Automated And Orchestrated Response

Filtering Out Noise, Freeing Up Resources and Shutting Down Threats at Speed.

By **Tony Cole**
Vice President and Global Government CTO
FireEye, Inc.

> All of this is a real game changer for defenders. They can now understand attacks before they happen through pre-breach threat intelligence, tie that in with machine-led threat intelligence and post breach threat intelligence, and integrate that with courses of action that automate response.

Perhaps the most common problem I hear about from customers these days is that security operations teams are overwhelmed with alerts and addressing every single one of them is eating up valuable resources.

As a result, defenders are unable to stay ahead of threats and may miss attacks altogether. Fortunately, not all is lost. There are tools and tactics that can be used to filter out the noise so security teams can more quickly turn their focus to important critical issues.

One of the first things an organization can do is look at the tools they already have and then establish a strategy to integrate those tools for incident response thorough security orchestration.

This can allow security teams to get more value out of their tools by building courses of action for all the daily mundane security tasks that must be accomplished and get in the way of real work, which involves focusing on the attacks that matter.

As the enterprise continues to evolve, orchestration can allow more flexibility through stitching together new capabilities on a frequent basis.

FireEye acquired Invotas because their security orchestration tool provides that capability, allowing defenders time to step outside the busy alert cycle so they can follow up on the more critical and possibly impactful alerts.

Actionable Data Prior To An Attack

Gathering threat intelligence from behind enemy lines can also help organizations stay ahead of attacks. This is something pivotal to militaries around the globe, yet the security industry doesn't do it nearly as well.

iSIGHT Partners, on the other hand, has built their entire company around gathering enemy intelligence. They have hundreds of analysts around the globe "living" inside attacker camps, and that is the very reason why the company is now part of FireEye.

iSIGHT Partners gives our customers a new perspective — one directly from the attackers' point of view. Suddenly, we know what tools will possibly be used against us, why we're a target, and how our systems will be broken into – all before the attack is executed. We have valuable information that we can use to stop an attack that hasn't even been launched yet.

Actionable Data Prior To An Attack

The threat actor's perspective combined with our machine-led intelligence from real-time breach alert detection via our FireEye MVX driven platform provides us with extremely useful and actionable data even prior to an attack.

However, it's important to keep in mind that breaches will inevitably happen since — as we all know in the security industry — nothing will stop a determined and well-resourced adversary. This is where our Mandiant Incident Response team comes into play. Mandiant teams come in and quickly investigate and mitigate the damage from an attack.

Throughout the incident response, they are gathering more threat intelligence that we can tie in to our threat actor intelligence and our machine-led intelligence. By combining this data with information from our existing legacy security tools, we can now better automate the courses of action for response.

Game Changer

All of this is a real game changer for defenders. They can now understand attacks before they happen through prebreach threat intelligence, tie that in with machine-led threat intelligence and post breach threat intelligence, and integrate that with courses of action that automate response. As a result, they can stop more threats dead in their tracks — and more quickly too — without having to use up most of their resources. This allows us to revamp our security strategy with an 'Intelligence-led' perspective and truly understand the risk to our environment.

SOLUTION FOCUS

Protecting Before, During and After a Breach

The FireEye Adaptive Defense approach to cyber security enables you recognize and apply the right mix of technology, intelligence, and expertise to protect against advanced persistent threats (APTs). Your security solution must be able to detect, prevent, analyze, and respond to both known and never-before-seen cyber attacks. Only Adaptive Defense lets you pick the perfect combination of industry-leading FireEye technology, real-time threat intelligence and proven expertise to meet your needs.

Technology

Protect your email, network traffic, and content files on mobile, endpoint, and network devices from never-before-seen malware. At the core of all FireEye products is the patented Multi-Vector Virtual Execution (MVX) engine. It detonates and analyzes suspected threats in a fully-secured, realistic virtual environment. Together, FireEye technology raises the bar when it comes to identifying unknown threats and protecting your organization before, during, and after an attack.

Intelligence

Quickly identify, prioritize, and respond to important security alerts with FireEye intelligence. Attack and attacker data is collected and constantly updated from millions of virtual machine deployments and decades of incident response cases. The FireEye Labs teams track and identify the latest attacker behaviors and technical innovations and post their findings to benefits the entire security community

Expertise

Extend your in-house team with FireEye experts who have front line experience analyzing environments for everyday threats and battling breaches that might otherwise make headlines. With a continuous monitoring service, we proactively hunt for threats in your environment and instantly help respond to incidents at your request.

Modern cyber security is not just technology you can "set and forget." Attackers are clever, technology is complex, and experts are in short supply. FireEye puts insight, power, and talent in your hands to give you agile, flexible, and integrated protection. Get started now to evolve your cyber security and protect your organizational assets.

To read the full article visit www.onthefrontlines.net**.**