ATTACKIQ

White Paper

The CISO's Guide to MITRE ATT&CK® in Healthcare and Public Health

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

"Owing to the insidiousness of its onset, the victims of cancer are often totally unconscious of the seriousness of the disease which has attacked them. They are quite naturally lulled by the entire absence of symptoms into a sense of security..."

– Charles Plumley Childe, The Control of a Scourge: Or, How Cancer is Curable[1]

About MITRE

Founded in 1958, The MITRE Corporation is a not-for-profit organization that operates federally funded research and development centers (FFRDCs), as well as independent research programs. In 2015, MITRE Corporation first released the MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) cybersecurity framework. Today, the MITRE ATT&CK framework is considered the most authoritative, comprehensive, and complete set of up-to-date attack techniques and supporting tactics.

Though cancer diagnosis and treatment have advanced significantly since Childe wrote these words in the early 20th century, his observations still hold true. Moreover, they are also applicable today to a type of threat that was beyond Childe's imagination: in cybersecurity, as in medicine, an insidious and malicious presence may spread undetected, leaving organizations reeling once the attack is exposed. The seeds of the infamous SolarWinds breach, which was publicly disclosed in December 2020, were likely sown as early as the fall of 2019.[2] The attack is still metastasizing throughout the economy.

Just as those who fight various cancers require a deep understanding of the wayward strains of DNA, healthcare and public health (HPH) CISOs need exhaustive knowledge of their cyberadversaries. Who are they? What do they seek? How do they go about pursuing their ends? The MITRE ATT&CK® framework, developed and maintained by the MITRE organization, is the manifestation of a collective effort to answer these questions. More important, the framework provides actionable information that cyberdefenders can use to validate and improve their security controls.

This guide offers a high-level overview of the MITRE ATT&CK framework, why using it to validate security controls is essential for HPH organizations, and how you can take advantage of the framework as part of your comprehensive cyberdefense efforts.

[1] Charles Plumley Childe, The Control of a Scourge, Or How Cancer is Curable, Dutton, 1907., pp 153-154

[2] Sudhakar Ramakrishna, "New Findings From Our Investigation of SUNBURST," Solarwinds.com, January 11,2021.

What Is MITRE ATT&CK?

MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that have been observed in actual cyberattacks against organizations around the world.

Threat-Informed Defense

According to MITRE, threat-informed defense "applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks." AttackIQ is a founding member of MITRE Engenuity's Center for Threat-Informed Defense, a privately funded research and development center that advances threat-informed defense for the public interest.

Globally accessible and based on real-world data, the ATT&CK knowledge base is foundational for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. MITRE's stature in the cybersecurity community, and its objectivity, make it the ideal platform from which healthcare industry security operations management, compliance and governance teams, executive management, and boards of directors can objectively evaluate and measure the performance, risk, and capabilities of their cybersecurity controls.

Using the MITRE ATT&CK framework, security and compliance teams can assess the cybersecurity threats that their organization is likely to face and create organization-specific models of these threats. Then they can apply the models to simulate the threats in a protected version of their network environment. With frequent, comprehensive simulations, healthcare security teams can verify that their technology, staff, and processes are capable of delivering appropriate defenses and mitigations.

A big part of MITRE ATT&CK's value lies in the collective and standardized nature of its threat intelligence gathering effort. Other threat intelligence communities often suffer from incoherence, as different contributors use different terminology to describe threats. The MITRE ATT&CK framework imposes a common lexicon on all contributions, which improves information quality. As an example, the U.S. Cybersecurity and Infrastructure Agency (CISA) uses MITRE ATT&CK to develop its alerts for the HPH sector.[3] This makes it easy for security professionals in healthcare organizations to compare the alerts with their existing threat intelligence.

