a OWASP 10 2021 compliant scan:
  - A01-2021 – Broken Access Control
  - A02-2021 – Cryptographic Failures
  - A03-2021 – Injection
  - A04-2021 – Insecure Design
  - A05-2021 – Security Misconfiguration
  - A06-2021 – Vulnerable and Outdated Components
  - A07-2021 – Identification and Authentication Failures
  - A08-2021 – Software and Data Integrity Failures
  - A09-2021 – Security Logging and Monitoring Failures
  - A10-2021 – Server-Side Request Forgery

  It is designed to be non-disruptive and avoids overwhelming the services by simulating human behavior.

NEW VULNERABILITY SCAN - PROFILES

Profile 13 – PCI-DSS Preparation for Web Applications

- Scans web applications for compliance with the Payment Card Industry Data Security Standard (PCI DSS) requirements.
- This profile will perform A Vulnerability Scan for web applications on the selected targets.
- PCI does not allow self assessments, but requires an external vulnerability scan
- from an Authorized Scanning Vendor (ASV).
- Secpoint Penetrator will perform an Internet based scan as it would be done by an ASV.
- Lethal Attack Crawler - SQL Injection, Blind SQL Injection, XSS, XSS Attack String Reflection, RCE, Remote File Inclusion, Directory Traversal.

- Essential technical checks for preparing for PCI compliance:
- 1. TLS Encryption Verification: Check for the use of TLS 1.2 or higher on all services exposed to the internet.
- 2. Firewall Configuration Review: Verify that only necessary ports are open and default rules do not allow unrestricted access.
- 3. Default Credentials Test: Scan for services using default or weak credentials.
- 4. Software Vulnerability Scan: Identify outdated software versions and known vulnerabilities in operating systems and applications.
- 5. Data Encryption at Rest: Verify encryption of stored cardholder data.
- 6. Access Rights Audit: Check for proper implementation of access control measures and validate that only authorized personnel have access to cardholder data.
- 7. Malware Protection Effectiveness: Confirm that antivirus/antimalware solutions are operational and signatures are up-to-date.
- 8. Application Vulnerability Scanning: Perform web application scans for common vulnerabilities (e.g., SQL Injection, XSS) and misconfigurations.
- 9. System Logging and Monitoring Configuration: Ensure that logging is enabled for all access to network resources and cardholder data, with a mechanism for regular review.
- 10. Patch Management Verification: Scan for missing security patches and outdated software that may present a security risk.
- 11. Secure Configuration Checks: Verify that systems and applications are hardened according to the best security practices.
- 12. Network Segmentation Tests: Check that the cardholder data environment is properly segmented from the rest of the network.
- 13. Two-Factor Authentication for Remote Access: Ensure that two-factor authentication is required for any remote access to the network.
- 14. File Integrity Monitoring: Confirm that file integrity monitoring tools are in place and configured to alert on unauthorized changes to critical files.
- 15. SSL/TLS Best Practices Check: Scan for weak ciphers, expired certificates, and other SSL/TLS misconfigurations.

