ATTACKIQ

White Paper

The CISO's Guide to NIST Security Control Compliance

Using MITRE ATT&CK® to Achieve Effective NIST 800-53 Compliance

Notice

AttackIQ® publications are made available solely for general information purposes. The information contained in this publication is provided on an "as is" basis. Any additional developments or research since the date of publication will not be reflected in this report.

Table of Contents

Executive Summary

In late 2020, MITRE Engenuity's Center for Threat-Informed Defense mapped the security controls in the NIST 800-53 framework to the adversary behaviors described by the MITRE ATT&CK® framework. Federal agencies and private organizations can benefit in a number of ways from the connections that this process has revealed.

Still, if organizations are unable to test their defenses' performance in the real world, a gap remains in their assessment of their security technologies, people, and processes. New compliance mapping capabilities built into the AttackIQ Security Optimization Platform close this loop by validating that the technologies an organization has deployed to meet NIST 800-53 security standards are successfully detecting and responding to ATT&CK-defined threat behaviors. The platform's compliance functionality also provides evidence of controls' effectiveness, which auditors can use to confirm the agency's or company's NIST compliance.

The Evolution of Two Cybersecurity Frameworks

As interconnected computing evolved in the 1970s and 1980s, so too did threats to the systems involved and the information they stored. Regulations soon emerged to set a baseline for security controls that individuals and organizations could follow to protect their hardware, software, and data. From the U.K.'s Computer Misuse Act of 1990 to the U.S.'s 2002 Homeland Security Act to the proposed Cybersecurity Act of 2012, which was considered but ultimately rejected by the U.S. Congress, governments have worked for three decades to establish security standards that are applicable across all types of organizations.

In 2005, the U.S. National Institute of Standards and Technology (NIST) published a set of standards, guidelines, and best practices that federal government agencies could use to manage their cybersecurity risk, "Recommended Security Controls for Federal Information Systems", known as Special Publication 800-53. In lieu of any broader, or binding, regulatory or legislative guidance, businesses in a wide range of industries adopted those practices as well.

When Congress failed to adopt the Cybersecurity Act of 2012, an ambitious legislative proposal to legally codify national cybersecurity standards across sectors, President Barack Obama's administration used the NIST 800-53 framework as a baseline for building a comprehensive, digestible framework of cybersecurity best practices with which to engage the U.S. public and private sectors. Rather than referring to that strategy by a number (i.e., "800-53"), the Obama administration referred to this 2014 document as the "NIST Cybersecurity Framework". Built through a collaborative multi-stakeholder process, the "NIST Framework" became a leading reference for cybersecurity best practices across the globe.

At around the same time as the NIST framework was being developed, in 2012-2013 the nonprofit MITRE Corporation began developing a curated knowledge base and model of behaviors expected from cyberadversaries. This framework, called Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), was officially released in May 2015. It represented another step forward in predicting attacks and, in doing so, helping to prevent them. Still, corporate and government security leaders had limited visibility into the actual effectiveness of different approaches to threat detection and mitigation. They needed a means of verifying the performance of the defenses they employed, especially in light of the ever-evolving nature of cyberattacks.

The Evolution of Two Cybersecurity Frameworks (cont.)

MITRE's work to align the ATT&CK framework with the NIST security control structure helps close gaps in an organization's security ecosystem. This alignment marries a threat-informed approach to defense, focused on adversaries' likely behaviors, to the world's leading security control regulatory framework. When the combined frameworks are then integrated into an automated testing platform, security leaders can measure and test the effectiveness of their internal controls in detecting and responding to threats described by ATT&CK. They can simultaneously determine the degree to which their people, processes, and technologies comply with NIST requirements.

As a result, businesses and government agencies can now move beyond simple compliance to measuring the true effectiveness of their approach to security. By automating this approach, they can ensure that controls testing happens routinely, not just on the occasion of an audit or internal security review. Security leaders can report to their boards about their program's effectiveness in meeting the NIST controls. Ultimately, leveraging an automated testing platform that incorporates both NIST 800-53 and MITRE ATT&CK improves an organization's overall security posture.

A Tale of Two Communities

Although NIST 800-53 and MITRE ATT&CK are both focused on strengthening organizational defenses, they represent opposite sides of the cybersecurity coin. NIST 800-53 has traditionally taken the perspective of the network defender—the agency or organization with assets to defend—while MITRE ATT&CK takes on the adversary's approach and aims to inform defenders about how the adversary will likely behave in relation to an organization's cybersecurity program.