MITRE ATT&CK is also part of a larger universe of cybersecurity standards, regulations, and best practices. Many HPH CISOs use MITRE ATT&CK in conjunction with other key frameworks, such as International Organization for Standardization (ISO) 27001®, the Health Insurance Portability and Accountability Act (HIPAA), HITRUST CSF, the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) and NIST Special Publication 800-53, Center for Internet Security (CIS) Controls®, and Information Systems Audit and Control Association (ISACA)®'s COBIT® 2019, as part of a multipronged, threat-informed approach to protecting their organizations.[4]

[3] "Joint Cybersecurity Advisory | Ransomware Activity Targeting the Healthcare and Public Health Sector," CISA, October 28, 2020.

[4] For more information about these frameworks, see "A CISO's Guide to the Top Cybersecurity Frameworks."

[5] Mitre.org, accessed Feb 2, 2021.

Why Validating Cybersecurity Controls Is Crucial in HPH Settings

HPH organizations rely on security controls to protect a broad range of critical assets that are vulnerable to attack and whose failure can have serious consequences.

To defend their networks — and the associated endpoints, data, applications, and users — organizations employ security controls. "Security control" is a broad term that may refer to a process or a standard. It may also refer to the software or hardware technology that performs gatekeeping, inspection, quarantining, alerting, or other defensive or impact-mitigating tasks in service of the process or standard. The National Institute of Standards and Technology defines a security control as "a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements."[6]

HPH organizations rely on security controls to protect a broad range of critical assets that are vulnerable to attack and whose failure can have serious consequences, not only for business operations, but for individual and collective human life. These include:

- **Medical devices (connected to the Internet of Things, or IoT) and clinical and administrative applications** are particularly susceptible to malware-induced malfunction or distributed denial of service (DDoS). The impact of such attacks can be devastating. In September 2020, for example, Düsseldorf University Hospital experienced a ransomware attack that rendered the hospital incapable of admitting an acutely ill patient.[7] During late 2020, when COVID-19 vaccinations had just started rolling out, one research team detected a 51 percent increase in web application attacks on healthcare targets in a single month.[8]

- **HIPAA-governed personal health information** can be exfiltrated and exposed. The U.S. Dept. of Health and Human Services (HHS) collects reports of breaches of unsecured protected health information affecting 500 or more individuals. A recent review revealed that more than 700 breaches were reported within the last 24 months.[9]

- **Vaccine and other research data** are ripe targets for exfiltration or corruption, for economic or political gain. In a cyberattack on the European Medicines Agency (EMA), first reported in December 2020, documents related to COVID-19 medicines and vaccines were leaked on the internet. In January 2021, the EMA revealed that the leaked data "included internal/confidential email correspondence dating from November 2020, relating to evaluation processes for COVID-19 vaccines."[10] More alarmingly, the EMA stated, "Some of the correspondence has been manipulated by the perpetrators prior to publication in a way which could undermine trust in vaccines."

[6] NIST website glossary, accessed February 2, 2021.

[7] "Police launch homicide inquiry after German hospital hack," BBC.com, September 18, 2020.

[8] Terry Ray, "Web Application Attacks on Healthcare Spike 51% As COVID-19 Vaccines are Introduced," Imperva.com, January 12, 2021.

[9] U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, accessed February 3, 2021.

[10] Cyberattack on EMA - update 5, European Medicines Agency, January 15, 2021.

Why Validating Cybersecurity Controls Is Crucial in HPH Settings

Verizon estimates that 82 percent of enterprise breaches should have been stopped by existing security controls but weren't.

- **Manufacturing facilities** for vaccines and other critical medical supplies are vulnerable to ransomware that could shut down production. And it's not just at the leading pharma companies. In India, where manufacturers are working to produce affordable vaccines for the world's poorer communities, ransomware attacks are also intensifying.[11]

- **Healthcare supply chains** aren't safe, either. Security researchers at IBM discovered attempts to use targeted phishing to disrupt the temperature-controlled supply chain essential for the distribution of COVID-19 vaccines.[12]

- **Healthcare facilities** are vulnerable to attacks that can disrupt power supplies and heating, ventilation, and air conditioning (HVAC) systems, as well as patient oxygen supply.