Profile 14 – HIPAA Policy Scan for Compliance

- The HIPAA profile will perform a scan on the requested targets to assess compatibility with the HIPAA security regulations.
- This vulnerability scan should be considered as a part of the HIPAA Security Risk Analysis assessment (SRA).
- This scan will check if the audited target systems are exposed to risk or comply with the key HIPAA security regulations.
- Designed for healthcare organizations, this scan checks for compliance with the Health Insurance Portability and Accountability Act (HIPAA) security rules.
- This scan will check if the audited target systems are exposed to risk or comply with the key HIPAA security regulations
- To ensure HIPAA compliance through vulnerability scanning, it is critical to concentrate on Electronic Protected Health Information (ePHI) protection against threats that might compromise its confidentiality, integrity, and availability. Vulnerability scanning can automate the identification of security weaknesses that could potentially be exploited.
- A list of checks tailored to the capabilities of vulnerability scanning for a thorough assessment for HIPAA compliance:
- 1. SSL/TLS Security: Check for weak ciphers, expired certificates, and SSL/TLS misconfigurations that could jeopardize ePHI transmission.
- 2. Firewall Configuration Audit: Assess firewalls to ensure they are correctly configured with unnecessary ports closed to protect ePHI.
- 3. Default Credentials Test: Identify services and devices with default or weak credentials.
- 4. Patch Management Verification: Detect missing security patches in operating systems and applications that pose risks to ePHI.
- 5. Antivirus/Antimalware Status: Ensure antivirus and antimalware tools are operational, up-to-date, & scanning effectively.
- 6. Secure Configuration Audits: Check system & application configurations for unnecessary services & vulnerabilities.
- 7. Security Configuration Management: Review system and application security configurations for compliance with ePHI protection best practices.
- 8. Vulnerability and Configuration Management: Continuously scan for and address vulnerabilities and misconfigurations.
- 9. Encryption Validation: Confirm encryption of ePHI both in transit and at rest to meet data protection standards.
- 10. Insecure Services & Protocols: Identify insecure services & protocols that could allow unauthorized ePHI access.
- 11. Physical Access Check (Policy Review): Although not directly scannable, ensure there is a process to review and control physical access to systems and devices storing ePHI.
- 12. Wireless Security Assessment: Evaluate the security of wireless networks, ensuring encryption and strong authentication methods protect access to ePHI. This can be performed in the WiFi Pen Testing menu.
- 13. Vulnerability Management: Perform continuous vulnerability scanning and address identified vulnerabilities in a timely manner to protect ePHI from known threats.
- This checklist focuses on how vulnerability scanning identifies and assesses risks to ePHI. Regular scans and prompt remediation are crucial for HIPAA compliance and safeguarding ePHI from unauthorized access.

NEW VULNERABILITY SCAN - PROFILES

Profile 15 – SCADA ICS PLC

- Targets vulnerabilities in Industrial Control Systems (ICS), Programmable Logic Controllers (PLC), and Internet of Things (IoT) devices, crucial for critical infrastructure.
- Optimized Scan for Industry Scanning
- SCADA (Supervisory Control and Data Acquisition)
- ICS (Industrial Control Systems)
- PLC (Programmable Login Controllers)
- IoT (Internet of Things)
- Including Popular Systems such as:
- Niagara / Foxboro / Moxza / Emerson
- GE General Electrics / Hitachi
- Mitsubishi / Panasonic / Rockwell
- Fisher / IEEE / Schneider / Beckhoff
- OSIsoft / OMRON / OPC / ABB
- Iconic / SNC / Sielco / Telvent
- RUGGEDCOM / Danfoss / Modbus
- Phoenix / Siemens / Tridium
- Lethal Attack Crawler - SQL Injection, Blind SQL Injection, XSS, XSS Attack String Reflection, RCE, Remote File Inclusion, Directory Traversal.

Profile 16 – CWE 2011 Compliance

- Checks for vulnerabilities listed in the 2011 Common Weakness Enumeration (CWE), focusing on software and hardware weaknesses. The scan checks whether the target complies with the 2011 CWE/SANS Top 25 Most Dangerous Software Errors list. Compliance with CWE Top 25 (CWE 2021 for the year-specific list) focuses on identifying & mitigating the most critical software issues that could lead to vulnerabilities. A scan for CWE 2021 compliance aims to detect weaknesses that could cause security breaches. Below is a list of checks for vulnerability scanning to ensure CWE 2021 compliance:

1. Injection Flaws: Scan for vulnerabilities allowing code injection, including SQL, NoSQL, OS, & LDAP injections.
2. Broken Authentication: Identify flaws in authentication mechanisms that could allow unauthorized access.
3. Sensitive Data Exposure: Check for weak protection of sensitive data like financial or personal info, which could lead to breaches.
4. XML External Entities (XXE): Detect issues in XML data processing that could result in unauthorized access or denial of service.
5. Broken Access Control: Flaws allowing attackers to bypass authorization & access sensitive data.
6. Security Misconfiguration: Identify poorly implemented security settings that create vulnerabilities.
7. Cross-Site Scripting (XSS): Detect vulnerabilities allowing attackers to inject scripts into web pages viewed by others.
8. Insecure Deserialization: Check for vulnerabilities where untrusted data is used, leading to attacks like remote code execution.
9. Using Components with Known Vulnerabilities: Identify outdated or vulnerable software components.
10. Insufficient Logging & Monitoring: Assess whether logging & monitoring are adequate to detect potential breaches.
11. Insecure Direct Object References (IDOR): Scan for vulnerabilities where an attacker can access objects via user-supplied input.
12. Cross-Site Request Forgery (CSRF): Detect vulnerabilities that enable unauthorized commands from trusted users.
13. Improper Error Handling: Identify flaws in error handling that may disclose sensitive information.
14. Hard-coded Credentials: Check for vulnerabilities related to embedded, unchangeable credentials.
15. Server-Side Request Forgery (SSRF): Detect vulnerabilities that allow attackers to force servers to make arbitrary requests.

