ATTACKIQ®

Case Study

Leading Bank Strengthens Security Posture with AttackIQ

Breach and Attack Simulation Identifies Critical Security Gaps

Executive Summary

This case study examines the successful deployment of AttackIQ Enterprise at a prominent banking institution. AttackIQ's Breach and Attack Simulation (BAS) Enterprise and Flex platforms prove instrumental in identifying critical security vulnerabilities within Microsoft Defender for Endpoint (MDE), potentially averting a major cyberattack and data breach.

The Superhero Challenge

The banking and financial sector remains a prime target for cybercriminals due to the vast amounts of sensitive data and valuable assets it holds. In 2023 and 2024, banks and financial institutions faced a dynamic and evolving landscape of cyber threats.

In this case study a leading bank was undergoing a significant technological transition, moving from McAfee ePO to Microsoft Defender for Endpoint (MDE). However, concerns arose about the effectiveness of MDE in providing adequate endpoint protection. The bank recognized the critical importance of a robust security posture, especially given its prominent role in the financial sector.

Continuous Security Validation Steps Up

To address these concerns and ensure the effectiveness of their new endpoint protection solution, this financial institution deployed AttackIQ Enterprise. This advanced security platform offered a comprehensive approach to testing and validating security controls against real-world threats. The security team utilized the platform to conduct comparative assessments between MDE and McAfee ePO.

The results of this assessment included surprising data:

- **MDE Gaps Discovered**
  During initial testing, AttackIQ Enterprise revealed critical gaps in its protection: the endpoint solution was failing to block malware samples on the test devices. This included dangerous malware such as Locky, Petya, and WannaCry. This alarming discovery raised significant concerns about the bank's overall security posture.
- **Escalation & Collaboration**
  The findings prompted discussions with Microsoft product owners, leading to a priority case investigation. The financial institution immediately escalated the issue to Microsoft, initiating a high-priority investigation. The close working relationship and excellent collaboration between the bank and Microsoft was essential in addressing the problem promptly.

Continuous Security Validation Steps Up (cont.)

- **Widespread Risk Identified**
  Further testing across the bank's extensive network of devices, conducted using AttackIQ's Flex product, confirmed that the coverage gaps were widespread, potentially affecting all of the many thousands of MDE-protected endpoints in use by the bank. This alarming discovery underscored the urgency of the situation and the potential consequences of a successful cyberattack.

- **Root Cause Analysis**
  A thorough investigation revealed that the root cause of the issue was a misconfigured legacy setting for Real-Time Protection within MDE. This setting, which was set to block outgoing traffic only, was preventing the endpoint protection solution from effectively blocking incoming threats.

- **Remediation & Improvement**
  Microsoft engineers corrected the configuration, resulting in a significant improvement in MDE's effectiveness. Microsoft engineers quickly identified the misconfiguration and implemented the necessary corrective actions. This remediation process resulted in a significant improvement in MDE's effectiveness, mitigating the immediate risk posed by the vulnerability.

- **Additional Discoveries**
  The investigation also uncovered other potential vulnerabilities, including disabled MDE notifications and potential command prompt access issues. These findings highlighted the importance of ongoing security assessments and the need for continuous security validation.

- **Enhanced Security Posture**
  AttackIQ's proactive testing validates critical vulnerabilities, prompting corrective actions and strengthening the financial institution's overall security posture. By proactively identifying and addressing these critical vulnerabilities, the bank significantly enhanced its security posture. The successful resolution of the MDE issue demonstrated the value of AttackIQ's platform in preventing potential breaches and protecting sensitive customer data.

Misconfiguration – A Closer Look

Often the gateway to a successful attack is a vulnerability inadvertently exposed by a misconfiguration. Misconfiguration refers to errors or deviations from the intended configuration of systems, applications, or network devices. Misconfiguration, often overlooked or underestimated, is a significant contributing factor to successful cyber intrusions, data breaches, cyberattacks, and other attacks on financial institutions. These misconfigurations can create vulnerabilities that malicious actors can exploit to gain unauthorized access and compromise sensitive data.

Misconfiguration can grant unauthorized users access to systems and data they should not have access to. Misconfigured data storage and transfer mechanisms can allow attackers to exfiltrate sensitive data from an organization's network.

To prevent misconfigurations and reduce the risk of cyberattacks, organizations should implement a BAS technology solution for continuous security validation. Additionally, establishing clear policies and procedures for configuring systems and applications, along with promptly applying security patches and updates, are essential best practices.

BAS Benefits for the Bank

The timely identification and remediation of the MDE vulnerability through AttackIQ's testing likely prevented a large-scale malware attack. Such an attack could have had severe financial and reputational consequences for the bank. The compromised endpoint protection could have allowed malicious actors to gain unauthorized access to sensitive customer data, leading to data breaches, financial losses, and regulatory fines. Additionally, a successful attack could have damaged the bank's reputation and eroded customer trust.

Moreover, AttackIQ provided the bank with a comprehensive view of their security posture, enabling them to make data-driven decisions and identify areas for improvement. By emulating real-world attacks, AttackIQ helped the bank understand the effectiveness of their existing security controls and identify weaknesses that could be exploited by malicious actors. This increased visibility allowed the bank to prioritize risk mitigation efforts and allocate resources more efficiently.

ATTACKIQ ENTERPRISE

AttackIQ Enterprise is our flagship product for large banks and financial institutions designed to help banks and financial organizations to validate and improve their security posture through Breach and Attack Simulation (BAS). AttackIQ Enterprise is a comprehensive breach and attack simulation platform that provides maximum flexibility and customization in testing with on-demand support.

Fully Customizable Testing.
Test continuously with both on-demand and fully automated testing.

Test at Scale, in Production.
Testing that is safe, realistic, and can be executed seamlessly and at scale over large enterprise environments.

Detailed Reporting.
Detailed metrics into security control performance with actionable mitigation guidance to close gaps quickly and improve performance.

MITRE ATT&CK Aligned.
Close product alignment with MITRE ATT&CK means unparalleled emulation realism and results that are actionable, easy to understand, and aligned at every step of the way with industry best practices.

Detection Engineering.
Native integration with your security products enables you to continuously validate and refine security control detections with results from real-world attack scenarios

Expert Consulting.
On-demand access to AttackIQ's experienced team of security operations consultants and adversary researchers to build your testing strategy and implement best practices.

ATTACKIQ
U.S. Headquarters
171 Main Street, Suite 656
Los Altos, CA 94022
+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 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.

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