Given the different perspectives and backgrounds of the two frameworks, the two approaches to cybersecurity have tended to exist as separate analytic entities. Aligning the two frameworks together helps ensure that the defensive community adopts a "threat-informed defense" approach to cybersecurity strategy. Rather than focusing solely on compliance, defenders can now look at their NIST security control effectiveness through the lens of adversary behaviors.

Compliance and Controls

For any organization embarking on a cybersecurity program, NIST 800-53 provides a thorough controls management framework. The "meat" of the framework lives inside the 18 Control Families, which cover diverse areas of cybersecurity from Access Control to System and Service Acquisition. The Control Families house the Controls themselves as well as any Control Enhancements that have been established to offer more prescriptive guidance on how a given Control should be implemented.

NIST 800-53 controls are officially applicable to the IT infrastructure of every U.S. federal government agency, both within and outside the Department of Defense, with the exception of national security systems. The controls also apply to government contractors and others who work in the federal space. Chief Information Security Officers (CISOs) in federal agencies and contractors can use the framework as a motivation to drive adoption of certain technologies. They can also use NIST 800-53 as a reference in describing, baselining, building, and (incrementally) maturing their programs to effectively detect and prevent any incoming attacks.

Federal adoption is just the starting point for NIST 800-53. Since the voluntary framework was first published in 2005, private companies around the world have incorporated it into their cybersecurity planning and practices. Following NIST 800-53 guidelines helps organizations achieve compliance with the cybersecurity portions of the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Modernization Act (FISMA), among many other laws and regulations in jurisdictions globally.

Compliance and Controls (cont.)

Because NIST 800-53 addresses such a wide range of security controls, large numbers of businesses and other organizations choose to adhere to the standards, with the goal of improving their security infrastructure and building confidence in its effectiveness. This is true not only within the United States, but around the world. Global adopters of the framework typically cite several reasons:

- The comprehensiveness of the NIST 800-53 standards, which support development of a complete security roadmap;
- The framework's focus on detection and response, rather than after-the-fact identification of attacks and recovery of lost data or capabilities;
- Its support for a common language about cybersecurity throughout complex organizations; and
- Its promise of a shared understanding of cybersecurity issues and definitions among organizations in different countries and across myriad industry sectors.

Comprehensive frameworks such as 800-53 are not undertaken lightly. An implementer of 800-53 must remain detail-oriented as they align their security environment to the standards that are established by the framework itself.

Adversary Behavior Specialists and MITRE ATT&CK

One goal of the MITRE ATT&CK framework is to document known adversary behaviors. Instead of detailing control objectives, ATT&CK provides a common language to describe how an adversary would breach or undermine the defenses commonly in use.

Anticipating the adversary's approach requires a different type of technical skill when compared to a person focused on implementing a control framework; adversary-focused individuals tend to be strategic thinkers with extensive technical expertise. Traditionally and by perspective, they may be more interested in what a hostile government cyberattacker is reading and how the attacker operates than in an organization's compliance with a security control framework. But that era is coming to an end with the rise of the threat-informed defense strategy.

Where Do These Communities Intersect?

A threat-informed defense strategy hinges on the notion that both communities—security control managers and adversary-focused, cyberthreat intelligence experts—have insights that can dramatically improve an organization's security posture if they work together. That is why marrying NIST 800-53 and MITRE ATT&CK has such powerful implications for improving the effectiveness of an organization's cybersecurity program. Aligning the two allows for the fusion of risk management and threat management.

Resource limitations have presented organizations with an historical challenge to incorporating these two perspectives into a single security program. Typically, only exceptionally large, regulated organizations like major investment banks or the U.S. military have been able to build a unified program that aligns security control compliance with cyberthreat intelligence, largely because they can employ large numbers of professionals from both security communities.

Through the use of automated breach and attack simulation and the contributions of MITRE Enginuity, it is now possible for organizations of all types—not just those amongst the world's largest—to bring a unified, threat-informed perspective to their cybersecurity programs.

Mapping NIST 800-53 to ATT&CK

In the winter of 2020, MITRE Enginuity mapped Revisions 4 and 5 of the NIST 800-53 controls to the adversary behaviors described by the ATT&CK framework. With the NIST 800-53 security control family, MITRE ATT&CK, and a data-driven automated breach and attack simulation platform, it is now possible to provide a universal means to communicate between the three teams that have classically managed and enforced an organization's cybersecurity:

- **Red teams** can now direct their operations against a specific, known set of security controls. Red teams are traditionally responsible for testing the effectiveness of the organization's defense security controls; the NIST framework clarifies the compliance implications of the red team's activities. The red team can now understand not only how the defensive team's technical controls can mitigate their behaviors, but also how those controls fit into the NIST 800-53 framework.

