EXPERT TIPS INSIDE

COUNTERING RANSOMWARE WITH MITRE ATT&CK 101

Brought to you by ATTACKIQ

PRIMER: WHY FOCUS ON RANSOMWARE?

"Ransomware is unique among cybercrime because in order for the attack to be successful, it requires the victim to become a willing accomplice after the fact."[1]

James Scott, Sr. Fellow,
Institute for Critical Infrastructure Technology

INTRODUCTION

Within the span of a few years, ransomware has become the bane of the chief information security officer's (CISO) existence. In 2023, 72% of businesses worldwide were affected by ransomware attacks.[2] In total, 2,207 U.S. 3 hospitals, schools, and governments were directly impacted by ransomware over the course of the year.[3]

The FBI advises against paying a ransom, and for good reason. While some organizations, desperate to regain access to their data and resume operations, may be tempted to pay, statistics paint a grim picture. A recent study found that 56% of organizations suffered more than one ransomware attack in the last 24 months.[4] Even more concerning, less than half (47%) of those who paid ransoms were able to recover their data and services completely.[5]

CISOs can no longer handle this issue alone. Ransomware is a C-suite and board-level concern.

STUDY PLAN

OBJECTIVES

1. Why and how are organizations under increased threat from ransomware?
2. How can CISOs leverage the MITRE ATT&CK framework with breach and attack simulation to confidently find gaps and improve their security posture?
3. What are practical steps a CISO can take to ensure the company's infrastructure is adequately protected?

STUDY PLAN

STRUCTURE

1. Why focus on ransomware?
2. How CISOs can build a bulkhead of threat-informed defense.

WHY IS RANSOMWARE SO HARD TO CONTROL?

- ***Ransomware has become commoditized.*** As adversaries learned that most companies pay the ransom, they increased the frequency of attacks. Malware code is now shared in underground marketplaces or stolen from one criminal by another. Some even offer ransomware-as-a-service (RaaS), opening the market to would-be attackers who do not have the skills or resources to develop their malware. One study concluded that threat groups utilizing RaaS from groups such as LockBit, BlackCat, and Cl0p in the latter part of 2023 saw a much larger victim count.[6]

- ***Ransomware payments have exploded.*** In 2023, ransomware payments exceeded $1 billion.[7] A significant contributing factor to the surge is the growing availability of RaaS platforms. These platforms provide cybercriminals with all the tools and infrastructure necessary to launch ransomware attacks, even without extensive technical expertise. By lowering the technical barrier to entry, RaaS has democratized ransomware, enabling a more comprehensive range of actors to participate in these malicious activities.

- ***Nation states have become bolder.*** Cyberspace exists in a gray area of jurisdiction: The pursuit of cybercriminals happens below the level of declared armed conflict, and the anonymity of the internet gives governments the cover of plausible deniability. Thus, some nations turn a blind eye to criminal groups or even give them tacit approval to strike at a government's geopolitical adversaries.

US $1 BILLION:

Ransomware Payments Exceeded $1 billion in 2023

PARTICULARLY THORNY THREATS AND RISKS

- ***China's state-sponsored threat activity is the leading offender.*** According to the Cybersecurity and Infrastructure Security Agency (CISA), China's state-sponsored threat is the broadest, most active, and most persistent cyber espionage threat to the U.S. Government and private sector networks.[8] This multifaceted threat encompasses a range of malicious activities aimed at stealing sensitive data, disrupting critical infrastructure, and gaining an advantage across various sectors.

- ***U.S. utilities are in the crosshairs.*** According to the FBI's Internet Crime Report, 2023 saw a significant increase in ransomware attacks, with over two-thirds targeting critical infrastructure.[9] In November of 2023, the Municipal Water Authority of Aliquippa,[10] servicing thousands of residents in Pennsylvania, was targeted by an Iran-linked threat group due to the municipality's usage of Israeli-made equipment. The group that claimed responsibility, Cyber Av3nger, did not stop there and released messages stating that all equipment made in Israel is a target to them.

