Complying with NIST 800-53 Revision 5 Standards with XSPM

NIST Special Publication **(SP) 800-53A, Revision 5**, **"Assessing Security and Privacy Controls in Information Systems and Organizations"**, was published on January 25, 2022, and supersedes the previous version. Cymulate XSPM platform is upgraded to guarantee continued compliance with NIST's new standards.

NIST Revision 5 aims to:

- Improve the efficiency of conducting control assessments.
- Provide better traceability between assessment procedures and controls.
- Better support the use of automated tools, continuous monitoring, and ongoing authorization programs.

The requirements for assessments are considerably increased, in terms of efficiency, traceability, and continuousness. NIST considers that "risk assessments are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems."

The Extended Security Posture Management (XSPM) approach is particularly well suited to streamline compliance with the new NIST standards. XSPM platforms implement that approach by automating end-to-end risk assessment, thus challenging, assessing, and optimizing cyber-security posture simply and continuously and equipping security professionals with the visibility to know, control, and remediate their dynamic environment.

How Cymulate XSPM Facilitates Complying with NIST (SP) 800-53A, Revision 5 Standards

Cymulate XSPM's comprehensive continuous security validation approach is ideal to address all the aspects broached in Revision 5, as it covers all the sections of its chapter on procedures as detailed below:

01 **Access Controls:** As a subsection of security controls, those can automatically be validated through regularly running simulated attack scenarios using a BAS (Breach and Attack Simulation) tool. Cymulate BAS solution automatically verifies that all assessment objectives, methods, and objects delineated in NIST Revision 5 are included.

02 **Awareness and Training:** Cymulate built-in scenarios and campaigns templates that can be leveraged by SOC to run Incident Response Training practical exercises. Cymulate Phishing Awareness assessment pinpoints employees in need of additional awareness training, and the security gaps uncovered through the email and web gateway vectors can be used to document awareness campaigns with examples drawn directly from employee's behavior and increase awareness campaigns' relevance.

03 **Audit and Accountability:** Continuous Security Validation performs ongoing audits with detailed reports that increase collaboration between IT security and internal GRC and risk management teams in organizations.

04 **Assessment, Authorization, and Monitoring:** Cymulate XSPM continuously assesses and verifies that authorizations are not flaunted by attempting, through production-safe attacks, to find gaps in the least privileged access policy and leverage these authorization gaps to gain unauthorized access.

05 **Configuration Management:** When integrated with SIEM and SOAR, Cymulate XSPM automatically maps out the misconfiguration and security gaps enabling 'attackers' intrusion and the ensuing attack path. It then provides prescriptive guidance for enhancing configuration management.

06 **Contingency Planning:** The reports of attacks' potential reach and damages yielded by Incident Response Training exercises run with Cymulate attack scenarios and campaigns can be used by SOC and the Board as comprehensive databases on which to create contingency plans.

07 **Identification and Authentication:** Production-safe attacks scenarios and campaigns are designed to take advantage of insufficiently tight identification and authentication policies. Reports list all detected ID or authentication security gaps and include actionable mitigation recommendations.

08 **Incident Response:** As launching production-safe attacks is an integral part of Cymulate XSPM, IR playbooks can be updated with live production information, and setting up a TTE (Tabletop Exercise) requires minimal labor.

09 **Maintenance:** Once a required level of protection for a media is defined, Cymulate can validate that it is applied and enforced across the board and raise an alert if its personnel or roles fail to implement the required procedures.

10 **Media Protection:** Once a required level of protection for a media is defined, Cymulate can validate that it is applied and enforced across the board and raise an alert if its personnel or roles fail to implement the required procedures.

11 **Physical and Environmental Protection:** This is not typically covered by the information security software, including XSPM, and should be complemented by on-site, physical measures.

12 **Planning:** The overarching view of the entire environment's exposure, including the attack surface, provides invaluable information when establishing a list of the people who should be informed of security and policy procedures and can be used to automatically update them of any relevant modification.
The ability to define accurate granular and global baselines reflecting the organization's risk appetite and measure its variance with precise metrics facilitates both planning and monitoring.

13 **Program Management:** The information regarding SIEM and SOAR tools efficacy extracted from Cymulate assessments uncovers overlapping and missing capabilities and provides prescriptive recommendations to optimize the configuration of the available detecting, monitoring, and response solutions.

14 **Personnel Security:** Same remarks as for point 9.

15 **PII (Personally Identifiable Information) Processing and Transparency:** Same remarks as point 8.

