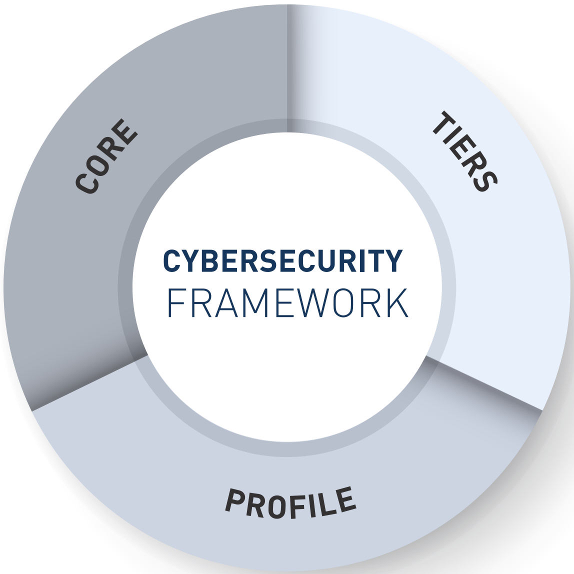
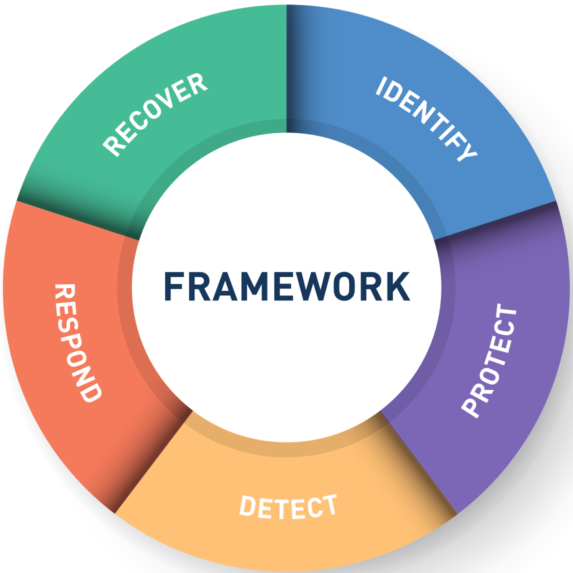
Cymulate
Breach & Attack Simulation

Cymulate and the NIST Cyber Security Framework

The National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) sets guidelines to strengthen cybersecurity for organizations that engage in elements of the critical infrastructure of the United States. Although CSF came about as the result of U.S President issued Executive Order (EO) 13636 it is now being used extensively in the U.S[1] and internationally in both private and public sectors.

CSF is comprised of three main components. The key component is the Framework Core which is a set of desired cybersecurity activities and outcomes. The second component is the Framework Implementation Tiers. This is a qualitative measure of organizational cybersecurity risk management practices on a scale of 1-4. Framework Profiles are the third component. These align an organization's business objectives, risk appetite and industry specific regulations and best practices against the desired outcomes of the Framework Core.





The Framework Core is comprised of five functions, they are:

- **IDENTIFY**
What processes and assets need protection.
- **PROTECT**
What safeguards are available.
- **DETECT**
What techniques can identify incidents.
- **RESPOND**
What techniques can contain impacts of incidents.
- **RECOVER**
What techniques can restore capabilities.

[1] Federal agencies are obliged to apply the framework to their information systems.
Contractors that do business with the federal government must also comply with the NIST Cybersecurity Framework (CSF).

The five functions of the Framework Core are broken down into 23 categories and 108 subcategories. These describe the “what” of a cybersecurity practice or technique. The “how” or “how much” is provided through Informative References. These are detailed technical references that are meant to provide organizations with a starting point for implementing practices to achieve the Framework's desired outcomes described in the associated Subcategory. These include:

- NIST SP 800-53 Rev. 4
- ISO/IEC 27001:2013
- COBIT 5
- CIS CSC
- ISA 62443-2-1:2009
- ISA 62443-3-3:2013

Additional Informative References can be found in the Online Informative Reference Catalog. This program was setup to provide organizations a more robust set of tools to achieve Framework Core outcomes.