- ***Healthcare is under persistent attack.*** The FBI's 2023 Internet Crime Report cites 249 ransomware attacks affecting the healthcare and public health sector. Within the first three months of 2024, the healthcare sector has already suffered several cyberattacks, including the devastating attack on Change Healthcare which directly impacted patient care in 74% of U.S. hospitals.[11] These disruptions endanger public safety, cause economic damage, and erode trust. We must act to strengthen defenses, share information, and prioritize cybersecurity in critical sectors.

SO WHAT SHOULD PRIVATE AND PUBLIC SECTOR CISOS BE DOING?

AT THE HIGHEST LEVEL, CYBERSECURITY PREPAREDNESS EFFORTS SHOULD CONSIST OF:

- Assuming breach of the infrastructure and planning for the highest-risk known threats using the MITRE ATT&CK® framework in combination with breach and attack simulation.
- Reviewing, rationalizing, and investing in security controls to defend data and applications, and to optimize processes.
- Validating the effectiveness of cyberdefenses by testing them continuously against real-world threats using an automated platform versus manual testing that is infrequent and expensive.

Many CISOs build their ransomware defenses on the second step alone. They invest in supposed best practices without adequate planning or testing, losing sight of the fact that even well-built corporate security controls fail against ransomware attacks.

Chief information security officers who do not lay out a cybersecurity roadmap that reflects their organization's unique assets and priorities may leave gaps in controls that attackers can leverage in ransomware exploits. Likewise, those who build a cybersecurity infrastructure but don't routinely validate that their controls are working may not be protecting corporate assets as well as they think they are.

Enter MITRE ATT&CK®. Developed by the nonprofit MITRE Corporation, the MITRE ATT&CK framework is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that security professionals have observed in cyberattacks around the world. For each listed TTP, the framework provides a description, an explanation of sub-techniques, and a list of threat actors known to use the approach. The ATT&CK framework also maps each threat to the specific security controls that organizations typically use to thwart it.

MITRE ATT&CK is generally considered to be the most authoritative and comprehensive list of TTPs available. Following every major cybersecurity incident, the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security uses the MITRE ATT&CK framework to describe the attacker's behavior.

MITRE ATT&CK includes a broad assortment of TTPs relevant to ransomware. Yet too few private-sector security executives are following the CISA's lead and enhancing their own ransomware defenses by harnessing the framework.

> ***"For companies that have already spent billions on cybersecurity — and are expected to shell out $1.75 trillion more between now and 2025 — many are humbled by the idea that a ... Fortune 500 company could be brought to its knees by someone sitting at a computer on the other side of the world."***[13]
>
> - David Braue, Cybercrime Magazine

Chief information security officers need to ensure they're adequately prepared for prospective ransomware attacks by developing a data-driven, threat-informed, ATT&CK-based defense strategy. The following are practical steps CISOs can take to ensure an effective threat-informed defense, with ATT&CK at the center.

HOW CISOS CAN BUILD A BULKHEAD OF THREAT-INFORMED DEFENSE

1. IDENTIFY HIGH-VALUE ASSETS AND DATA

No security team can quickly and easily protect every data asset against every threat the organization might face. If that was the case, cybersecurity would be an easy challenge. Real-world security requires that you prioritize the threats most likely to do the most damage to the organization and its customers. You should begin the development of a threat-informed defense against ransomware by identifying which of their assets are most crucial to protect.

- ***Identify the data that matters most to your organization.*** For each type of information, consider:
  - Could our operations continue if we lost access to this data indefinitely?
  - What would the ramifications be for customers, employees, and other stakeholders if an attacker stole this data or made it public?
  - In what ways could a breach of this data impact our business relationships or undermine our brand reputation?
- ***Map the locations and movement of your highest-value data.*** For the highest-priority information, establish:
  - Where does this data reside?
  - What applications access this data?
  - What are our user access controls for that data?
  - What is the status of our back-up strategy for this data?

2. IDENTIFY THE ORGANIZATION'S MOST SIGNIFICANT THREATS

Next, approach the risk landscape from the opposite direction. Starting with the comprehensive MITRE ATT&CK universe of detected tactics, techniques, and procedures, determine which pose the greatest threat.