- **Blue teams** can now see clearly how their defense technologies support the organization's security compliance. Blue teams are responsible for the design, operation, and management of the organization's detection and response capabilities; armed with real data about their security program performance against NIST 800-53, the blue team can make adjustments to better meet its regulatory requirements and improve the organization's overall audit readiness.

- **White teams** gain greater clarity from the NIST-ATT&CK alignment about the organization's overall security performance. White teams often include an organization's auditors, and they have traditionally depended on interviews and log entries for their audit evidence. This new approach streamlines audit processes through real performance data, allowing the white team and everyone in the organization to operate off the same page. Armed with clear performance data and a clear line-of-sight into the blue and red team's automated defensive testing activities, white teams can better assess the organization's overall security effectiveness and ensure regulatory success.

Benefiting from the NIST 800-53 and ATT&CK Alignment

Connecting NIST 800-53 controls to MITRE ATT&CK techniques across all three internal security teams strengthens the overall security program in several important ways. First, it creates a common understanding of the adversary techniques that a specific security control or set of controls is designed to detect or mitigate. From this understanding flows shared knowledge about which security controls the organization should implement to properly defend itself against a particular adversary behavior. The security team can validate that deployed policies, teams, and technologies function as intended; data then helps team leaders to optimize their security program over time to ever greater operational effectiveness and resource use.

What does that mean specifically? The integrated NIST-ATT&CK perspective provides security leaders with greater clarity about overall program readiness in relation to known threats and the existence of compensating security controls for all of the relevant NIST 800-53 Control Families. The net result is that the organization better understands where gaps exist—and where the organization may benefit from additional security investments to better adhere to specific Control Families. With that information, security leaders can prioritize investments and make longer-term budgeting and resource-allocation decisions.

Benefiting from the NIST 800-53 and ATT&CK Alignment (cont.)

Automation stands at the center of the process. Historically, smaller agencies and organizations have lagged behind those with greater resources not only in threat intelligence, but in the security control validation process as a whole. Organizations have faced a variety of challenges, including a lack of an agreed-upon threat and security control lexicon, a lack of continuous validation of security controls across an organization, and a lack of prioritization in where and how to improve security effectiveness. Today, ATT&CK provides a common threat lexicon, NIST 800-53 provides a common security control lexicon, and automated adversary emulation software empowers a wide range of organizations to incorporate security control validation and security optimization as routine elements of their cybersecurity program. The result is not only a tactical improvement in security operations, but a strategic change in where—and how—to make adjustments and investments to improve security effectiveness.

Jointly harnessing NIST 800-53, the MITRE ATT&CK framework, and an automated testing platform like the AttackIQ Security Optimization Platform is a new best practice for securing organizations around the world. By putting real performance data at the center of their analysis, security teams can measure their security program effectiveness against the adversaries that matter most—and make meaningful changes to achieve NIST 800-53 compliance.

Using the AttackIQ Security Optimization Platform to Align NIST 800-53 and ATT&CK

The AttackIQ Security Optimization Platform enables organizations to emulate the largest set of adversary behaviors that are aligned to the ATT&CK framework. By automating these attack emulations, the solution works autonomously, testing an agency's or company's controls on a continuous basis. AttackIQ assessments require minimal oversight by security staff, and they can run in the background as the organization goes about its daily business. This means they become regular and routine, rather than infrequent one-off events precipitated by an audit or by emerging threats.

Building on MITRE Engenuity's research to map the NIST 800-53 Controls and Control Enhancements with ATT&CK techniques, AttackIQ has introduced new Assessments into the Security Optimization Platform. These Assessments take adversary behaviors from the AttackIQ Library to guide the testing activity, producing evidence that makes it possible for a government agency or business to easily understand how it is fulfilling the NIST 800-53 control objectives they intend to uphold.

At the same time, AttackIQ's automated security control validation supports an organization's internal assessment of its people, processes, and technologies in detecting and thwarting identified ATT&CK adversary behaviors. The platform can now validate that a federal agency's or business's defenses effectively comply with NIST 800-53 controls.

