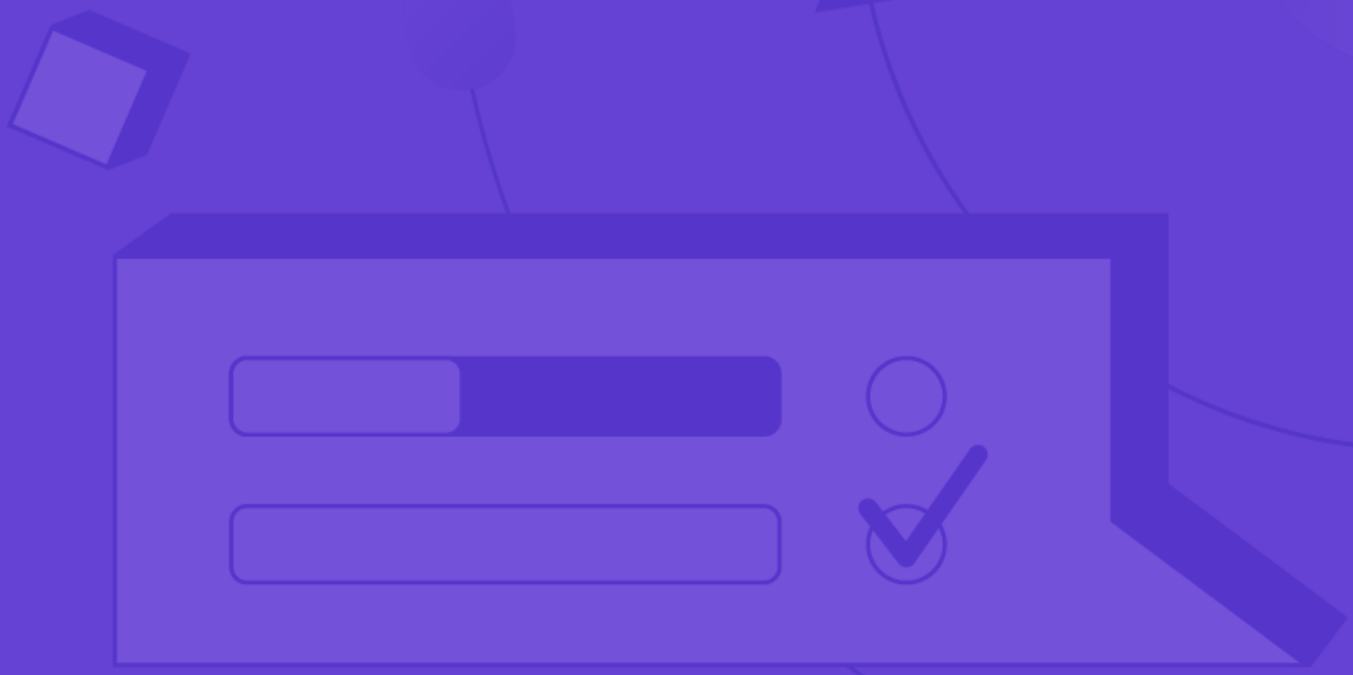
ATTACKIQ® + TheChertoffGroup

Case Study

The Chertoff Group Leverages the AttackIQ Security Optimization Platform to Deliver Compelling Security Service for Clients



After leaving office as the second United States Secretary of Homeland Security, Michael Chertoff realized that the security and risk management knowledge he had gained would be of significant benefit to the private sector. The Chertoff Group was therefore established to empower enterprises with security expertise, technology insights, and policy intelligence to help them build resilient organizations, gain competitive advantage, and accelerate growth.

David London, Managing Director within the Chertoff Group's cybersecurity practice, runs engagements that helps large enterprises understand and mitigate the threats posed by cyber threat actors. London explains: *"Our work includes cybersecurity assessments based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), as well as cybersecurity governance and risk management consulting. We arm clients with an understanding of their inherent risk profile and how this changes according to evolving threat behaviors, regulatory demands, and changes to their IT environment."*

In addition to mapping security threats, the Chertoff Group also helps organizations test their defenses against the threats most relevant to their business using the AttackIQ Security Optimization Platform. The platform assists the Chertoff Group in delivering service engagements as an independent, neutral service provider, and benefits their clients by giving them a higher level of fidelity around what kind of threat activity could potentially exploit their environment.

> *"The partnership with AttackIQ has supercharged our cyber risk service offerings. The company offers an evergreen, out-of-the-box solution for threat emulation and automated breach and attack simulation that is fully integrated with MITRE ATT&CK. That means it's easy for us to use, and that it's always up to date with the latest in adversary techniques and threat behavior."*
>
> – **David London**, Managing Director, The Chertoff Group

In Search of Precision and Validation

The Chertoff Group's approach to security assessments is born of the realization that security frameworks such as NIST CSF are not in themselves sufficient. *"NIST is a great framework for expressing a security program,"* says London, *"but you don't get the precision and validation around whether the security controls put in place by an organization are actually fit-for-purpose."*

London and his team have therefore built a powerful cyber diagnostic capability. Unlike traditional maturity assessments that move through a process of "identify, protect, detect, respond, and recover" along with associated controls, the Chertoff Group starts by building a threat-informed security model.