- ***Delineate the attackers most likely to threaten your organization.*** Moving left to right through the MITRE ATT&CK framework: which threat actors are most active in your industry? Which are likely to target your data?
- ***Determine which TTPs you're most likely to face.*** Leverage "Mapping ATT&CK to CVE for Impact," a research project from the MITRE Engenuity's Center for Threat Informed Defense that describes how common vulnerabilities and exposures (CVE) relate to the MITRE ATT&CK framework.
    - Which attack patterns are common among the adversaries that pose the greatest threat to your organization?
    - How could they do the most damage? For example, consider an email phishing scam: If the attack utilized information provided by users to enable credential theft and privilege escalation, the adversary might gain lateral movement between servers.
- ***Consider how the most threatening TTPs map to your most valuable data.***
    - What TTPs reside at the intersection of "most likely to be used against your organization" and "highest impact in the event of a successful attack"? For more on how to use the MITRE ATT&CK framework, see the Dummies Guide to MITRE ATT&CK, written in partnership with MITRE Engenuity's Center for Threat-Informed Defense.
    - Prioritize controls on the basis of threat groups.
    - Develop a "most wanted" list of the attackers and TTPs that you must protect company assets against.

- ***Identify the security controls necessary to defend your highest-value data.*** Utilize the MITRE ATT&CK framework to prioritize them.
  - Make sure to consider all controls your organization leverages, including those native to Microsoft Azure, Amazon Web Services, and Google Cloud Platform.
  - MITRE ATT&CK streamlines mapping for the Azure security stack.[14]

3. BUILD BEST-PRACTICE DEFENSES FOR HIGH-VALUE ASSETS AND DATA

- ***Compare your list of needed controls with your current infrastructure.*** Where are the obvious gaps and vulnerabilities? For example:
  - Do you have an access control system for managing user access to the company's crown jewels?
  - Do you have ring-fences between servers to prevent unauthorized internal actions?
- ***Dig deeper to determine whether the right features and settings are turned on in each key security solution.***
  - Are protections configured to work the way you need them to?
- ***Review the most recent catalog of critical vulnerabilities published by CISA.***[15] The 2023 edition includes 187 known security issues within a wide range of common software platform. This catalog includes known security issues within a wide range of common software platforms, from Microsoft Exchange and Adobe Acrobat to Windows, Apple iOS, and Linux and Apache.
  - Evaluate your exposures, correct vulnerabilities as soon as possible, and use the MITRE ATT&CK framework to test your compensating controls to increase your protection against known and potential vulnerabilities.
- ***Prioritize investments in security capabilities to defend your assets.*** Focus on closing your infrastructure's vulnerabilities and security gaps to the TTPs on your "most wanted" list.

4. DEVELOP A STRATEGY FOR SECURITY CONTROL VALIDATION

"Amongst over 500 information technology and security leaders across sectors, 53 percent have said they are uncertain about the effectiveness and performance of their cybersecurity capabilities. Why? Because when controls fail, they fail silently." [27]

The failure to properly test EDR solutions has far-reaching and often devastating consequences. The only way to be sure controls are working as intended is to run regular tests simulating real-world attacks and gauge the response of the organization's people, processes, and technologies. In the wake of the deluge of ransomware events and cyberattacks this past year, breach and attack simulation is mission critical. Why? Because when incorporated as a routine part of security operations, CISOs can use real-time performance data to be confident that their organization is adequately prepared.

- ***Prioritize.*** You have already identified the organization's most important security controls. Use that information to prioritize specific controls for regular validation.
- ***Automate.*** No human team can test every control as frequently as it needs to be tested to protect against the growing ransomware threat.
  - Automated security control validation ensures the organization's most crucial controls can be tested continuously.
  - Ongoing validation means changes in configurations or staffing that may introduce control gaps are detected — and can be mitigated — more quickly.
- ***Streamline.*** Select a BAS solution that accelerates testing, to improve staff productivity.
  - The AttackIQ Breach and Attack Simulation Platform emulates adversary behaviors in a production environment, as described in the MITRE ATT&CK framework, with adequate specificity and realism to validate whether controls currently in place would prevent an actual attack.