Specifically, the output of this compliance capability assessment is data that reads "[NIST control] mitigates [ATT&CK technique]." In other words, the AttackIQ Security Optimization Platform now provides evidence that an organization's defenses which comply with the specified NIST control are effectively protecting against the specified ATT&CK technique.

The AttackIQ Security Optimization platform can provide output in an easy-to-understand visual presentation, which can be delivered as a report for reference and briefings. The Security Optimization Platform also offers API access to its results in order to support a host of other integration and automation use cases across the security program. With this data, security teams have higher confidence in their defenses' compliance with NIST 800-53, and the audit team has more granular, detailed audit evidence to show to auditors.

Through this testing method, the AttackIQ Security Optimization Platform makes NIST 800-53 compliance feasible for agencies and organizations of all sizes, not just the largest and best-resourced ones.

AttackIQ Compliance Analysis in Action

So how might this work in practice? Imagine that you're part of a private organization or federal agency that needs to evaluate its current performance related to the Priority 1 (P1) security controls captured in 800-53. Where do you start? How can you produce evidence without spinning up a giant effort that detracts from your primary mission?

AttackIQ makes it easy to get started. By executing an Assessment inside the Security Optimization Platform, an authorized user can gain insight into which adversary behaviors were successfully detected and prevented by a security technology that directly fulfills the controls and Control Enhancements inside a NIST 800-53 Control Family.

Let's walk through an example of how you might do this with the Security Optimization Platform. We will use the new Assessment Template to evaluate security technology performance using the tactics and techniques of the MITRE ATT&CK framework in accordance with NIST 800-53.

1. **Assessment.** Figure 1, below, is an Assessment Template showing MITRE ATT&CK Tactics and associated Scenarios in the Security Optimization Platform that are ready to run on your security technologies. You will note that the AttackIQ Security Optimization Platform offers broad coverage across all the MITRE ATT&CK Tactics that are relevant to the controls specified, with more delivered on a regular basis to our customers as the Security Optimization Platform evolves over time.

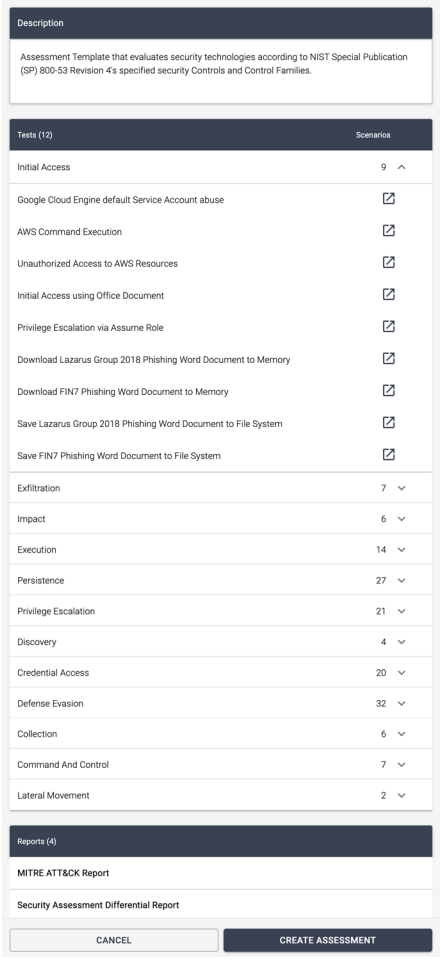


Figure 1. Assessment that evaluates security technologies against adversary behaviors according to NIST 800-53.

2. **Prevention and Detection Results.** Figure 2, below, shows the Results Summary view of the AttackIQ Security Optimization Platform, and how your technologies fared against 111 unique techniques aligned with NIST 800-53.

