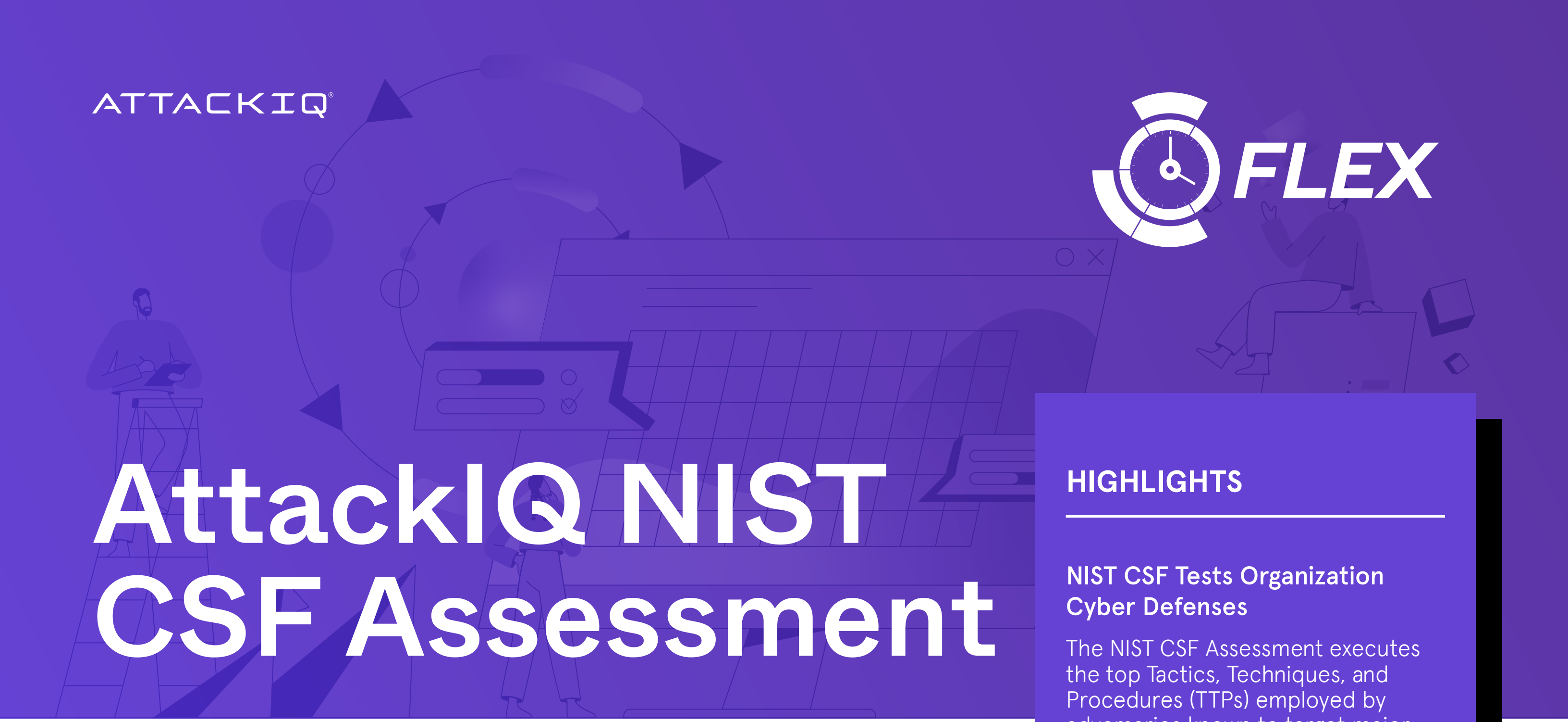


AttackIQ NIST CSF Assessment

The National Institute of Standards and Technology (NIST) CSF Assessment enables any organization to leverage Breach and Attack Simulation (BAS) to rapidly evaluate their cybersecurity posture alignment with the NIST CSF Framework.

Breach and Attack Simulation for NIST CSF

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) offers a voluntary, risk-based approach for organizations of all sizes and industries to systematically improve their cybersecurity posture. NIST CSF provides a flexible framework that can be customized to an organization's specific needs and resources. It emphasizes achieving desired outcomes through continuous improvement. This means organizations can identify their critical assets and potential threats, implement appropriate safeguards to protect them, and establish plans for effectively detecting, responding to, and recovering from cyberattacks. By adopting NIST CSF, organizations can benefit from a reduced risk of cyberattacks, improved incident response capabilities, enhanced compliance with industry regulations, and increased stakeholder confidence in their cybersecurity posture.