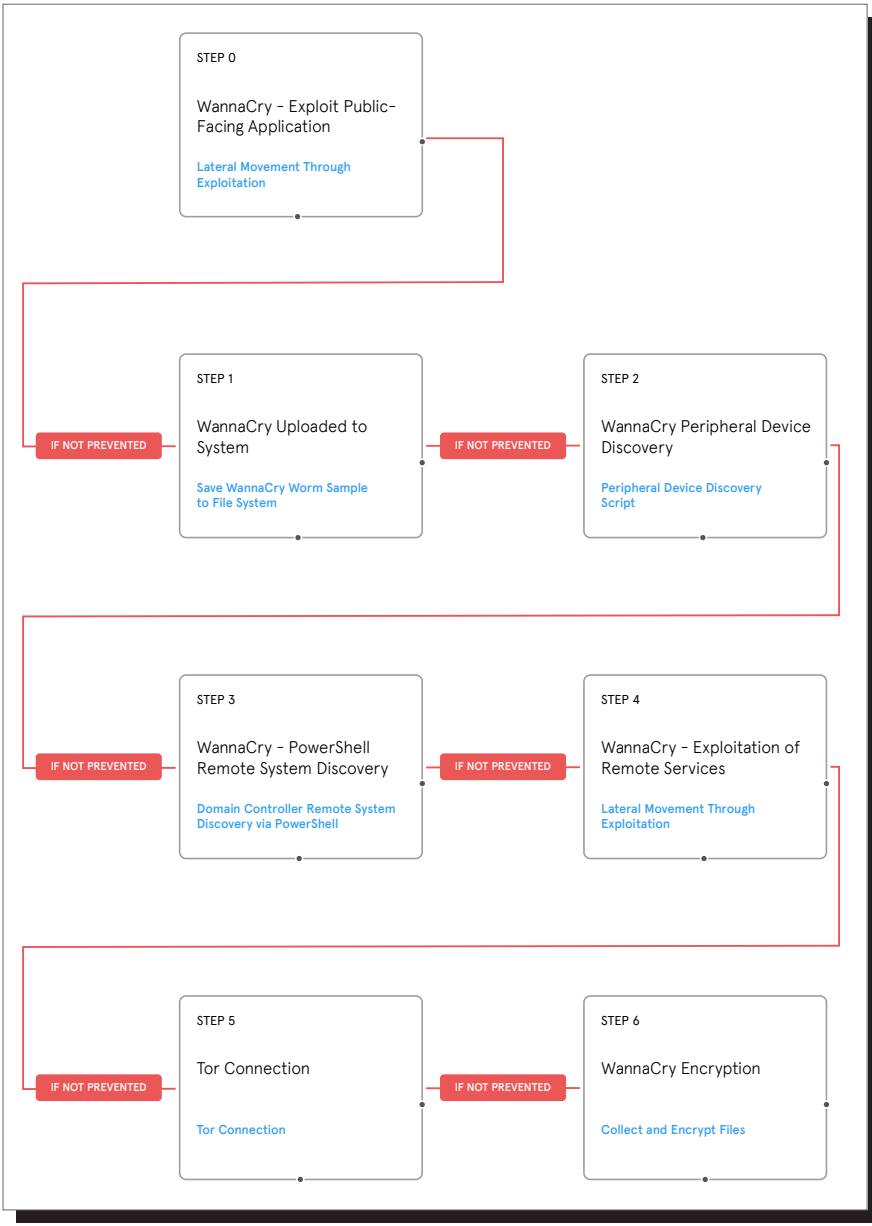
- AttackIQ's Network Security testing capabilities include prebuilt scenarios that transmit files through network traffic and playback captures of known adversary behavior.
  - It can test next-generation firewalls' ability to prevent unwanted lateral movement of network traffic.
  - It can attempt to exfiltrate sensitive data beyond the network perimeter to test for data loss prevention.
  - It can test network segmentation and micro-segmentation by discovering open and closed ports and evaluating whether specific types of adversary communications are effectively blocked.
- The industry, alongside AttackIQ, has leveraged attack graphs (or attack flows) to address a critical need. These graphs model multi-stage attacks, enabling defenders to rigorously evaluate their automated cybersecurity controls in a realistic and targeted manner.
  - The TTPs execute sequentially, as they would in a ransomware attack.
  - Through this chain of simulations, the Continuous Security Validation Platform emulates complex intrusions observed in the real world.
  - Such automated simulations are the most effective way to test security controls that leverage artificial intelligence (AI) and machine learning (ML).