- This list aligns with the CWE 2021 Top 25 & supports regular scans to identify and mitigate software weaknesses. Immediate action on detected vulnerabilities is crucial to prevent potential security breaches.

NEW VULNERABILITY SCAN - PROFILES

Profile 17 – ISO 27001 Compliance

- Assesses systems and processes against the ISO/IEC 27001 standard for information security management systems (ISMS). ISO 27001 compliance, an international standard for ISMS, involves a systematic, ongoing approach to managing sensitive company information securely. It covers people, processes, and IT systems through risk management. Vulnerability scanning for ISO 27001 helps identify and assess vulnerabilities affecting information confidentiality, integrity, and availability. Below is a structured checklist for ISO 27001 standards:

1. Information Security Policies: Ensure compliance with policies by scanning for unauthorized changes to policies, procedures, and configurations.
2. Organization of Information Security: Scan for proper management of information security within organizational processes, ensuring clear responsibilities.
3. Human Resource Security: Update access controls before, during, & after employment to reduce unauthorized access risks.
4. Asset Management: Identify systems storing, processing, or transmitting sensitive data without proper protection, ensuring assets are managed securely.
5. Access Control: Scan for misconfigurations that could allow unauthorized access, enforcing least privilege principles.
6. Cryptography: Check for weak encryption algorithms and poor key management practices that could compromise data.
7. Physical and Environmental Security: Ensure logical access controls for physical security systems remain uncompromised.
8. Operations Security: Identify vulnerabilities in malware protection, backups, logging, & operational software control.
9. Communications Security: Scan for network security weaknesses and vulnerabilities affecting data in transit.
10. System Acquisition, Development, and Maintenance: Check for vulnerabilities throughout the system lifecycle, protecting against data loss, malware, and unauthorized access.
11. Supplier Relationships: Assess security in supplier data interfaces, ensuring monitoring and auditing for compliance.
12. Information Security Incident Management: Identify gaps in incident detection and response, ensuring effective breach management.
13. Business Continuity Management: Scan for vulnerabilities impacting business continuity and data recovery.
14. Compliance: Ensure legal and contractual compliance with intellectual property, records protection, privacy, and cryptography regulation.

- This vulnerability scanning checklist aims to proactively identify weaknesses to maintain ISO 27001 compliance. Regular scanning and remediation ensure the confidentiality, integrity, and availability of information. ISO 27001 compliance extends beyond technical measures, encompassing policies, procedures, and organizational strategies alongside technical controls.

Profile 18 – NIST 800-53/FISMA Compliance

- Aims to ensure compliance with NIST SP 800-53 and the Federal Information Security Management Act (FISMA) for federal systems. NIST SP 800-53 provides security controls for U.S. federal information systems, excluding national security, and is widely used by non-federal systems for robust security management. Vulnerability scanning aligned with NIST SP 800-53 targets identifying and mitigating vulnerabilities threatening system confidentiality, integrity, and availability. Below is a focused list of vulnerability checks to support NIST SP 800-53 compliance:

1. Access Control (AC): Scan for weak access control enforcement, ensuring unauthorized users can't access or modify data.
2. Audit and Accountability (AU): Check logging and audit mechanisms, ensuring actions are traceable to individuals and unauthorized access is logged.
3. Awareness and Training (AT): Ensure systems enforce security awareness, with login security notices and reminders.
4. Configuration Management (CM): Detect unauthorized changes to configurations, ensuring systems are hardened.
5. Contingency Planning (CP): Scan for vulnerabilities in backup and recovery processes affecting system resilience.
6. Identification and Authentication (IA): Check for weaknesses in authentication mechanisms, ensuring they are strong and effective.
7. Incident Response (IR): Identify gaps in incident response, including the lack of automatic alerts for security incidents.
8. Maintenance (MA): Scan for vulnerabilities in maintenance processes, ensuring they don't introduce new risks.
9. Media Protection (MP): Check for data leakage vulnerabilities in digital and non-digital media protection.
10. Physical and Environmental Protection (PE): Ensure systems related to physical access controls aren't vulnerable to tampering.
11. Planning (PL): Verify security plans are reflected in system configurations and policies.
12. Risk Assessment (RA): Identify systems not regularly assessed for vulnerabilities, ensuring continuous risk management.
13. System and Services Acquisition (SA): Check for security in system and service acquisitions, ensuring security integration in life cycles.
14. System and Communications Protection (SC): Scan for communication protection weaknesses, ensuring data integrity and confidentiality.
15. System and Information Integrity (SI): Identify gaps in malware protection and data integrity checks.
16. Supply Chain Risk Management (SR): Assess supply chain vulnerabilities to prevent security weaknesses from third-party products.

- This checklist configures vulnerability scanning to address NIST SP 800-53 security controls. Regular scans aligned with these checks are vital for identifying and mitigating risks. Timely action on identified vulnerabilities ensures system security per NIST guidelines, with compliance requiring a combination of administrative, physical, and technical controls.

NEW VULNERABILITY SCAN - PROFILES

Profile 19 – CIS Controls v8.0 Compliance

- Evaluates security posture according to Center for Internet Security (CIS) Controls version 8.0 for robust cyber defense.
- CIS Controls are recognized global best practices for securing IT systems and data, formerly known as the SANS Top 20.
- Compliance with CIS v8.0 follows guidelines to counter key cyber threats. These controls are updated to address new risks and defense tactics. Scanning for CIS v8.0 compliance helps detect exploitable vulnerabilities. The following checks align with CIS Controls v8.0:

1. Enterprise Asset Control: Ensure all hardware is identified and managed, preventing unauthorized devices.
2. Software Asset Control: Identify unauthorized software and ensure only approved installations, reducing vulnerabilities.
3. Data Protection: Check vulnerabilities that could lead to breaches, ensuring encryption and secure handling of sensitive data.
4. Secure Configuration: Identify system and application misconfigurations and ensure secure setups based on current benchmarks.
5. Account Management: Scan for weak practices like default credentials or excessive privileges, following least privilege principles.
6. Access Control: Ensure access is based on necessity and prevent unauthorized entry.
7. Vulnerability Management: Continuously scan and address new vulnerabilities.
8. Audit Log Management: Ensure logs are configured and retained for security incident detection and investigation.
9. Email & Browser Protections: Detect vulnerabilities that could enable phishing or malware.
10. Malware Defenses: Check for missing or misconfigured malware protection.
11. Data Recovery: Ensure secure backups are in place for data loss prevention and recovery.
12. Network Infrastructure: Identify and secure vulnerabilities in network devices.
13. Network Device Security: Check for misconfigurations in firewalls, routers, and switches.
14. Boundary Defense: Identify weaknesses in perimeter defenses and ensure external threats are blocked.
15. Security Awareness: Enforce security awareness through system configurations promoting user notifications.
16. Service Provider Management: Assess third-party vulnerabilities and secure access.
17. Application Security: Identify vulnerabilities in web and non-web apps, ensuring secure development and maintenance.
18. Incident Response: Ensure incident response plans are prepared to detect and manage breaches.
19. Penetration Testing: Verify regular penetration testing catches vulnerabilities missed by automated scans.

- Routine scans and swift remediation are critical to maintaining a strong security posture. Combine automated scans with manual reviews for comprehensive defense.