Cymulate security validation enables companies to verify and support ongoing compliance to relevant CSF informative references and therefore to CSF. Not all CSF subcategories are relevant, these have been omitted for the sake of brevity. Technical controls will map directly and indirectly to Cymulate applicable functions and capabilities.
For procedural and organizational controls, the Cymulate platform provides a supporting role.

PCI DSS informative references were added by PCI SSC [2] and denotes PCI DSS v3.2.1 requirements that relate to NIST Cybersecurity Framework outcome. The other references were copied directly from the NIST Cybersecurity "Framework V1.1 Core.

[2] Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1 JULY 2019

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
IDENTIFY			
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 PCI DSS v3.2.1 6.1, 11.2, 11.3, 12.2	Cymulate integrations with vulnerability scanners supports this control by alerting on known vulnerable devices. Additionally, Cymulate correlates CVE's to immediate threats and attacks to identify exploitable assets and their degree of risk.
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	• CIS CSC 4 • COBIT 5 BAI08.01 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.6.1.4 • NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 • PCI DSS v3.2.1 6.1	Cymulate Immediate Threats module supports this control by enabling to test the latest threats found "in the wild" and provide all their relevant Indicators of Compromise.
	ID.RA-3: Threats, both internal and external, are identified and documented	• CIS CSC 4 • COBIT 5 BAI08.01 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.6.1.4 • NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 • PCI DSS v3.2.1 6.1	Cymulate Immediate Threats module supports this control by enabling to test the latest threats found "in the wild" and provide all their relevant Indicators of Compromise.
	ID.RA-4: Potential business impacts and likelihoods are identified	• CIS CSC 4 • COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14 • PCI DSS v3.2.1 6.1	Cymulate security validation is a critical component in the overall process of defining the business impact of cybersecurity risks. Every assessment result in a risk score of any given security control based on threat impact and likelihood. Additionally, the Lateral Movement vector enables companies to assess the likelihood of a hacker successfully gaining access to business impacting assets after achieving an initial foothold.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• CIS CSC 4 • COBIT 5 APO12.02 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 • PCI DSS v3.2.1 12.2	Cymulate security validations assigns a risk score to threats based on the results of testing an organizations security controls effectiveness against them. The score is based on the outcome of the test, in addition to the likelihood and impact of the threats used in the testing.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
IDENTIFY			
	ID.RA-6: Risk responses are identified and prioritized	• CIS CSC 4 • COBIT 5 APO12.05, APO13.02 • ISO/IEC 27001:2013 Clause 6.1.3 • NIST SP 800-53 Rev. 4 PM-4, PM-9 • PCI DSS v3.2.1 12.10.1	Cymulate platform is a critical component in the overall organization's risk management program. It enables an organization to identify and prioritize risk, and to test the effectiveness of the response plans to those risks.
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	• CIS CSC 4 • COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 • ISA 62443-2-1:2009 4.3.4.2 • NIST SP 800-53 Rev. 4 PM-9 • PCI DSS v3.2.1 12.2	The Cymulate platform supports Organizational Risk Management processes. By using the Cymulate platform, an organization has taken into consideration the need to assess its exposure and manage findings. Executive reports help to create stakeholder buy-in by showing the gaps and weaknesses within an environment.
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.2.6.5 • ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 • NIST SP 800-53 Rev. 4 PM-9 • PCI DSS v3.2.1 12.2	Weaknesses and gaps found during the Cymulate assessments provide full descriptions of both the potential impact and the level of effort required for remediation are clearly spelled out. This allows for a true measure of risk tolerance to be gained, by allowing all parties to determine the actual impact of the threats in question. The platform enables companies to set a risk tolerance score as a comparative baseline for each vector.
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.2.6.5 • ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 • NIST SP 800-53 Rev. 4 PM-9 • PCI DSS v3.2.1 12.2	Weaknesses and gaps found during the Cymulate assessments provide full descriptions of both the potential impact and the level of effort required for remediation are clearly spelled out. This allows for a true measure of risk tolerance to be gained, by allowing all parties to determine the actual impact of the threats in question. The platform enables companies to set a risk tolerance score as a comparative baseline for each vector.