- **Communications networks** in and among HPH facilities serve as expedient vectors for cyberattacks. The exposure of these networks to the public internet, through internet and cloud service providers, makes them difficult for HPH security teams to protect. A cyberthreat that infects one cloud service provider can spread quickly to many cloud subscribers, potentially endangering critical HPH operations.

Recognizing the urgency of protecting their information assets, HPH organizations are expected to spend a cumulative $125 billion on cybersecurity from 2020 to 2025.[13] But they will reap little return on this investment if the security controls they employ fail.

And they do fail. What's worse, they fail silently so that breaches keep occurring, even when security leaders are confident that their organizations are protected. Verizon estimates that 82 percent of enterprise breaches should have been stopped by existing security controls but weren't. What's more, the healthcare sector ranks among the highest in the rate of severe security flaws.[14] As a result, CISOs are under increasing pressure to pinpoint these silent failures so they can deliver risk assessment and mitigation data that is accurate, extensive, and current. This is possible only if CISOs know what security controls they have in place and how effective they actually are at preventing and mitigating real-world attacks.

[11] Prabhjote Gill, "Another Indian pharmaceutical giant reports cybersecurity breach within two weeks of ransomware hack on Dr Reddy's," Business Insider India, November 5, 2020.

[12] Frank Bajak, "Phishing ploy targets COVID-19 vaccine distribution effort," Associated Press, December 3, 2020.

[13] "The 2020-2021 Healthcare Cybersecurity Report," Cybersecurity Ventures, accessed February 4, 2021.

[14] "Internet Risk Surface in The Healthcare Sector: Benchmarking digital risk factors facing healthcare institutions," RiskRecon, the Cyentia Institute, and Health-ISAC, accessed February 3, 2020.

How to Validate Security Control Effectiveness Using MITRE ATT&CK

The MITRE ATT&CK framework provides the real-world basis for creating these organization-specific threat models.

In order to validate security control effectiveness, you need to create threat models that describe the threats that are likely to affect your HPH organization and the associated impact of each threat. The MITRE ATT&CK framework provides the real-world basis for creating these organization-specific threat models.

Here is a high-level overview of an approach to MITRE ATT&CK:

1. Use the knowledge base to **research the cyberthreat groups** that might target your organization. Below is a summary of what you might find by searching for the term "healthcare" on the groups page of the MITRE ATT&CK site:

Name	Associated Groups	Description
APT41		APT41 is a group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity. APT41 has been active since as early as 2012. The group has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries.
Deep Panda	Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine	Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. The intrusion into healthcare company Anthem has been attributed to Deep Panda. This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. Deep Panda also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. Some analysts track Deep Panda and APT19 as the same group, but it is unclear from open source information if the groups are the same.
FIN4		FIN4 is a financially-motivated threat group that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013. FIN4 is unique in that they do not infect victims with typical persistent malware, but rather they focus on capturing credentials authorized to access email and other non-public correspondence.
menuPass	Stone Panda, APT10, Red Apollo, CVNX, HOGFISH	menuPass is a threat group that appears to originate from China and has been active since approximately 2009. The group has targeted healthcare, defense, aerospace, and government sectors, and has targeted Japanese victims since at least 2014. In 2016 and 2017, the group targeted managed IT service providers, manufacturing and mining companies, and a university.
Orangeworm		Orangeworm is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015, likely for the purpose of corporate espionage.
Whitefly		Whitefly is a cyber espionage group that has been operating since at least 2017. The group has targeted organizations based mostly in Singapore across a wide variety of sectors and is primarily interested in stealing large amounts of sensitive information. The group has been linked to an attack against Singapore's largest public health organization, SingHealth.
Tropic Trooper	Pirate Panda, KeyBoy	Tropic Trooper is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. Tropic Trooper focuses on targeting government, healthcare, transportation, and high-tech industries and has been active since 2011.