Profile 20 – CMMS Level 1 Compliance Scan

- As CMMC Level 1 does not require formal documentation, processes are expected to be performed rather than institutionalized. The emphasis is on demonstrating that the organization performs the specified practices consistently.
- This scan evaluates the environment for technical controls that correspond to Level 1 requirements, such as:
- - Account and password controls
- - System boundary defenses
- - Endpoint protection mechanisms
- - Media handling safeguards
- - Limited access to information systems and storage
- The scan results will help identify gaps in foundational cyber hygiene, serving as a first step toward strengthening overall cybersecurity readiness and supporting compliance with DoD contracting requirements.
- ID Description Scan Type
- AC.1.001 Limit access to FCI to authorized users Human
- AC.1.002 Limit operations to least privilege Human
- AC.1.003 Control external system connections Scannable
- AC.1.004 Protect publicly posted information Human
- IA.1.076 Track system users and devices Scannable
- IA.1.077 Verify identity before granting access Human
- MP.1.118 Sanitize or destroy media before disposal Human
- PE.1.131 Restrict physical access to systems Human
- PE.1.132 Escort and monitor visitors Human
- PE.1.133 Maintain physical access logs Human
- PE.1.134 Control physical access devices Human
- SC.1.175 Protect communications at boundaries Scannable
- SC.1.176
- Scannable
- Identify and correct system flaws Scannable
- Use malware protection on systems Scannable
- Keep malware protections updated Scannable
- Perform periodic and real-time scans Scannable

NEW VULNERABILITY SCAN - PROFILES

Profile 21 – DORA Compliance SCan

- Ensures compliance with the EU Digital Operational Resilience Act (DORA) for financial entities and ICT service providers.
- This profile focuses on identifying vulnerabilities, misconfigurations, and ICT risks to align with DORA's requirements for operational resilience and risk management.
- Vulnerability Scanner Checks:
- System Vulnerabilities: Scan for weaknesses in ICT systems that could be exploited by attackers.
- Access Control Validation: Identify misconfigured or overly permissive access controls.
- Incident Reporting Readiness: Detect gaps in log collection, retention, and incident response configurations.
- Third-Party Risks: Scan for vulnerabilities in integrations with ICT service providers.
- Patch Management: Identify outdated or missing patches that could lead to exploits.
- Network Monitoring Gaps: Assess network configurations for potential monitoring blind spots.
- Human Actions (Consultant Required):
- Policy Development: Craft incident response, risk management, and operational resilience policies tailored to the organization.
- Third-Party Risk Assessments: Conduct in-depth reviews of vendor contracts, security measures, and operational dependencies.
- Governance Reviews: Ensure that DORA compliance efforts align with the organization's business strategy and regulatory obligations.
- Simulated Tests: Perform hands-on resilience tests, such as tabletop exercises or cyberattack simulations.
- Regulatory Reporting: Assist in preparing reports required by DORA regulatory authorities.
- Performs Penetration Testing-level checks using automated, safe technique.
- APT Group Fingerprinting Module added for enhanced threat detection.

Profile 22 – GLBA Integrity Compliance

- Ensures systems handling financial data comply with the Gramm-Leach-Bliley Act (GLBA) to protect consumer financial information.
- The Gramm-Leach-Bliley Act (GLBA), or Financial Services Modernization Act of 1999, mandates financial institutions explain data-sharing practices and safeguard sensitive information. GLBA compliance focuses on protecting customer data from unauthorized access or alterations. Vulnerability scanning for GLBA compliance identifies and mitigates risks to the confidentiality, integrity, and availability of customer financial information. Key vulnerability checks for GLBA integrity:

1. Access Controls: Ensure proper access control, restricting access to authorized personnel based on the least privilege principle.
2. Data Encryption: Identify areas where financial data lacks encryption, ensuring protection in transit and at rest.
3. Change Management: Check for vulnerabilities in change management procedures to ensure changes are logged, reviewed, and authorized.
4. Network Security: Identify network security weaknesses, ensuring firewalls and other defenses are properly configured and updated.
5. Vulnerability Management: Detect outdated systems or software, ensuring regular scanning and patching to address vulnerabilities.
6. Incident Response: Assess the effectiveness of incident response plans and monitoring systems to protect customer information.
7. Secure Software Development: Scan for vulnerabilities in applications managing financial data, ensuring secure development and integration.
8. Third-party Oversight: Evaluate third-party providers with access to financial information, ensuring compliance with GLBA standards.
9. Disposal of Information: Ensure policies for securely disposing of financial data, preventing unauthorized access to unused data.
10. User Authentication: Check for weak authentication systems, ensuring strong methods to prevent unauthorized access.
11. Data Integrity: Identify the absence of integrity controls like checksums to ensure data hasn't been tampered with.
12. Audit Trails: Verify systems maintain audit trails for accessing and modifying customer information, ensuring accountability.