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	• CIS CSC: 4.8 • COBIT 5: APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 • ISA 62443-2-1:2009: 4.3.4.2 • ISO/IEC 27001:2013: A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 • NIST SP 800-53: SA-9, SA-12, PM-9 • PCI DSS v3.2.1 12.2, 12.8, 12.9	Cymulate security validation can be performed on supply-chain partners as an integral part of an organizations risk management process. Licensing models are available for an organization to perform security assessments against internal and/or external partner systems providing a security score to measure and track the risk they pose. Internal assessments require the partner to agree to the process.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
IDENTIFY			
	ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	• CIS CSC 4 • COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 • ISA 62443-2-1:2009 4.3.4.2 • NIST SP 800-53 Rev. 4 PM-9 • PCI DSS v3.2.1 12.2	The Cymulate platform supports Organizational Risk Management processes. By using the Cymulate platform, an organization has taken into consideration the need to assess its exposure and manage findings. Executive reports help to create stakeholder buy-in by showing the gaps and weaknesses within an environment.
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	• COBIT 5: APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 • ISA 62443-2-1:2009: 4.3.2.6.7 • ISA 62443-3-3:2013: SR 6.1 • ISO/IEC 27001:2013: A.15.2.1, A.15.2.2 • NIST SP 800-53: AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12 • PCI DSS v3.2.1 12.8	Cymulate automated security validation enables organizations to schedule 3rd party assessments, to routinely assess their security performance. Security scoring enables the organization to track 3rd party performance over time to ensure continuous validation.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
PROTECT			
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	• CIS CSC 1.5, 15, 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 • PCI DSS v3.2.1 2.1, 8.1, 8.2, 8.5, 8.6, 12.3	The Cymulate Recon vector enables organizations to determine commonly used/accessible employee and contractor credentials. Combined with the Lateral Movement Vector, use of these data sources can ensure that proper credential handling is being enforced. Legacy connectivity which bypasses MFA can be discovered, and overall interconnectivity of segregated networks can be confirmed.
	PR.AC-3: Remote access is managed	• CIS CSC 12 • COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6 • ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20 • PCI DSS v3.2.1 2.3, 8.1.5, 8.3, 8.5.1, 12.3.8, 12.3.9, 12.3.10	Cymulate Lateral Movement assessments can discover inappropriate and/or unexpected access via remote connectivity. The Recon vector can find potentially open areas that could be leveraged for remote access attacks.
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	• CIS CSC 3, 5, 12, 14, 15, 16, 18 • COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.7.3 • ISA 62443-3-3:2013 SR 2.1 • ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 • NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 • PCI DSS v3.2.1 6.4.2, 7.1, 7.2, 8.7, 9.3	Cymulate Recon and Lateral Movement assessments can test multiple segregated networks to validate the effectiveness of segmentation policy enforcement points and to ensure that cross-system privileges do not permit over-privileged access.
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	• CIS CSC 9, 14, 15, 18 • COBIT 5 DSS01.05, DSS05.02 • ISA 62443-2-1:2009 4.3.3.4 • ISA 62443-3-3:2013 SR 3.1, SR 3.8 • ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7 • PCI DSS v3.2.1 1.1, 1.2, 1.3, 2.2, 6.2, 10.8, 11.3	The Cymulate Lateral Movement vector enables an organization to test and ensure that network segregations and segmentation policies are effectively enforced. It discovers infrastructure weaknesses that enable clandestine network propagation, in addition to providing remediation guidance.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
PROTECT			
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	• CIS CSC 1, 12, 15, 16 • COBIT 5: DSS05.04, DSS05.10, DSS06.10 • ISA 62443-2-1:2009: 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 • ISA 62443-3-3:2013: SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 ISO/IEC 27001:2013 A.9.2.1, • ISO/IEC 27001:2013: A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 • NIST SP 800-53: Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 • PCI DSS v3.2.1 8.2, 8.3	The Cymulate Lateral Movement (LM) vector challenges authentication controls to identify weak or inappropriate authentication instances per asset. It can also ensure that legacy login methods that can bypass MFA are not active or allowed. Furthermore, the Recon module discovers openly-available credentials (such as from 3rd-party breach and leak activity) that can be validated by the Lateral Movement vector.
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	• CIS CSC 17, 18 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 • NIST SP 800-53 Rev. 4 AT-2, PM-13 • PCI DSS v3.2.1 6.7, 7.3, 8.4, 9.9.3, 12.4, 12.6	The Cymulate Phishing Awareness vector enables companies to validate the effectiveness of security awareness training and to identify users that require additional education.