Table 1. Sample MITRE ATT&CK search results for adversary groups targeting healthcare
[Source: HHS Cybersecurity Program, Office of Information Security[15]]

[15] "HPH-Sector Cyber Threat Actor Modeling with MITRE ATT&CK®," HHS Cybersecurity Program, Office of Information Security, July 23, 2020.

How to Validate Security Control Effectiveness Using MITRE ATT&CK

Many CISOs are now turning to breach and attack simulation (BAS) software.

Click on a group to **explore the techniques** they employ. From there, you can drill down into specific tactics for achieving each technique and the related procedures (specific implementations of techniques).

2. Using these prospective adversaries' TTPs, **simulate the chosen techniques** against your current security controls. Some security teams employ penetration testers or red teams to do this. But these methods alone can focus too narrowly on a few controls. Pen testers and red teams can also be expensive to engage and train. Many CISOs are now turning to breach and attack simulation (BAS) software, which helps create and run testing scenarios, and compile and analyze the results. The best BAS solutions can be configured to run automatically at regular intervals, to improve red and blue team efficiency and help ensure they are not caught off guard by rapidly emerging threats.

3. **Identify any gaps** in protection against expected threats. The simulation results will reveal the extent to which each of the selected MITRE ATT&CK tactics succeeded and the extent to which the existing security controls detected the tactics in use. Figure 1 shows an example of this.

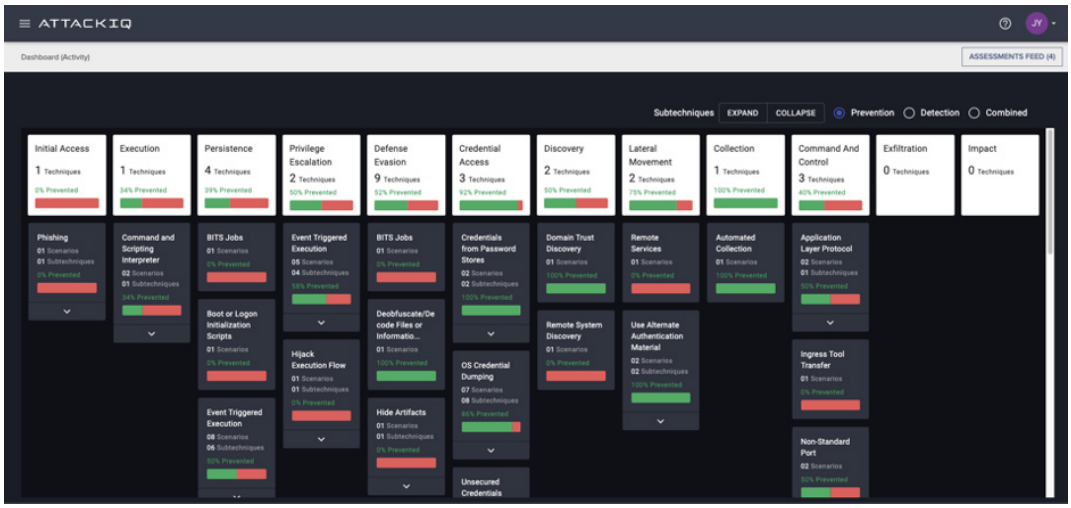

Figure 1. The AttackIQ Security Optimization Platform helps assess and describe exposure to cyber risks.

How to Validate Security Control Effectiveness Using MITRE ATT&CK

Security Optimization

Security optimization is the management practice of maximizing the efficiency and effectiveness of your total security program (people, process, and technology) by ensuring that existing control investments are measured, monitored, and modified continuously from a threat-informed perspective.

4. **Close gaps** by updating and/or replacing controls, business processes, and training. Blue teams can first re-examine the security control configurations; if these are not at fault, it may be the orchestration of the controls that allows tactics to succeed. Documenting these changes will help you demonstrate to executive and external stakeholders that the cyberthreats have been exposed and are being progressively contained. A breach and attack simulation platform, such as the one shown in Figure 1, can also provide useful visualizations that show stakeholders how you are testing security controls and emulating potential adversaries.