CUSTOMER

The Chertoff Group

LOCATION

U.S.

INDUSTRY

Security

HIGHLIGHTED SOLUTION AREAS

- MITRE ATT&CK® Evaluation
- Security Control Validation
- Threat Emulation

BUSINESS IMPACT

- Assists the Chertoff Group in delivering service engagements as an independent, neutral service provider
- Enables threat emulation and automated breach and attack response to help the Chertoff Groups' clients embrace a threat-informed defensive posture
- Helps the Chertoff Group's customers prove ROI in existing security capabilities and justify the business case for new investments
- Provides seamless integration with the MITRE ATT&CK® framework, improving on the efficiency and effectiveness of the company's threat emulation capabilities

London provides the context: *"The diagnostic threat model we develop for clients is aligned to the real-world adversary tactics and techniques listed in the MITRE ATT&CK® Knowledge Base. The framework allows us to build a model that reflects a client's sector, digital assets, and IT infrastructure. We then downselect threats using MITRE ATT&CK® to build a custom threat model for that particular client. Next, we apply a coverage overlay of prioritized protective and detective controls that organizations have in place to address threats that either are most likely to target them, or which are easiest to protect against."*

Calibrating Threat Emulation

Once the coverage mapping is complete, the Chertoff Group moves to threat emulation, which includes breach and attack simulation (BAS). In the past, London's team relied on open-source scripts and other tools to patch together the BAS capabilities required to put clients' controls to the test. The approach was sub-optimal, however. *"None of the tools we used were integrated with MITRE ATT&CK, which made them time consuming to apply and analyze,"* says London. *"The reporting was limited, and the overall usability of the system was inefficient."*

It was at this time that the company made the switch to the AttackIQ Security Optimization Platform. London comments: *"The decision to partner with AttackIQ was easy. The company offers an evergreen, out-of-the-box solution for threat emulation and automated breach and attack simulation that is fully integrated with MITRE ATT&CK. That means it's easy for us to use, and that it's always up to date with the latest in adversary techniques and threat behavior."*

Several other elements factored into the Chertoff Group's decision to use the AttackIQ Security Optimization Platform including its lightweight agent that works seamlessly with third-party systems, its intuitive interface and controls, and the straightforward reporting provided by the system.

> ***"We've had a lot of success with the AttackIQ Security Optimization Platform across client engagements, internal training, and also in identifying opportunities to further apply threat-informed defense in our own environment. The platform is an important tool for our business and a key component of our value proposition."***
>
> – **David London**, Managing Director, The Chertoff Group

Putting Security Controls to the Test

With the AttackIQ Security Optimization Platform in place, London's team now benefits from a more streamlined and effective approach to threat emulation. Once the threat model is complete, it is migrated into the AttackIQ Security Optimization Platform where it is applied within the environment for simulated attacks that mimic the top threats the client will likely face, or against the parts of the IT infrastructure that are most critical to the business or tempting to criminals. London adds: *"These simulated attacks that are aligned to the organization's customized threat model generates visibility into the effectiveness of their controls for a threat-informed defensive posture."*

The results of the simulations in the AttackIQ Security Optimization Platform are fed into the Chertoff Group's scoring methodology, which enables clients to understand the relative risk reduction value of their security controls at-a-glance. The Chertoff Group provides these scores along with detailed reporting derived from AttackIQ, which helps clients understand whether they are achieving a strong return on investment for their security programs and helps them make a business case for new investments.

The company also uses the platform to help clients improve the performance of security information and event management (SIEM) or centralized logging systems. The AttackIQ Security Optimization Platform helps these organizations understand the volume of alerts they receive and how they are triaged and prioritized. *"A big benefit of AttackIQ is that the platform works across both Windows and Linux servers, giving us broad coverage. The insights from AttackIQ help us show clients where in the kill chain they are most vulnerable and how they can shift left to identify malicious behavior more rapidly."*

Optimizing AttackIQ

The relationship between the Chertoff Group and AttackIQ is a two-way street. On occasion, AttackIQ's customers need help optimizing their security programs. When this happens, AttackIQ brings in the Chertoff Group to apply its diagnostic methodology and help ensure that the customer is getting the most value possible from their security investments.

"In cases where organizations don't have the resources to deploy hundreds of agents across their IT infrastructure, we can help them identify the assets most at risk. Sometimes, we help these businesses put their assets on rotation with the platform to ensure the broadest coverage possible at the lowest cost," London explains.

Leveraging AttackIQ Security Optimization Platform Internally

In addition to helping clients improve their security posture, the Chertoff Group uses the AttackIQ Security Optimization Platform internally. It uses the platform on its own security controls to identify opportunities to further strengthen defensive posture and to train new employees on the system and its functionality. London comments: *"When we use AttackIQ for training, we achieve greater visibility into our own cyber hygiene and countermeasures. That helps us further apply threat-informed defense internally, especially as adversary tradecraft evolves."*

London concludes: *"We've had a lot of success with the AttackIQ Security Optimization Platform across client engagements, internal training, and internal controls assurance. The AttackIQ platform is extremely valuable for our business and a key component of our value proposition."*

ATTACKIQ

U.S. Headquarters
171 Main Street, Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com