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	PR.DS-1: Data-at-rest is protected.	• CIS CSC 13, 14 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 • ISA 62443-3-3:2013 SR 3.4, SR 4.1 • ISO/IEC 27001:2013 A.8.2.3 • NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28 • PCI DSS v3.2.1 3 (all), 8.2.1	Multiple modules can determine if unauthorized access to data at rest is possible. The Cymulate Data Exfiltration vector specifically attempts to move data which should be considered "protected" via multiple methodologies known to be used by threat actors.
	PR.DS-2: Data-in-transit is protected.	• CIS CSC 13, 14 • COBIT 5 APO01.06, DSS05.02, DSS06.06 • ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12 • PCI DSS v3.2.1 4 (all), 8.2.1	Multiple modules can determine if unauthorized access to data is possible. Cymulate assessments validate that passwords, tokens and other sensitive forms of data are not easily intercepted and used.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
PROTECT			
	PR.DS-5: Protections against data leaks are implemented.	• CIS CSC 13 • COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 • ISA 62443-3-3:2013 SR 5.2 • ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 • PCI DSS v3.2.1 10.6	The Cymulate Data Exfiltration vector enables organizations to assess the effectiveness of its protections against data leaks, identify gaps and provide remediation guidance. The Red Team Module can test protections against malicious remote access methodologies and other forms of inappropriate communication pathways.
	PR.DS-7: The development and testing environment(s) are separate from the production environment.	• CIS CSC 18, 20 • COBIT 5 BAI03.08, BAI07.04 • ISO/IEC 27001:2013 A.12.1.4 • NIST SP 800-53 Rev. 4 CM-2 • PCI DSS v3.2.1 6.4.1, 6.4.2	The Cymulate Lateral Movement vector enables organizations to validate network segregation to ensure that non-production and production systems are indeed separate. The Data Exfiltration vector can ensure that production data cannot be transferred to or from the test environment.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	• CIS CSC 3, 9, 11 • COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 • PCI DSS v3.2.1 1.2, 2.2	Cymulate security validation enables individual security control and defense-in-depth testing to help define an organizations baseline, assist in remediation to reach baseline, and ensure that systems remain concurrent with the baseline. It can also determine if violations of least functionality are possible by testing multiple intrusion methods that rely on systems and software which should not be present.
	PR.IP-3: Configuration change control processes are in place	• CIS CSC 3, 11 • COBIT 5 BAI01.06, BAI06.01, • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10 • PCI DSS v3.2.1 6.4	Cymulate security validation can be an integral component of an organization's configuration change control process to validate security effectiveness after changes in the IT architecture and security controls. Cymulate security validation is performed on the production network and can be scheduled or ad-hoc to discover and help rectify alterations to the environment that have not gone through proper change control, misconfigurations, and human error.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
PROTECT			
	PR.IP-7: Protection processes are improved	• COBIT 5 APO11.06, APO12.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 • PCI DSS v3.2.1 10.8, 12.10.6, 12.11	Cymulate continuous security validation enables organizations to continuously improve their protection processes by revealing new security gaps as they become known to the cybersecurity world.
	PR.IP-8: Effectiveness of protection technologies is shared	• COBIT 5 BAI08.04, DSS03.04 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4	Cymulate assessment results and reports can be automatically provided in various formats and detail to senior management and other stakeholders
	PR.IP-10: Response and recovery plans are tested	• CIS CSC 19, 20 • COBIT 5 DSS04.04 • ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.17.1.3 • NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14 • PCI DSS v3.2.1 12.10.2	Cymulate testing enables organizations to launch controlled attacks to safely test response and recovery plans. Security situations can be executed to exercise response processes, subsequent staff and system activity to counter and recovery from these situations can be evaluated.
	PR.IP-12: A vulnerability management plan is developed and implemented	• CIS CSC 4, 18, 20 • COBIT 5 BAI03.10, DSS05.01, DSS05.02 • ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 • NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 • PCI DSS v3.2.1 6.1, 6.2, 6.5, 11.2	Vulnerability scans can be combined with Cymulate simulations and assessments to prioritize vulnerability management and confirm adherence to the vulnerability management plan
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• CIS CSC 1, 3, 5, 6, 14, 15, 16 • COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 • ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • NIST SP 800-53 Rev. 4 AU Family • PCI DSS v3.2.1 10.1, 10.2, 10.3, 10.4, 10.5, 10.6.1, 10.6.2, 10.7	Audit logs are part of the Cymulate platform providing organizations the capability to monitor all actions performed within the platform (user management, access, performance, etc.)