Breach and Attack Simulation (BAS) plays a valuable role in supporting NIST CSF through proactive and continuous testing. BAS tools emulate real-world adversaries, allowing organizations to assess the effectiveness of their existing cybersecurity defenses against the latest threats. This aligns perfectly with the NIST CSF's emphasis on continuous improvement. By regularly conducting BAS exercises and analyzing the results, organizations can identify and address security weaknesses before they can be exploited by attackers. This proactive approach strengthens an organization's overall cybersecurity posture and helps them achieve the desired outcomes outlined in the NIST CSF framework.

HIGHLIGHTS

NIST CSF Tests Organization Cyber Defenses

The NIST CSF Assessment executes the top Tactics, Techniques, and Procedures (TTPs) employed by adversaries known to target major organizations worldwide. These TTPs reflect our latest intelligence and threat research into the top methods used by these adversaries.

Comprehensive Reporting Covers Recommendations and Mitigations

The NIST CSF Assessment Report provides comprehensive recommendations and mitigation strategies for any testing scenario that was not prevented. Recommendations are derived from the extensive knowledge base of the AttackIQ research team, enriched with insights from MITRE ATT&CK standards and industry best practices.

MITRE ATT&CK Aligned

The NIST CSF Assessment aligns with MITRE ATT&CK, offering actionable insights in a framework leveraged by cybersecurity practitioners worldwide.

BAS Aligns with the Core Principles of NIST CSF

The cybercriminal landscape is constantly evolving, with attackers developing ever more sophisticated tactics to exploit vulnerabilities in even the most robust security systems. This necessitates a proactive approach to cybersecurity risk management. Breach and Attack Simulation (BAS) aligns with this need, as outlined in the NIST Cybersecurity Framework (CSF), by enabling organizations to identify and address weaknesses before they can be exploited.

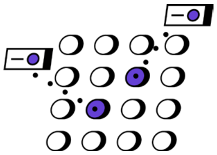
BAS offers a dynamic testing environment that emulates real-world adversary methods. These emulations allow organizations to comprehensively assess their entire security posture – encompassing firewalls, intrusion detection systems, user awareness training, and incident response procedures. By proactively identifying vulnerabilities before malicious actors can exploit them, BAS empowers organizations to prioritize remediation efforts and fortify their overall defenses.

Shifting to a proactive approach to security testing aligns perfectly with the core principles of the NIST Cybersecurity Framework (CSF). This framework emphasizes continuous improvement, achieved through ongoing evaluation of an organization's security posture. BAS fulfills this critical need by providing a repeatable and automated method for assessing the effectiveness of existing security controls. Regular BAS exercises offer valuable insights, allowing organizations to identify security gaps and prioritize remediation efforts. This not only helps achieve the desired outcomes outlined in the NIST CSF (Identify, Protect, Detect, Respond, and Recover) but also demonstrates a commitment to continuous improvement, a cornerstone of the framework. By integrating BAS into their cybersecurity strategy alongside NIST CSF, organizations gain a powerful tool for continuous validation of their security posture and proactive mitigation of cyber risks.

Testing Methodology Using AttackIQ NIST CSF

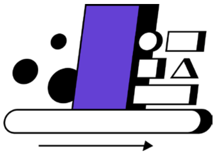
Organizations use AttackIQ to test and audit their security posture to ensure their people, processes and technologies work as expected.

The Business Value of NIST CSF Assessments



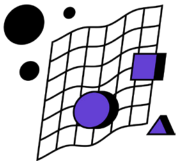
Assess Threat Actors

AttackIQ's advanced adversary emulation software fully emulates cyberattacks and the TTPs employed by real-world adversaries targeting organizations worldwide.



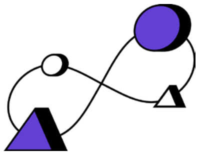
Testing for All Organizations

Organizations of all types can harden their defenses and align with NIST CSF, ensuring they can interdict threat actors before they can achieve their objectives.



Save Time and Resources

AttackIQ provides an economical yet continuous means of validating NIST CSF security controls.



Help Organizations Meet NIST CSF Compliance

NIST CSF establishes a clear oversight framework to ensure compliance and demonstrates a commitment to cybersecurity excellence to stakeholders, auditors, regulators and your organization.

ABOUT ATTACKIQ

AttackIQ, the leading independent vendor of breach and attack simulation (BAS) solutions, built the industry's first BAS Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. AttackIQ is passionate about giving back to the cybersecurity community through its free award-winning AttackIQ Academy and partnership with MITRE Engenuity's Center for Threat-Informed Defense.

For more information visit www.attackiq.com and follow AttackIQ on Twitter, LinkedIn, and YouTube.