- One example is a simulation of the WannaCry ransomware cryptoworm, which can use a long list of MITRE ATT&CK techniques.[28] Since its first appearance in 2017, WannaCry continues to spread and infect unpatched systems.[29] The relevant attack graph (what some call an "attack flow") in the AttackIQ Continuous Security Validation Platform validates network and endpoint security control prevention and detection capabilities to thwart it. A high-level overview of the AttackIQ Continuous Security Validation Platform's emulation of this threat's behavior is described below and shown in figure 1 and 2 below (pg. 18-19).
  - The WannaCry cryptoworm actively scans for systems (ATT&CK tactic T1595 – Active Scanning) vulnerable to CVE-2017-0144, exploited by EternalBlue.
  - Like the real threat, the AttackIQ scenario checks specified targets for an SMBv1 service being published. It can be configured to either check for this vulnerability only or exploit it if the check passes (T1190 - Exploit Public-Facing Application), opening the door for the worm to infiltrate the WannaCry payload onto vulnerable targeted assets.
  - If the target asset is vulnerable, the WannaCry payload is saved to the file system, and, if not stopped by endpoint security controls, it executes peripheral device discovery and remote system discovery scripts. This emulates the behavior of the worm to enumerate additional local filesystems and files for encryption as well as additional targets for malware propagation.
  - It then establishes an encrypted Tor channel, enabling command and control (T1573), and finally, the worm encrypts its first target (T1486), allowing the intruder to hold the data for ransom.

- The first image below shows the full appearance of the attack graph in the Continuous Security Validation Platform, and the second zooms in to show more detail.
- We describe the WannaCry-EternalBlue attack graph here given its historical importance and continued impact. Aligned to the MITRE ATT&CK framework, the AttackIQ Continuous Security Validation Platform emulates a range of ransomware families, and strings together adversary tactics, techniques, and procedures in an attack graph to emulate the adversary with specificity and realism to test an organization's security program continuously and automatically. AttackIQ will demonstrate a full range of our ransomware adversary emulation capabilities on January 27.

Figure 1, above, shows the attack graph as it appears in the AttackIQ Continuous Security Validation Platform, showing the step-by-step chain of the emulation.

Figure 2, below. zooms into the attack graph to make it readable in this format.



5. ANALYZE RESULTS FOR DECISION-MAKING

- As assessment results flow in, you will need to address any failures in the organization's prevention and detection capabilities. Questions to consider in designing the analysis process:
  - What teams should assess the risk and/or mitigation strategy?
  - What is the expected service level agreement (SLA) for mitigation/remediation?
  - What are the risk acceptance criteria for scenarios that were not successfully prevented?
  - How do we determine whether a control failure is a one-off situation or a recurring issue?
- Security must be dynamic; adjust investment priorities continuously to reflect testing data.
  - As control gaps are identified, evaluate how they can be filled. Can settings be changed to close the gaps, or do you need another security solution?
  - Are there human performance factors to address, such as additional training to take or team salary bands to adjust?
  - If testing reveals vulnerabilities in assets that would be prohibitively difficult to lock down — perhaps critical databases, Active Directory, or legacy systems — determine whether the controls surrounding those assets are as effective as they can be without impacting production systems.

6. REPEAT IN PERPETUITY, BASING FREQUENCY OF ASSESSMENTS ON CONTROL PRIORITIZATION

- Test your security controls continuously to determine effectiveness over time.
  - Longitudinal data gives you a better picture of your team's performance over time. Are your controls working as they should on a consistent basis?
  - Use performance data to analyze underlying issues. As you measure the results of the tests, what problems does your team face consistently? What are the underlying issues that impact team performance over time?

CONCLUSION

In building out their organization's threat-informed defense, some CISOs are also merging internal red and blue teams. Traditionally, these groups operated separately, with blue teams managing defensive operations and red teams conducting periodic (typically infrequent) tests of security controls. Moving to a model of "purple teaming" brings together all security staff and turns their focus to data on controls' effectiveness.

The MITRE ATT&CK framework provides a structure for focusing security teams (red, blue, and/or purple) on the defenses most critical for protecting high-priority assets. When assessed through automated adversary emulations, MITRE ATT&CK TTPs validate whether controls currently in place are effectively protecting your organization against the threat of ransomware that looms on the horizon. And if the answer is no, such an approach provides the opportunity to correct control errors and gaps, then retest to make sure you've solved the problem.