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
PROTECT			
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	• CIS CSC 3, 11, 14 • COBIT 5 DSS05.02, DSS05.05, DSS06.06 • ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • ISO/IEC 27001:2013 A.9.1.2 • NIST SP 800-53 Rev. 4 AC-3, CM-7 • PCI DSS v3.2.1 2.2, 7.1, 7.2, 9.3	Data Exfiltration, Lateral Movement, and Endpoint Security modules can be used to test that least functionality is being adhered to. The Cymulate platform itself allows for different roles and access for users that have need to directly interact with the Cymulate platform.
	PR.PT-4: Communications and control networks are protected	• CIS CSC 8, 12, 15 • COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43 • PCI DSS v3.2.1 1 (all), 2 (all)	Cymulate validates the effectiveness of protections for communications and control networks through breach and attack simulations.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
DETECT			
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-2: Detected events are analyzed to understand attack targets and methods	• CIS CSC 3, 6, 13, 15 • COBIT 5 DSS05.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4 • PCI DSS v3.2.1 10.6 (all), 12.5.2	Cymulate permits testing of specific defined events to test the ability of security staff to identify threats-in-progress and analyze threats after the fact.
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors	• CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 • COBIT 5 BAI08.02 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 • PCI DSS v3.2.1 10.1, 12.10.5, 10.6	Cymulate Platform can be integrated via API with SIEM and other solutions to ensure that simulations of security events are properly recorded in reporting and tracking systems; and that correct event alarms and notifications are working as intended.
	DE.AE-4: Impact of events is determined	• CIS CSC 4, 6 • COBIT 5 APO12.06, DSS03.01 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4 • PCI DSS v3.2.1 10.6.3, 12.5.2	Cymulate can assist in learning the impact of various security events by providing simulations of these events in a safe, repeatable methodology.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	• CIS CSC 7, 8, 12, 13, 15, 16 • COBIT 5 DSS01.03, DSS03.05, DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 • PCI DSS v3.2.1 10.6.1, 10.6.2, 11.4	Cymulate integrates via API with SIEM and EDR solutions to ensure that simulations of security events are properly detected and recorded in reporting and tracking systems; and that correct event alarms and notifications are working as intended.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• CIS CSC 5, 7, 14, 16 • COBIT 5 DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 • NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 • PCI DSS v3.2.1 9.1.1	Cymulate integrates via API with SIEM and EDR solutions to ensure that simulations of security events are properly detected and recorded in reporting and tracking systems; and that correct event alarms and notifications are working as intended.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
DETECT			
	DE.CM-4: Malicious code is detected	• CIS CSC 4, 7, 8, 12 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.3.4.3.8 • ISA 62443-3-3:2013 SR 3.2 • ISO/IEC 27001:2013 A.12.2.1 • NIST SP 800-53 Rev. 4 SI-3, SI-8 • PCI DSS v3.2.1 5 (all)	The Cymulate Endpoint Protection and Red Team Vectors simulate malicious code in order to confirm that monitoring systems and security controls detect this code and handle it appropriately.
	DE.CM-5: Unauthorized mobile code is detected	• CIS CSC 7, 8 • COBIT 5 DSS05.01 • ISA 62443-3-3:2013 SR 2.4 • ISO/IEC 27001:2013 A.12.5.1, A-12.6.2 • NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44 • PCI DSS v3.2.1 5 (all)	The employment of mobile code (Java, JavaScript, ActiveX) within the organization can be tested using the Cymulate platform to make sure no malicious mobile code can bypass deployed security controls.
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	• COBIT 5 APO07.06, APO10.05 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 • PCI DSS v3.2.1 8.1.5, 10.6	Cymulate's Endpoint Security and Red Team Vectors can simulate malicious code in order to confirm that monitoring systems detect this code and handle it appropriately. Lateral Movement simulations can determine if unauthorized parties can move between systems and networks
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	• CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 • COBIT 5 DSS05.02, DSS05.05 • ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 • PCI DSS v3.2.1 10.1, 10.6.1, 11.1, 11.4, 11.5, 12.10.5	Cymulate Lateral Movement, Endpoint Security and Red Team vectors enable and organization to test that the information system and assets are monitored for unauthorized access and connections.
	DE.CM-8: Vulnerability scans are performed	• CIS CSC 4, 20 • COBIT 5 BAI03.10, DSS05.01 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-5 • PCI DSS v3.2.1 11.2	Cymulate RECON assessments detects external vulnerabilities (open object storage, known compromised credentials, etc.). Other Cymulate vectors integrate with Vulnerability Scanners to correlate attack simulations and threat intelligence to prioritize vulnerability findings.
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-3: Detection processes are tested	• COBIT 5 APO13.02, DSS05.02 • ISA 62443-2-1:2009 4.4.3.2 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.14.2.8, A.7.2.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 • PCI DSS v3.2.1 10.6.1, 10.9, 11.2, 11.3, 12.10	The Cymulate platform safely simulates adversarial behavior across all vectors of the attack kill chain to test monitoring and detection processes.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
DETECT			