- This vulnerability checklist helps identify potential threats to financial data integrity under GLBA. Regular scans and quick remediation are crucial for financial institutions to protect sensitive data and remain GLBA-compliant. A comprehensive approach, including technical, administrative, and physical safeguards, is essential for maintaining data security.

NEW VULNERABILITY SCAN - PROFILES

Profile 23 – FFIEC Compliance Scan

- Ensures compliance with the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook, covering critical areas for financial institutions.
- **Scope:** Comprehensive scan covering all critical systems and applications within the organization.
- **Key Checks:**
- - Access Controls: Verify proper access controls to ensure only authorized personnel have access to sensitive financial data.
- - Authentication Mechanisms: Assess the strength and implementation of authentication methods.
- - Data Encryption: Ensure encryption of sensitive financial data both in transit and at rest.
- - Patch Management: Identify outdated systems and missing security patches.
- **Human actions:**
- - Audit Logs: Check for proper logging and monitoring of all access and changes to critical systems.
- - Incident Response: Evaluate the effectiveness of incident response plans and procedures.
- - Vendor Management: Assess the security measures and controls of third-party service providers.
- - Backup and Recovery: Verify the existence and effectiveness of backup and recovery processes.
- - Physical Security: Ensure proper physical security measures are in place for data centers and other critical facilities.

Profile 24 – CyberScope Compliance Scan

- Ensures compliance with CyberScope reporting requirements for federal agencies.
- This profile focuses on identifying misconfigurations, vulnerabilities, and non-compliance with best practices in federal information systems to meet CyberScope compliance requirements.
- Key Checks:
- Configuration Management: Assess the configurations of systems and applications for compliance.
- Vulnerability Scanning: Perform regular vulnerability scans and ensure timely remediation.
- Access Control: Check for proper implementation of access controls and user authentication.
- Continuous Monitoring: Ensure continuous monitoring of systems and networks.
- Patch Management: Identify and remediate missing patches and outdated software.
- Human actions:
- System Inventory: Verify a comprehensive inventory of all IT assets.
- Risk Management: Assess the organization’s risk management practices and documentation.
- Incident Response: Evaluate incident detection, response, and reporting mechanisms.

NEW VULNERABILITY SCAN - PROFILES

Profile 25 – NERC Compliance Scan

- Targets compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.
- This profile focuses on systems and assets critical to the operation of the bulk electric system.
- Key Checks:
- Access Control: Verify strict access controls to critical cyber assets.
- Systems Security Management: Check for secure configuration and management of critical systems.
- Information Protection: Ensure sensitive information is protected against unauthorized access.
- Configuration Change Management: Assess the processes for managing changes to critical systems.
- Human actions:
- Electronic Security Perimeters: Assess the security of electronic perimeters surrounding critical cyber assets.
- Physical Security: Ensure proper physical security measures are in place for critical assets.
- Incident Reporting and Response: Evaluate the effectiveness of incident reporting and response plans.
- Recovery Plans: Verify the existence and effectiveness of recovery plans for critical assets.

Profile 26 – SCAP Compliance Scan

- Ensures compliance with the Security Content Automation Protocol (SCAP) for automating vulnerability management and compliance.
- This profile focuses on comprehensive scan of all systems and applications for SCAP compliance.
- Key Checks:
- Vulnerability Scanning: Perform SCAP-compliant vulnerability scans.
- Patch Management: Identify and remediate missing security patches.
- Configuration Management: Assess configurations against SCAP benchmarks.
- Continuous Monitoring: Ensure continuous monitoring for vulnerabilities and compliance.
- Reporting: Generate SCAP-compliant reports for auditing and compliance purposes.
- Security Automation: Ensure automation of security checks and remediation processes.
- Human actions:
- Inventory Management: Verify comprehensive inventory of IT assets.