16 **Risk Assessment:** Cymulate XSPM provides the highest and most comprehensive level of risk assessment attainable with today's technology.

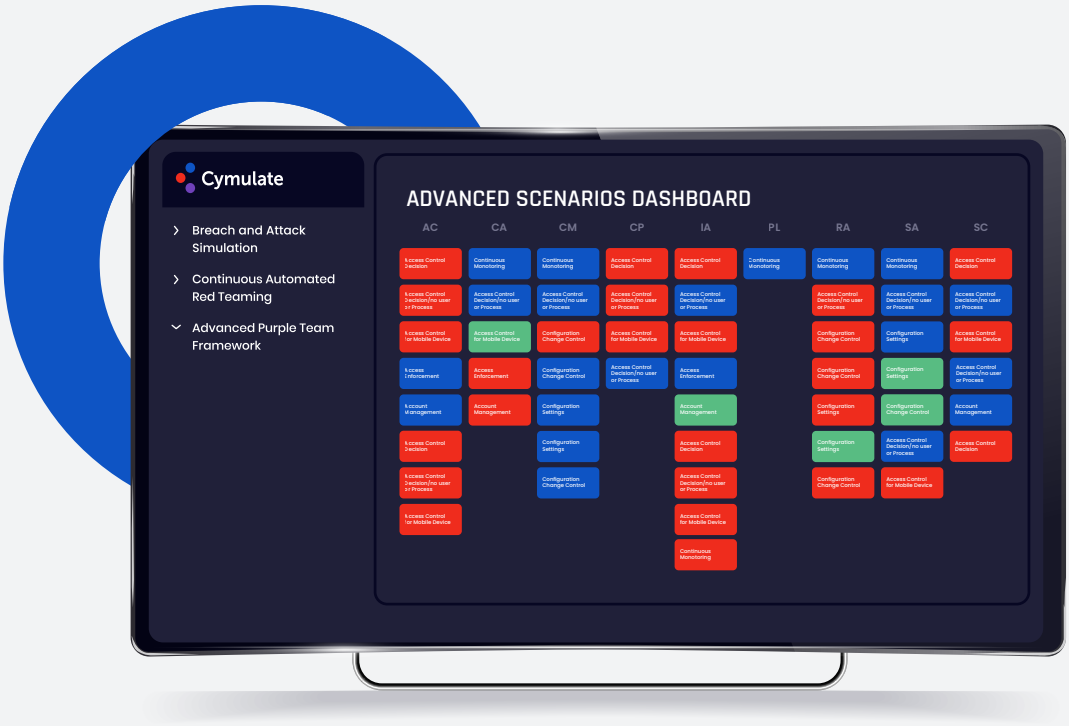
17 **System and Service Acquisition:** Cymulate XSPM can be used to comprehensively and granularly evaluate the risk introduced by granting access to an external service provider or integrating with an external system by testing the impact on the security posture during the trial period.

18 **System and Communication Protection:** As Cymulate XSPM identifies security gaps in the entire network, including those affecting system and communication, protecting those can be achieved by applying the mitigation recommendation provided in XSPM automatically generated reports.

19 **System and Information Integrity:** Same remarks as for point 15.

20 **Supply Chain Risk Management:** Same remark as point 14, except that, instead of testing the impact on security posture during a trial posture, it would require testing the impact of momentarily disconnecting the third party.

Cymulate XSPM comprehensive offensive-based cyber risk assessment is the only continuous security validation platform that covers the entire kill-chain, from intelligence gathering and initial foothold to execution and Command & Control, and network propagation and, of course, action on objectives such as data exfiltration. It can also establish a quantified baseline for security control resilience and security drift monitoring.



Advanced offensive-based assessment tools, such as Cymulate Extended Security Posture Management (XSPM) platform, meet all the NIST increased requirement stringency for risk assessment and are invaluable in achieving compliance quickly, efficiently, and comprehensively.

As a bonus, it provides 360° visibility into the inner working of each cyber-defensive tool, from their ability to improve security controls to their detection and attack-prevention mechanisms and detailed itemized cyber risk quantification.

- Deploys in minutes, SaaS-Based
- Broadest coverage across the full kill-chain
- Vulnerability prioritization guidance
- Granular analytics
- Very latest threats simulated with a few clicks
- Comprehensive assessments out-of-the-box
- Highly customizable red team automation

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 continuously 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 Free Trial

Headquarters: Maze St 3, Tel Aviv 6578931, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632