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-3: Detection processes are tested	• COBIT 5 APO13.02, DSS05.02 • ISA 62443-2-1:2009 4.4.3.2 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.14.2.8, A.7.2.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 • PCI DSS v3.2.1 10.6.1, 10.9, 11.2, 11.3, 12.10	The Cymulate platform safely simulates adversarial behavior across all vectors of the attack kill chain to test monitoring and detection processes.
	DE.DP-4: Event detection information is communicated	• CIS CSC 19 • COBIT 5 APO08.04, APO12.06, DSS02.05 • ISA 62443-2-1:2009 4.3.4.5.9 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.16.1.2, A-16.1.3 • NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 • PCI DSS v3.2.1 12.10	The Cymulate platform safely simulates adversarial behavior across all vectors of the attack kill chain to test monitoring and detection processes, including the communications of a detected event.
	DE.DP-5: Detection processes are continuously improved	• COBIT 5 APO11.06, APO12.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 • PCI DSS v3.2.1 12.10.6	The Cymulate Platform performs automated testing of all vectors at regular intervals. Through integrations with EDRs and SIEM systems this allows for refinement and improvement of detection processes over time.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
RESPOND			
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• CIS CSC 19 • COBIT 5 BAI08.04 • ISA 62443-2-1:2009 4.3.4.5.5 • ISO/IEC 27001:2013 Clause 7.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • PCI DSS v3.2.1 12.10.1	The Cymulate platform supports this control by enabling to test response plans and level their coordination. This includes Blue team \ Red Team drills across the full attack kill chain.
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities	RS.AN-1: Notifications from detection systems are investigated	• CIS CSC 4, 6, 8, 19 • COBIT 5 DSS02.04, DSS02.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 • PCI DSS v3.2.1 10.6.3, 11.5.1, 12.5.2, 12.10.5	Cymulate assessments can ensure that security controls are providing thorough and complete information which can be used should an actual incursion take place.
	RS.AN-2: The impact of the incident is understood	• COBIT 5 DSS02.02 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4 • PCI DSS v3.2.1 10.6.3, 11.5.1, 12.5.2	Cymulate assessments can ensure that security controls are providing thorough and complete information which can be used should an actual incursion take place. Cymulate assists in learning the impact of various security events by providing simulations of these events in a safe, repeatable methodology.
	RS.AN-3: Forensics are performed	• COBIT 5 APO12.06, DSS03.02, DSS05.07 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • ISO/IEC 27001:2013 A.16.1.7 • NIST SP 800-53 Rev. 4 AU-7, IR-4 • PCI DSS v3.2.1 11.5.1, 12.5.2	Cymulate supports this control by enabling the SOC and security experts to simulate adversarial behavior for analysis and forensics. Cymulate can re-create threat activity to help determine what paths were taken and/or what actions were successful to aid the forensics process.
	RS.AN-4: Incidents are categorized consistent with response plans	• CIS CSC 4, 19 • COBIT 5 DSS02.02 • ISA 62443-2-1:2009 4.3.4.5.6 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 • PCI DSS v3.2.1 11.5.1, 12.5.2	Cymulate simulates multiple forms of incidents safely, allowing processes for categorization and response to be developed and tested in the absence of actual threat activity.
	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the	• CIS CSC 4, 19 • COBIT 5 EDM03.02, DSS05.07 • NIST 800-53 Rev 4 SI-5, PM-15 • PCI DSS v3.2.1 6.1, 6.2	As a source of security gaps and weaknesses Cymulate security assessments and results is inclusive to this process - to receive, analyze and respond to vulnerabilities it discovers.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
RESPOND			
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1: Incidents are contained	• CIS CSC 19 • COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.6 • ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 • ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4 • PCI DSS v3.2.1 11.5.1, 12.5.2	Cymulate assessments can ensure that security controls are providing thorough and complete information to contain an actual incursion. This can be tested using all the modules in the Cymulate platform as part of a Blue Team \ Red Team drill
	RS.MI-2: Incidents are mitigated	• CIS CSC 4, 19 • COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 • ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4 • PCI DSS v3.2.1 11.5.1, 12.5.2	Cymulate assessments can ensure that security controls are providing thorough and complete information to mitigate an actual incursion. This can be tested using all the modules in the Cymulate platform as part of a Blue Team \ Red Team drill
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• CIS CSC 4 • COBIT 5 APO12.06 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 • PCI DSS v3.2.1 6.1, 6.2, 10.6.3, 11.2, 11.5.1, 12.5.2, 12.10	Cymulate Immediate Threats module incorporates threat intelligence to identify new security gaps, assess their risk and provide mitigation guidance. Test results are documented in the platform and can be exported to other repositories.
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	• COBIT 5 BAI01.13 • ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6, Clause 10 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • PCI DSS v3.2.1 12.10.6	Response plans can be tested by controlled use of simulate threats through Cymulate Vectors. This allows for the Blue Team members to go through the process of response, without the risk of destruction or disruption an actual attack would cause.
	RS.IM-2: Response strategies are updated	• COBIT 5 BAI01.13, DSS04.08 • ISO/IEC 27001:2013 A.16.1.6, Clause 10 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • PCI DSS v3.2.112.10.6	Response plans can be tested by controlled use of simulate threats through Cymulate Vectors. This allows for the Blue Team members to go through the process of response, without the risk of destruction or disruption an actual attack would cause.