Developing a security program that revolves around threat-informed defense is challenging, for sure, but the end result is well worth the effort. Establishing a continuous testing regime gives the management team data-driven control over the security program's overall performance. It gives the security team a means for implementing a threat-informed defense against ransomware. By putting MITRE ATT&CK, automated security control validation, and a threat-informed defense at the center of your cybersecurity strategy, you gain a comprehensive, data-driven understanding of your security program's preparedness against ransomware.

TEST YOUR KNOWLEDGE!

1. **What three key initial steps for an effective security strategy are discussed above?**

   a. Draft a cybersecurity strategy; invest in an intrusion detection system; hire an MSSP

   b. Assume breach; invest in best-in-class defenses; test your defenses continuously

   c. Wring your hands with anxiety; call your mom and dad; complain to your dog.

   d. Adopt a zero trust strategy; partner with the government; test your security a few times a year.

2. **Why is ransomware so hard to stop?**

   a. Ransomware is increasingly a commodity.

   b. Nation-states use criminal groups to serve their objectives.

   c. Cryptocurrency has exploded as a platform for payments.

   d. All of the above.

3. **What percentage of security leaders lack confidence in their security controls?**

   a. 20 percent

   b. About 40 percent

   c. Approximately 50 percent

   d. 75 percent

TEST YOUR KNOWLEDGE!

4. What does the MITRE ATT&CK do?

a. Instructs users on compliance frameworks for achieving cybersecurity

b. Organizes known adversary tactics, techniques, and procedures into a matrix

c. Helps organizations adopt a zero trust strategy

d. Identifies qualifications for security personnel

5. Fill in the blank: MITRE ATT&CK is a framework of _____ (TTPs).

a. Adversary tokens, tickets, and plans

b. Adversary tactics, techniques, and procedures

c. Adversary temperament, transactions, and prescriptions

d. Adversary tips, taxonomy, and patterns

6. Purple teams include aspects of both red and blue teams?

☐ TRUE

☐ FALSE

PAGE LEFT BLANK INTENTIONALLY

Test answers on next page.

ANSWER KEY

1. Answer: B
2. Answer: D
3. Answer: C
4. Answer: B
5. Answer: B
6. Answer: True

CITATION

[1] James Scott, "33 Ransomware Strategies," O'Reilly

[2] Ani Petrosyan. "Businesses worldwide affected by ransomware 2018-2023," Statistia. March 28, 2024

[3] "The State of Ransomware in the U.S.: Report and Statistics 2023," Emsisoft. January 2, 2024

[4] "Ransomware: The Trust Cost to Business 2024," Cybereason. February 22, 2024

[5] "Ransomware: The Trust Cost to Business 2024," Cybereason. February 22, 2024

[6] "Rise in Active RaaS Groups Parallel Growing Victim Counter," Trend Micro. March 27, 2024

[7] "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," Chainalysis. February 7, 2024

[8] "People's Republic of China Cyber Threat," CISA.

[9] "Federal Bureau of Investigation Internet Crime Report 2023," FBI. December 12, 2023

[10] Jonathan Greig, "Pennsylvania water authority hit with cyberattack allegedly tied to pro-Iran group," November 27, 2023

[11] "AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances," American Hospital Association. February 21, 2024

[12] Cynthia Brumfield, "No easy solutions to the ransomware threat despite takedowns," CSO, March 19, 2024

[13] David Braue, "CISO Report: Ransomware Business Is Booming," Cybercrime Magazine, December 10, 2021.

[14] Andrew Costis, "Azure Security Stack Mappings: The Top Native Security Controls for Ransomware,"AttackIQ blog, August 23, 2021.

[15] "Known Exploited Vulnerabilities Catalog," Cybersecurity & Infrastructure Security Agency

ABOUT ATTACKIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Breach and Attack Simulation 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 cyber defenses work as expected, aligned with the MITRE ATT&CK framework.

The company is committed to supporting its MSSP partners with a Flexible Preactive Partner Program that provides turn-key solutions, empowering them to elevate client security. 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