NEW VULNERABILITY SCAN - PROFILES

Profile 27 – SOX Compliance Scan	Profile 28 – CERT Compliance Scan
• Ensures compliance with the Sarbanes-Oxley Act (SOX) for protecting financial data integrity and accuracy. • This profile focuses on systems and processes related to financial reporting. • Key Checks: • Access Controls: Verify proper access controls to financial reporting systems. • Data Integrity: Check for mechanisms to ensure the integrity and accuracy of financial data. • Change Management: Assess processes for managing changes to financial systems and data. • User Authentication: Evaluate the strength and implementation of user authentication mechanisms. • Vendor Management: Assess the security measures and controls of third-party service providers handling financial data. • Human actions: • Audit Trails: Ensure proper logging and monitoring of all access and changes to financial data. • Data Backup and Recovery: Verify the existence and effectiveness of backup and recovery processes for financial data. • Incident Response: Evaluate incident detection and response mechanisms for financial systems.	• Ensures compliance with the Computer Emergency Response Team (CERT) standards for handling and mitigating security incidents. • This profile focuses on comprehensive scan covering all critical systems and applications. • Key Checks: • Incident Detection: Ensure proper mechanisms are in place for detecting security incidents. • Vulnerability Management: Perform regular vulnerability scans and ensure timely remediation. • Configuration Management: Assess the configurations of systems and applications for compliance. • Access Control: Verify strict access controls and user authentication mechanisms. • Human actions: • Audit Logs: Check for proper logging and monitoring of all access and changes to critical systems. • Incident Response: Evaluate the effectiveness of incident response plans and procedures. • Security Training: Ensure that personnel are trained in incident response and handling. • Reporting: Verify that incidents are properly reported to relevant authorities and stakeholders.

NEW VULNERABILITY SCAN - PROFILES

Profile 29 – COBIT/ITIL Compliance Scan

- Ensures compliance with the Control Objectives for Information and Related Technologies (COBIT) and Information Technology Infrastructure Library (ITIL) standards for IT governance and management.
- This profile focuses on IT governance, risk management, and service management processes.
- Key Checks:
- - Access Controls: Verify proper access controls to critical IT systems.
- - Configuration Management: Ensure secure configurations of IT systems and applications.
- - Compliance Monitoring: Ensure continuous monitoring of compliance with COBIT and ITIL standards.
- Human actions:
- - Change Management: Assess processes for managing changes to IT systems and data.
- - Incident Management: Evaluate the effectiveness of incident detection, response, and resolution processes.
- - Service Management: Check for adherence to ITIL service management best practices.
- Audit Logs: Ensure proper logging and monitoring of IT activities.
- Risk Management: Assess the organization’s risk management practices and documentation.

Profile 30 – DISA STIGs Compliance Scan

- Ensures compliance with the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) for securing Department of Defense (DoD) systems.
- This profile focuses on comprehensive scan of systems and applications for compliance with DISA STIGs.
- Key Checks:
- Access Controls: Verify strict access controls to DoD systems.
- Configuration Management: Assess configurations against DISA STIGs benchmarks.
- Vulnerability Management: Perform regular vulnerability scans and ensure timely remediation.
- Patch Management: Identify and remediate missing security patches.
- Compliance Reporting: Generate reports to demonstrate compliance with DISA STIGs.
- Human actions:
- Audit Logs: Ensure proper logging and monitoring of all access and changes to DoD systems.
- Incident Response: Evaluate the effectiveness of incident detection and response plans.
- Security Training: Ensure personnel are trained in DoD security requirements.