NIST CSF V1.1			Cymulate
Function / Category	Subcategory	Informative References	Applicable functions and capabilities
RECOVER			
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	• CIS CSC 10 • COBIT 5 APO12.06, DSS02.05, DSS03.04 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 • PCI DSS v3.2.1 12.10.6	Recovery plans can be tested by controlled use of simulated threats available in for each of the vectors in the platform. This allows for the Blue and Red Teams to exercise the process of recovery; without the risk of destruction or disruption an actual attack would cause.
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	• COBIT 5 APO12.06, BAI05.07, DSS04.08 • ISA 62443-2-1:2009 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6, Clause 10 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • PCI DSS v3.2.1 12.10.6	Recovery plans can be tested by controlled use of simulated threat scenarios available in the platform. These scenarios are repeatable to validate the effectiveness of the recovery actions and lessons learnt.
	RC.IM-2: Recovery strategies are updated	• COBIT 5 APO12.06, BAI07.08 • ISO/IEC 27001:2013 A.16.1.6, Clause 10 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • PCI DSS v3.2.1 12.10.6	Recovery plans can be tested by controlled use of simulated threat scenarios available in the platform. These scenarios are repeatable to validate the effectiveness of the recovery actions to update recovery strategies.
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	• COBIT 5 APO12.06 • ISO/IEC 27001:2013 Clause 7.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4	Recovery plans can be tested by controlled use of simulated threat scenarios available in the platform and to verify communications procedures.

