Check How Effective Your CIS Critical Controls Are

Updated on May 18, 2021, the updated version of the recommended actions and practices described in CIS 18 Critical Security Controls was published. These 18 controls are a prioritized set of actions to protect your organization and data from known cyber-attack vectors.
This prioritization helps your organization work toward achieving effective cyber hygiene and is a cornerstone of most compliance requirements.
Once implemented, continuously validating that the implementation is properly configured and identifying security posture drift in real-time is crucial to maintain cyber-hygiene across deployments and protect your organization against emerging threats.
Cymulate's Extended Security Posture Validation (XSPM) platform provides validation modules and vectors that continuously verify the efficacy of your organization's cyber defenses.
This table lists the 18 CIS Security Controls in regard to the Cymulate's relevant module or vector.

	CIS Critical Security Controls Description	Cymulate Validation Solution
01	**Inventory and Control of Enterprise Assets** Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.	**Attack Surface Management (ASM)** Cymulate's ASM vector emulates cyber attackers recon attack phase by scouring the Internet for exposed assets, from stolen credentials on the Darknet to shadow IT. Any asset discovered by ASM that is not listed by the enterprise's asset management program indicates the presence of an exploitable flaw in the asset management. This enables enterprises to immediately include discovered assets in their asset management directory and reconfigure their asset management program to improve its effectiveness.
02	**Inventory and Control of Software Assets** Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	**Lateral Movement (Hopper)** The Lateral Movement (Hopper) vector challenges your internal network configuration and segmentation policies against different techniques and methods used by attackers to propagate within the network and control additional systems. The vector simulates an adversary that has control over a single workstation and attempts to move laterally within the organization. The assessment's result is a visualization of all the endpoints that the assessment was able to reach with a detailed description of the methods used for every hop. The assessment identifies infrastructure weaknesses, network misconfigurations, and weak passwords, and provides guidance to remediate them.

	CIS Critical Security Controls Description	Cymulate Validation Solution
03	**Data Protection** Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.	**Data Loss Prevention (DLP)** Cymulate's DLP vector emulates attackers' attempts to access, extract, or otherwise interact with privileged data. The automatically generated reports identify security gaps and provide actionable remediation recommendations to optimize security controls configuration and optimize security.
04	**Secure Configuration of Enterprise Assets and Software** Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).	**Breach and Attack Simulation (BAS)** Cymulate's BAS module simulates thousands of attack scenarios and correlates them to security controls findings through API integrations and provides actionable detection and mitigation guidance.
05	**Account Management** Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.	**Breach and Attack Simulation (BAS)** Cymulate's BAS module operationalizes MITRE ATT&CK TTPs to continuously validate that security controls are efficiently configured, or identifies security gaps and provide actionable remediation guidance.
06	**Access Control Management** Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.	**Breach and Attack Simulation (BAS)** Cymulate's BAS module operationalizes MITRE ATT&CK TTPs to continuously validate that security controls are efficiently configured, or identifies security gaps and provide actionable remediation guidance.
07	**Continuous Vulnerability Management** Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.	**Attack–Based Vulnerability Management (ABVM)** Cymulate's ABVM integrates with leading third party vulnerability management solutions and cross-references information on vulnerabilities provided by these vendors, along with the analysis from Cymulate's ABVM, and offers a practical view of compensatory security controls over unpatched vulnerabilities in the network. Cymulate's ABVM enables organizations to accurately prioritize remediation and patching or reconfiguration of compensating security controls.

	CIS Critical Security Controls Description	Cymulate Validation Solution
08	**Audit Log Management** Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack	**N/A**
09	**Email and Web Browser Protections** Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.	**BAS – Email and Web Gateways** Cymulate's BAS email and web gateway s test your email and web gateway security controls efficacy by launching a comprehensive array of threats concealed in thousands of emails to uncover security gaps and simulating employees accessing malicious websites.
10	**Malware Defenses** Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.	**Breach and Attack Simulation (BAS)** Cymulate's BAS module operationalizes MITRE ATT&CK TTPs to continuously validate that security controls are efficiently configured, or identifies security gaps and provide actionable remediation guidance. The Immediate Threat Intelligence vector goes beyond CIS recommendations by validating your infrastructure resilience even to emerging threats.
11	**Data Recovery** Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.	**N/A**
12	**Network Infrastructure Management** Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.	**Lateral Movement (Hopper)** The Lateral Movement (Hopper) vector challenges your internal network configuration and segmentation policies against different techniques and methods used by attackers to propagate within the network and control additional systems. The vector simulates an adversary that has control over a single workstation and attempts to move laterally within the organization. The assessment's result is a visualization of all the endpoints that the assessment was able to reach with a detailed description of the methods used for every hop. The assessment identifies infrastructure weaknesses, network misconfigurations, and weak passwords, and provides guidance to remediate them.

	CIS Critical Security Controls Description	Cymulate Validation Solution
13	**Network Monitoring and Defense** Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.	**Lateral Movement (Hopper)** The Lateral Movement (Hopper) vector challenges your internal network configuration and segmentation policies against different techniques and methods used by attackers to propagate within the network and control additional systems. The vector simulates an adversary that has control over a single workstation and attempts to move laterally within the organization. The assessment's result is a visualization of all the endpoints that the assessment was able to reach with a detailed description of the methods used for every hop. The assessment identifies infrastructure weaknesses, network misconfigurations, and weak passwords, and provides guidance to remediate them.
14	**Security Awareness and Skills Training** Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.	**Phishing Awareness** Cymulate's Phishing Awareness vector enables you to evaluate employee security awareness. It provides all the resources required to create, customize, launch and measure phishing campaigns. Each campaign is tracked for 5 different actions (opening, clicking, entering credentials, reporting, and completing a quiz) providing the full picture of employee security awareness levels, enabling the organization to focus on those that require more education and monitoring than others.
15	**Service Provider Management** Develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.	**Extended Security Posture Management (XSPM)** Enterprises can leverage Cymulate's capabilities to test service provider SLAs and assess the quality of security services they are getting, based on the MSSP security controls & policy scoring.

	CIS Critical Security Controls Description	Cymulate Validation Solution
16	**Application Software Security** Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.	**Web Application Firewall (WAF)** Cymulate's Web Application Firewall (WAF) vector enables you to test and optimize your web security controls. The WAF vector first identifies all means of data import available on the target domain and then challenges the WAF against thousands of attacks, including OWASP top payloads, command injection, and file inclusion attacks to assess the integrity of the WAF configuration and its blocking effectiveness.
17	**Incident Response Management** Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.	**Extended Security Posture Management (XSPM)** Cymulate allows running internal and managed soc validation and tabletop exercises to assess detection rates as well as escalation and response times and processes.
18	**Penetration Testing** Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.	**Extended Security Posture Management (XSPM)** Cymulate's XSPM platform includes all the elements described above and more to go way beyond basic periodic penetration testing by continuously validating your security posture

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness. **Measuring your cybersecurity performance is fundamental towards creating a more secure organization!**

Contact us for a live demo, or get started with a free trial

Start Your Demo

Headquarters: Maze St 3, Tel Aviv 6578931, Israel | +972 3 9030732 | info@cymulate.com