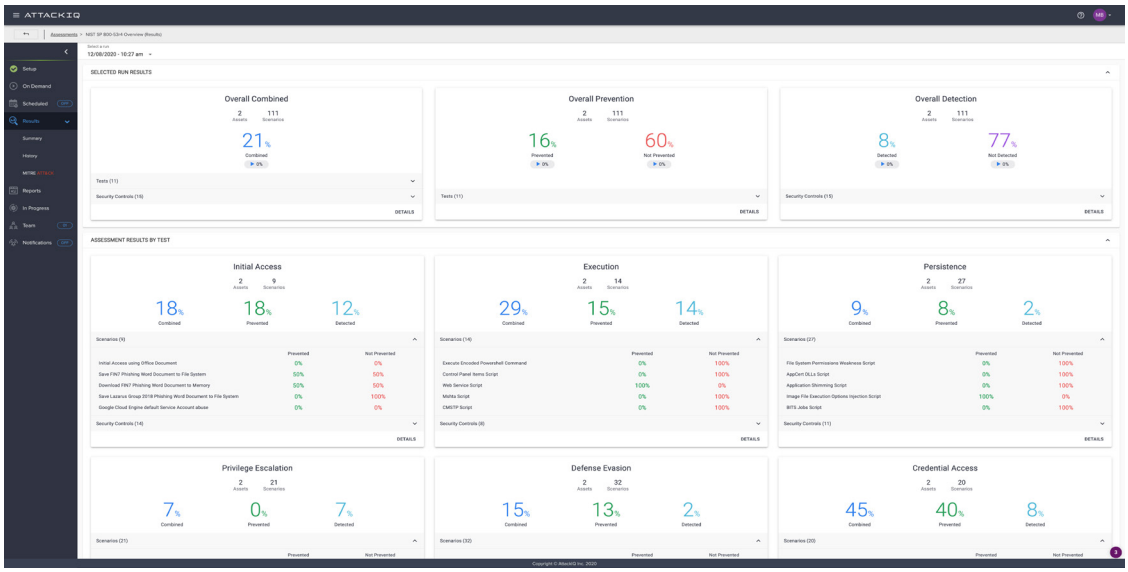


Figure 2: Prevention and detection results.

3. **MITRE ATT&CK Heatmap.** Figure 3, below, is a MITRE ATT&CK Matrix view showing how well your security technologies performed when evaluated against 111 techniques. In our hypothetical example below, a Carbon Black configuration was assessed using adversary behaviors that directly correspond to the controls specified in 800-53. Once you have had a chance to review the areas in your configuration that you would like to improve, the Security Optimization Platform generates more detail about specific steps you can take to improve your security effectiveness.

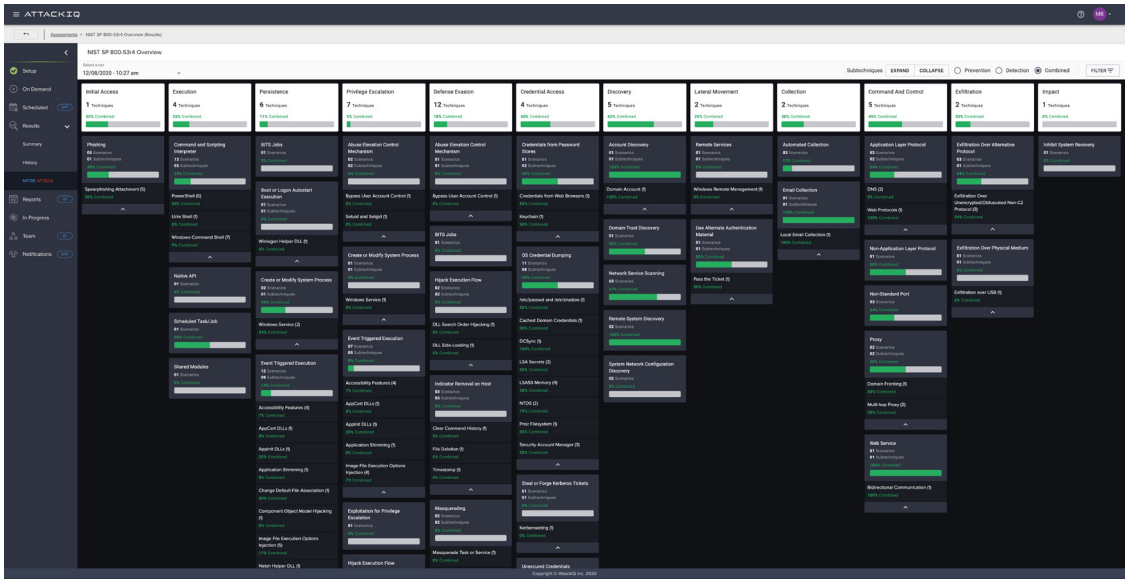
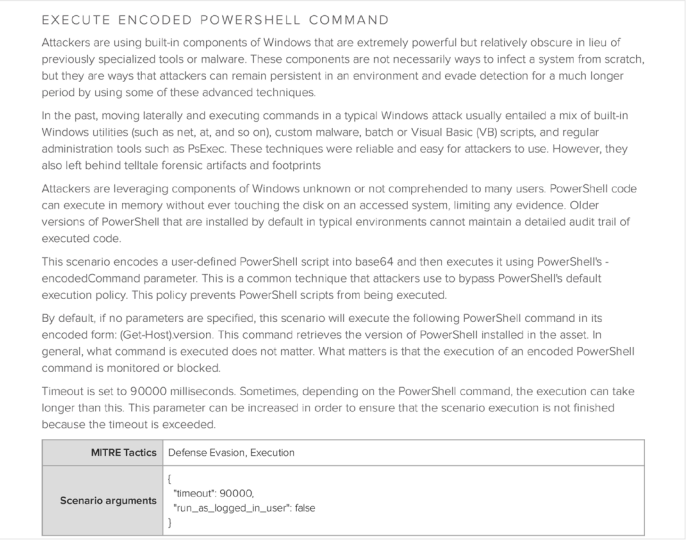