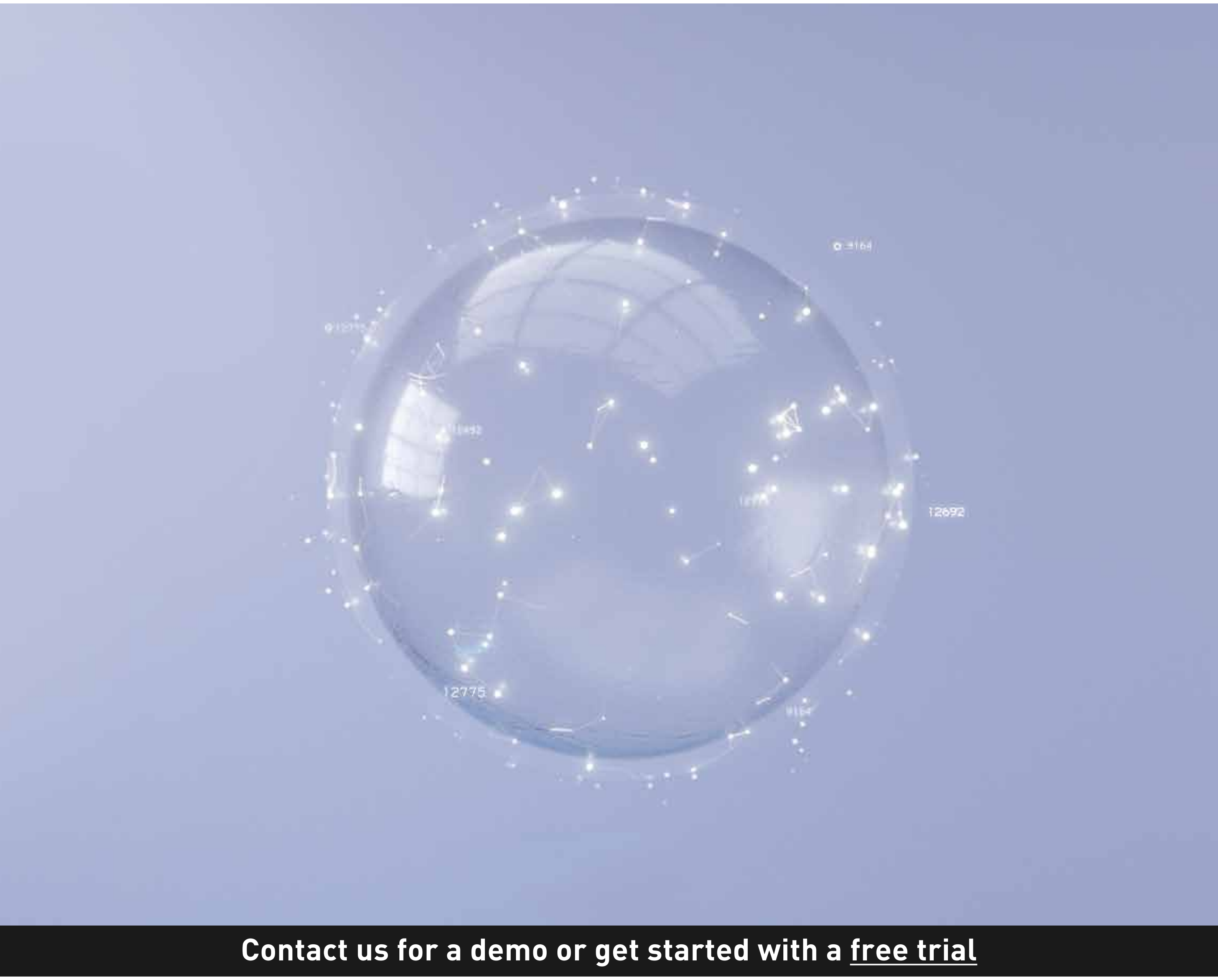
Summary

Automated security validation enables rapid and objective evaluation of new security controls, changes to the IT and cybersecurity architecture and continuous validation after deployment to new threats and hacking tactics and techniques.

Cymulate enables security operations to match the pace of changes in the IT architecture and of the evolving threat landscape, and to test and validate the security outcomes of the NIST Cybersecurity Framework.

Who we are

Cymulate SaaS-based continuous security validation makes it simple to measure and improve your security posture across the full attack kill-chain.
Every assessment is scored and includes actionable remediation guidance to mitigate risk and optimize security control effectiveness. Cymulate enables you to take data-driven decisions and manage your security resources efficiently.



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