FireEye
SECURITY REIMAGINED

WHITE PAPER

CLOSING THE SECURITY EXPERTISE GAP

Closing the Security Expertise Gap

Attackers are humans, not malware. As security teams implement new defenses, attackers change their tactics. It's a game of cat and mouse. One essential – but often overlooked – ingredient to an effective defense is expertise.

Technology Is Only the First Step

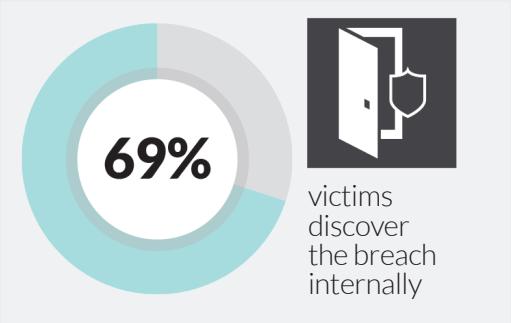
Security organizations are beginning to realize what it takes to keep up with advanced threat actors. To close the gap, security leaders are making significant investments in technology to help detect the presence of these advanced attackers on their networks.Despite these investments the attacks continue. And they continue to succeed. Security teams are beginning to recognize that while detection is an important first step, to effectively find and stop attackers you also need to be able to prevent, analyze and respond to attacks. This requires security expertise. However, recruiting, hiring and maintaining a top notch security staff capable of running the latest technology and stopping advanced attackers is a significant challenge.

Security Is Not a Technology Issue

Security budgets are tight. But attracting and retaining the right expertise can be even more challenging. Staffing and resource constraints can hinder even the most effective security strategies. A recent report from Mandiant, a FireEye company, noted that, despite having threat detection technology in place, over two thirds of organizations failed to detect they were breached using internal resources. It took an external entity to notify them.

The same study reported that even in the cases when an organization did discover the breach themselves, the median number of days that attackers were able to remain undetected on their networks was 205 days.[1] With network

Figure 1:
Victims often fail to detect breaches on their own.



[1] http://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

monitoring devices detecting and producing thousands of alerts each day, how does a diligent CISO identify the alerts that matter from the thousands of alerts generated?

The Power of Real-Time Intelligence

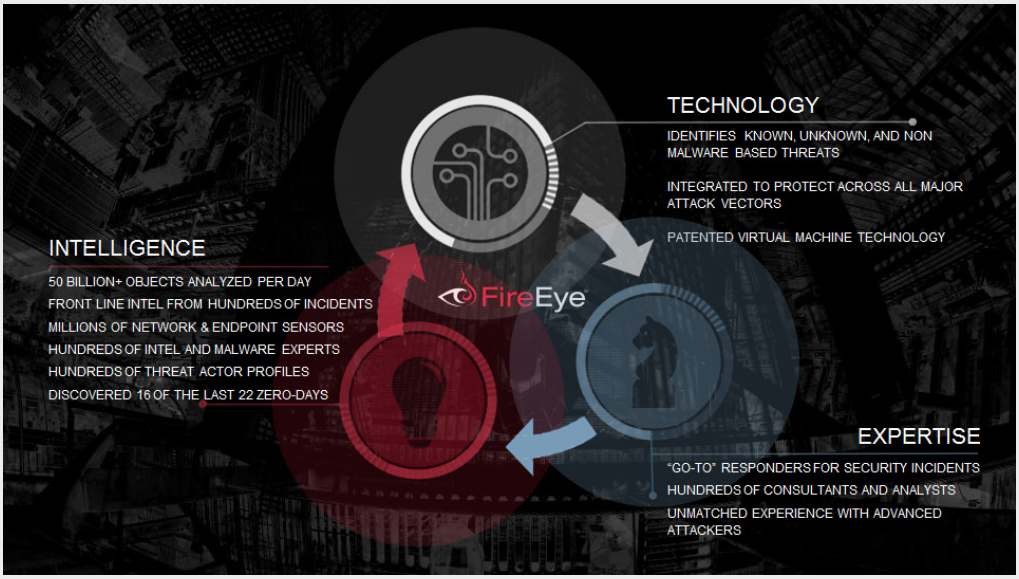
As the volume of alerts increases, it is more important to understand what the alerts actually mean. Which alerts matter most? Which deserve immediate follow up and which can be deprioritized? Context matters. When you know who the attacker is and what they are after you can better assess the risk they pose. Better yet, if you understand their tactics, you can begin to anticipate their next step.

To find and stop attackers, security teams need to be able to not only detect attacks but also determine their priority and eliminate false positives. Attackers are continually adjusting their tactics to evade detection. Effective intelligence that provides clarity about attackers' methods is vital to reduce the impact of security breaches.

Intelligence alone, however, is also not enough. Security teams need a way to apply that intelligence across their endpoints, logs and networks. By establishing a baseline of normal activity in an environment they can begin to proactively hunt for deviations from this baseline to identify anomalies that could indicate attackers are present in their environment.

When you know who the attacker is and what they are after you can better assess the risk they pose.

Figure 2:
An effective security solution should blend intelligence, technology, and expertise.



Defining the Solution

So how does a CISO address these staffing and intelligence needs while proactively hunting for advanced threats, all while on a limited budget? Let's outline what a potential solution would look like:

1. **Expertise:** An effective solution must be able to provide your organization with the expertise and staffing necessary to proactively monitor your network for the presence of advanced threats. In the event of a breach, the solution should provide your organization with responders that have experience with advanced attackers.

2. **Intelligence:** This solution should provide your staff with the necessary context about potential threats that your security environment may face. This intelligence should be comprehensive and vetted by professional malware and intelligence experts.

3. **Technology:** Yes, as the title of this piece suggests, technology is a critical foundation on which your security architecture is built. It must be able to identify known, unknown and non-malware-based threats. And whatever technology you deploy should also be able to protect your organization across all major attack vectors like web, email, endpoint and mobile.

FireEye as a Service

FireEye as a Service is a new solution that brings together the expertise, intelligence, and technology required to monitor threats, find attackers at any stage of an attack, and respond aggressively before attackers complete their mission.

It's a subscription-based service that provides continuous threat protection to help enhance your security team. It augments the value of the FireEye Security Platform with 24x7 expertise and monitoring from FireEye expert analysts.

FireEye as a Service customers receive tailored guidance about the threats that pose the greatest risk. But it doesn't just tell you when you are being attacked. This intelligence can also tell you who is behind the threat, how you should respond and what you need to do to contain it.

With multiple subscription options, FireEye as a Service provides a range of services that complement your current security approach. FireEye as a Service enables you to align the chosen service(s) with your team's skills and risk tolerance.

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. FireEye has over 3,100 customers across 67 countries, including over 200 of the Fortune 500.

To learn more about how FireEye can help protect your organization, visit fireeye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**