5. Institute an **ongoing program of security optimization** by operationalizing MITRE ATT&CK to plan, execute, and analyze TTP simulations, then remediate the gaps, validate the remediations, and capture the lessons learned for the next testing cycle (see Figure 2).

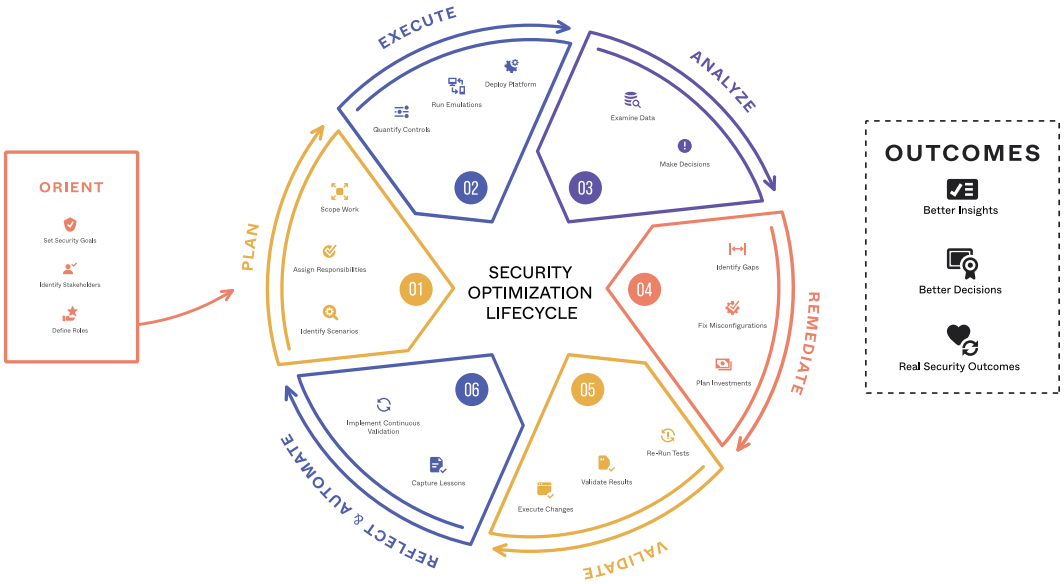

Figure 2. Organizations typically adopt the security optimization lifecycle in phases, as their processes and threat-informed defense infrastructure mature. AttackIQ offers blueprints that can guide your teams through this process.

Other Important Applications of MITRE ATT&CK

MITRE ATT&CK framework serves as the basis for other information security decisions and initiatives.

In addition to helping cyberdefenders discover gaps in the existing security infrastructure, the MITRE ATT&CK framework serves as the basis for other information security decisions and initiatives:

- **Developing cyberthreat intelligence (CTI).** Cyberthreats are a universal problem that demands collective and coordinated action. You can combine the CTI provided by the ATT&CK framework with the CTI that your team develops (either from its own forensic work or from external sources available either from vendors or open-source intelligence). You can then disseminate the CTI to your internal defenders and share it with HPH-based communities such as the Health Information Sharing and Analysis Center (H-ISAC), or with the more general cybersecurity community.

- **Security control analysis and selection.** When the time comes to invest in additional security technology, vendor specifications and even proofs of concept do not provide accurate assessments of how different options will work against real-world threats across your organization. Testing based on MITRE ATT&CK TTPs provides objective and demonstrable proof of performance.

- **Merger and acquisition onboarding.** As healthcare organizations merge, disparate security infrastructures can create easily exploitable gaps. Testing the effects of the merged infrastructure on security control performance — before the infrastructures are actually merged — can help to reduce the risks associated with the onboarding process.