NEW VULNERABILITY SCAN - PROFILES

Profile 31 – FDCC Compliance Scan	Profile 32 – NSA Compliance Scan
• Ensures compliance with the Federal Desktop Core Configuration (FDCC) standards for securing federal desktops and laptops. • This profile focuses on desktop and laptop configurations within federal agencies. • Key Checks: • Configuration Management: Assess configurations of desktops and laptops against FDCC benchmarks. • Access Controls: Verify proper access controls to federal desktops and laptops. • Vulnerability Management: Perform regular vulnerability scans and ensure timely remediation. • Patch Management: Identify and remediate missing security patches. • Compliance Reporting: Generate reports to demonstrate compliance with FDCC standards. • Human actions: • Audit Logs: Ensure proper logging and monitoring of all access and changes to federal systems. • Incident Response: Evaluate the effectiveness of incident detection and response plans. • Data Encryption: Ensure encryption of sensitive data on desktops and laptops.	• Ensures compliance with National Security Agency (NSA) guidelines for securing national security systems. • This profile focuses on comprehensive scan of systems and applications for compliance with NSA guidelines. • Key Checks: • Access Controls: Verify strict access controls to national security systems. • Configuration Management: Assess configurations against NSA guidelines. • Vulnerability Management: Perform regular vulnerability scans and ensure timely remediation. • Patch Management: Identify and remediate missing security patches. • Data Encryption: Ensure encryption of sensitive national security data. • Compliance Reporting: Generate reports to demonstrate compliance with NSA guidelines. • Human actions: • Audit Logs: Ensure proper logging and monitoring of all access and changes to national security systems. • Incident Response: Evaluate the effectiveness of incident detection and response plans.

NEW VULNERABILITY SCAN - PROFILES

Profile 33 – NIS2 Compliance Scan

- Ensures compliance with the Network and Information Security (NIS2) Directive, a regulation enacted by the European Union.
- NIS2 compliance refers to adherence to the Network and Information Security (NIS2) Directive.
- Key Checks:
- Risk Management & Vulnerability Detection - Scans for software vulnerabilities, misconfigurations, outdated software, and unpatched systems that may expose the network to threats.
- Incident Detection & Response - Checks if IDS/IPS systems are correctly configured and operational. Monitors whether logs and alerts are generated during simulated attacks or suspicious activities.
- Network Security & Firewall Configuration - Scans firewall rules, open ports, and network misconfigurations that could expose your network to external attacks, such as unauthorized access or malware injection.
- Access Control & Authentication - Identifies weak passwords, default credentials, and verifies if Multi-Factor Authentication (MFA) is enforced where possible.
- Encryption & Data Protection - Checks for weak encryption (e.g., outdated TLS versions) and ensures that SSL/TLS certificates are correctly configured. Detects whether sensitive data is being transmitted unencrypted.
- Patch Management & System Updates - Scans for outdated systems.

Profile 34 – CRA Compliance Scan

- 1. Vulnerability Management & CVE Detection - Scans systems and applications for known vulnerabilities (CVEs), outdated versions, and missing security patches that could compromise product security.
- 2. Secure Configuration & Hardening - Identifies misconfigurations, default credentials, and weak security settings in servers, IoT devices, and applications that may violate CRA "secure by default" principles.
- 3. Encryption & Secure Communications - Checks TLS/SSL configurations, weak cipher suites, expired certificates, and insecure communication channels to ensure protection of data in transit.
- 4. Authentication & Access Control - Detects weak or default passwords, missing Multi-Factor Authentication (MFA), and improper access control mechanisms.
- 5. Update & Patch Delivery Mechanisms - Verifies whether systems expose insecure update services, checks if secure update protocols (HTTPS, signed packages) are enforced, and identifies outdated software versions.
- 6. Logging & Monitoring - Confirms that systems generate security logs for critical events and checks whether logging functions are active and accessible for monitoring.
- 7. Exposure of Network Services - Scans for unnecessary open ports and services that may increase the attack surface, particularly in connected devices or embedded systems.
- 8. Default & Third-Party Components - Detects vulnerable open-source or third-party components embedded in software and firmware, ensuring compliance with CRA obligations to manage supply chain risks.
- 9. Web Application Security - Performs OWASP-aligned checks for SQL injection, XSS, CSRF, and insecure direct object references in web-enabled products.
- 10. Denial of Service Weaknesses - Identifies network or application misconfigurations that could be exploited for DoS/DDoS attacks against products or services.