FireEye and SafeBreach

Weaponizing Threat Intelligence Via Breach Simulations

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

SOLUTION COMPONENTS

The joint integration includes the SafeBreach platform — comprising the management platform and simulators — and the FireEye iSIGHT threat intelligence solution:

- **SafeBreach Management** - The SafeBreach centralized management system incorporates the complete Hackers' Playbook of breach methodologies, and manages a distributed network of breach simulators from a centralized location.
- **SafeBreach Simulators** - The SafeBreach simulators perform the role of the attacker, simulating traffic within the cyber kill chain.
- **FireEye iSIGHT Intelligence** - iSIGHT reports identifying malicious domains, malicious downloads, and malicious URLs are automatically translated into actionable SafeBreach breach methods.

OVERVIEW

It's clear that the threat landscape has evolved rapidly over the last couple of years. Not only are threats more targeted and using more sophisticated techniques, but attackers are innovating and collaborating at a much faster rate than defenders. In fact, many attackers are reusing malware and techniques, particularly when they are successful, to bypass newly updated security measures.

As more and more attacks occur, defenders are depending on threat intelligence to get early notification of attacks. By analyzing the latest indicators of compromise, organizations can act upon attacks targeting their industry and react quickly before they become a victim.

THE CHALLENGE

The challenge for organizations is how to operationalize and weaponize this threat intelligence data — from motivation and intent of adversaries, their campaigns and technical indicators, the malware used, and the vulnerabilities being exploited. In a recently published ESG research report titled, *Threat Intelligence and Its Role Within Enterprise Cybersecurity Practices*, 19% of organizations surveyed said they had difficulty analyzing and operationalizing threat intelligence data for risk management or incident response.

THE INTEGRATED SOLUTION

The SafeBreach integration with FireEye iSIGHT Intelligence aims to address these issues. The solution enables organizations to consume FireEye iSIGHT Intelligence indicators of compromise and transform them into hacker breach methods that can be executed within an environment. It allows organizations to proactively see which attacks are applicable in their environment in a practical, actionable manner.

HOW THE JOINT SOLUTION WORKS TOGETHER

A Better Approach To Weaponizing Threat Intelligence

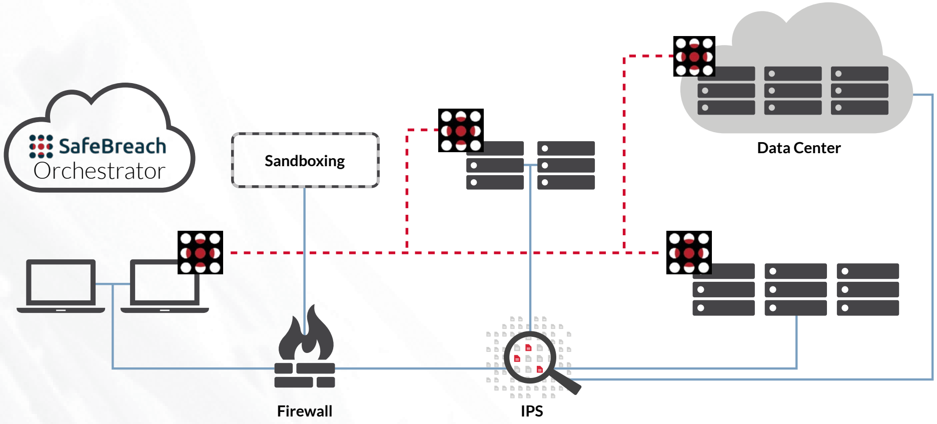
Today, threat intelligence feeds are typically sent to security information and event management (SIEMs). Thus, operationalizing threat intelligence and deriving value out of threat intelligence data today is very much dependent on specialized analysts. Watching and waiting to react as a defense is untenable. Simulating breach methods based on real-time threat intelligence enables organizations to proactively find weak spots in the specific context of their business and infrastructure.

FIREEYE PRODUCT

FireEye iSIGHT Intelligence (API version 2.0 and higher)

SAFEBREACH PRODUCT

SafeBreach Continuous Security Validation platform – July 2016 Neptune release



There are a number of benefits in simulating threat intelligence feeds:

- Better understanding of which indicators of compromise impact an organization
- Proactively address attacks that are being seen by the industry
- Predict variations of attacks being seen in the industry
- Improve analyst detection and response within SOC team

In this integration, the organization should have an existing license and API keys from FireEye iSIGHT Intelligence. Once the API key is input in the SafeBreach dashboard, breach methods are automatically generated. Breach methods powered by FireEye iSIGHT Intelligence feeds are designated in its own section on the SafeBreach dashboard, and clicking on the breach methods references the specific threat intelligence reports that are being simulated.

SafeBreach simulations enable organizations to not only put specific intelligence-based campaigns into motion in their environment but also assists in predicting variations of these attacks so that enterprise can adjust their security protection strategies to compensate.

THE VALUE OF THIS PARTNERSHIP

The SafeBreach and FireEye iSIGHT Intelligence solution enables the average organization to understand how applicable indicators of compromise would play out in their environment in a practical, actionable and proactive manner.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 2,700 customers across 67 countries, including over 157 of the Fortune 500.

ABOUT SAFEBREACH

Funded by Sequoia Capital and investor Shlomo Kramer, SafeBreach is a pioneer in the emerging category of continuous security validation. The company's groundbreaking platform provides a "hacker's view" of an enterprise's security posture for total and continuous security assessment, validation and reporting. SafeBreach automatically executes breach methods with an extensive and growing Hacker's Playbook™ of research and real-world investigative data. For more information, visit www.safebreach.com or follow on Twitter @SafeBreach.

For more information contact CSC@fireeye.com.