- **HIPAA compliance.** HPH organizations typically document compliance using logs and reports from tools such as security information and event management (SIEM) and access management systems. Validating the performance of these systems using MITRE ATT&CK-based simulations, HPH organizations can be confident that their compliance reporting rests on solid ground.

- **Assessing red and blue team performance.** Even with MITRE ATT&CK-based security validation, red and blue teams still have important roles to play in security control optimization. In this context, comparing the results of the TTP simulations with red team efforts can reveal areas of improvement for the red team. Repeated simulations can also show how effectively blue teams have closed security gaps. The lessons learned can inform red team and blue team training processes as well.

Case Study

AmerisourceBergen

AmerisourceBergen uses the MITRE ATT&CK framework through AttackIQ to support its decisions to invest in new cybersecurity technology and to rationalize its deployment of security controls.

AmerisourceBergen is a pharmaceutical distributor serving pharmaceutical manufacturers, healthcare providers, and the animal health sector.

The company's cyberdefense and vulnerability management team wanted to institute procedures and technologies that would enable it to stay ahead of cyberthreats that could disrupt its supply chain operations. So, it started by hiring a team of threat hunters to identify security vulnerabilities in the company's network, data, and applications.

The team correlates its threat hunting and mapping activities with the MITRE ATT&CK framework. According to Kumar Chandramoulie, Vice President of Cyberdefense, Data, and Threat Management, MITRE ATT&CK is the best option for threat-centric security. "The MITRE ATT&CK framework provides an exhaustive list of areas to explore, with a lot of detail," he says, "and it helps our threat-hunting team structure their day-to-day operations."

AmerisourceBergen also deployed an assortment of sophisticated security technologies to protect its data and logistics applications. But it realized they needed a way to verify that the tools — and the way they were configured — were delivering the expected results.

AmerisourceBergen opted for the AttackIQ Security Optimization Platform to perform its breach and attack simulation, because it automates the testing process, and it was easy to deploy and use. Also, AttackIQ allowed the company to simultaneously evaluate the effectiveness of their security investments and provide the threat-hunting team with information about detected vulnerabilities in the security infrastructure.

The cyberdefense and threat-hunting team leverages the MITRE ATT&CK framework, as well as numerous other sources of threat intelligence that are relevant to its industry and business. After evaluating the threat intelligence they acquire, they turn to the AttackIQ platform to see whether it can simulate attacks from those threat actors. "If a nation-state is engaging in retaliatory attacks against U.S. businesses," Chandramoulie explains, "we will look at the threat actors associated with that nation-state and run simulations that we think represent the types of attacks they might use against us."

AmerisourceBergen also uses the MITRE ATT&CK framework through AttackIQ to support its decisions to invest in new cybersecurity technology and to rationalize its deployment of security controls. In effect, it is combining the breadth of knowledge from MITRE ATT&CK with the efficiency and objectivity of the AttackIQ platform to optimize the company's security program.

Conclusion

You must get an accurate picture of your risk surface and critical exposures, which requires adopting broadly accepted sources of data and methods of analysis.

"Managing risk—whether internal or third-party—requires focus. There are simply too many things to assess and do, giving rise to the endless 'hamster wheel of risk management.' A better approach starts with obtaining an accurate picture of your risk surface and the critical exposures across it."

– Health-ISAC[16]

The Health-ISAC cyberthreat intelligence community has got it right: you must get an accurate picture of your risk surface and critical exposures, which requires adopting broadly accepted sources of data and methods of analysis. The MITRE ATT&CK framework provides an essential source of data for evaluating the risk surface, while the AttackIQ Security Optimization Platform provides the tools for continuously and efficiently verifying the efficacy of the controls that aim to protect against the company's critical exposures.

[16] "Internet Risk Surface in The Healthcare Sector: Benchmarking digital risk factors facing healthcare institutions," RiskRecon, the Cyentia Institute, and Health-ISAC, accessed February 3, 2020.

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 identify 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 MITRE Engenuity's Center for Threat Informed Defense.

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