Figure 3: MITRE ATT&CK Navigator heatmap showing security effectiveness.

4. **Remediation Report.** Figure 4.1 and 4.2, below, show a remediation report; it provides data and guidance to help you configure your technologies to produce a more effective result. In this case, you see how the Security Optimization Platform used encoded PowerShell commands to bypass local execution policies, a common technique used by PowerShell Empire (as well as other tools that adversaries use). The detail included here will help you improve how your technologies block adversary behavior, thereby achieving the objective of the 800-53 control and improving your overall security posture. It is also easy to schedule the Assessment to run on a continuous basis to produce visibility into how your security program performs—and your state of compliance—over time.

Figure 4.1: Remediation report (title page).



EXECUTE ENCODED POWERSHELL COMMAND

Attackers are using built-in components of Windows that are extremely powerful but relatively obscure in lieu of previously specialized tools or malware. These components are not necessarily ways to infect a system from scratch, but they are ways that attackers can remain persistent in an environment and evade detection for a much longer period by using some of these advanced techniques.

In the past, moving laterally and executing commands in a typical Windows attack usually entailed a mix of built-in Windows utilities (such as net, at, and so on), custom malware, batch or Visual Basic (VB) scripts, and regular administration tools such as PsExec. These techniques were reliable and easy for attackers to use. However, they also left behind telltale forensic artifacts and footprints

Attackers are leveraging components of Windows unknown or not comprehended to many users. PowerShell code can execute in memory without ever touching the disk on an accessed system, limiting any evidence. Older versions of PowerShell that are installed by default in typical environments cannot maintain a detailed audit trail of executed code.

This scenario encodes a user-defined PowerShell script into base64 and then executes it using PowerShell's -encodedCommand parameter. This is a common technique that attackers use to bypass PowerShell's default execution policy. This policy prevents PowerShell scripts from being executed.

By default, if no parameters are specified, this scenario will execute the following PowerShell command in its encoded form: (Get-Host).version. This command retrieves the version of PowerShell installed in the asset. In general, what command is executed does not matter. What matters is that the execution of an encoded PowerShell command is monitored or blocked.

Timeout is set to 90000 milliseconds. Sometimes, depending on the PowerShell command, the execution can take longer than this. This parameter can be increased in order to ensure that the scenario execution is not finished because the timeout is exceeded.

MITRE Tactics	Defense Evasion, Execution
Scenario arguments	{ "timeout": 90000, "run_as_logged_in_user": false }

Figure 4.2: Remediation report (detail).

Conclusion

These new capabilities in the AttackIQ Security Optimization Platform create significant new insight and opportunity for the platform's users, essentially allowing it to serve as a NIST 800-53 Validation Platform. Thanks to MITRE Engenuity's research into the relationship between these two frameworks, a strategic alignment now exists between them and AttackIQ can directly illustrate gaps and identify risks that arise through non-compliance.

The benefit is that organizations that design their security infrastructure around NIST 800-53 can prove that their security environment is in compliance with the control objectives of the framework. Not only that, but they can simultaneously understand how their defenses perform against known adversary behaviors that would otherwise be mitigated by fulfilling the control objectives of the framework.

Using AttackIQ for security control validation arms CISOs with metrics they can use to make an effective case about the compliance and performance of the broader security infrastructure. With the platform's human-oriented output, CISOs will find it easier to convey the meaning of these metrics to the rest of the C-suite and the board. The net result is a total improvement in cybersecurity strategy and effectiveness.

ATTACKIQ

U.S. Headquarters
2901 Tasman Dr. Suite 112
Santa Clara, CA 95054
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization 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. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Engenuity's Center for Threat-Informed Defense.

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