SECURITY ORCHESTRATION: Best practices for any organization

WHITE PAPER

THE NEED FOR ORCHESTRATION

Cyber-attack volume has never been higher and if your defenses can't keep up, you dramatically increase your risk of a breach. Skilled attackers can access the computing power they need as well as the backbone of the fastest digital delivery networks. They can test and adapt to your network defenses. Most security operations centers (SOCs) must contend with a huge volume of alerts, stressing understaffed teams. Therefore, most organizations with traditional programs that rely on manual intervention and containment face an asymmetric fight.

Faster responses can make the difference between a minor attack and a major breach.

The promise of orchestration

Cyber security professionals are required to respond quickly and flawlessly to combat potentially devastating threats. But they walk a tightrope between time spent on mundane tasks and higher value investigations that lead to a mitigated threat. Many analysts spend most of their time on repetitive activities that require frequent shifts between multiple, disparate tools to triage alerts using standard corrective actions for known issues.

Security orchestration levels the playing field by accelerating and simplifying the threat response process. It brings together disparate technologies and incident handling processes into a coordinated set of security actions and operational processes. A properly deployed orchestration solution ultimately buys time for your security professionals to focus on higher priority tasks, improves response times, reduces risk exposure and maintains process consistency across a security program.

But to achieve the promise of orchestration you must avoid misconceptions and flawed approaches when evaluating and adopting an orchestration strategy.

Every organization can benefit from orchestration

There are two significant misconceptions around orchestration:

- The entire security process, from end to end, including logic, must be outsourced.
- Only security mature organizations can find benefit from orchestration.

First, orchestration is not about outsourcing your entire security process. It's about finding the best use cases that fit your organization's current level of expertise, process maturity and proclivity or comfort with automating processes.

Second, there is a common, basic set of activities that can be automated. Most organizations will be able to immediately identify and gain value from orchestration.

Best practices for orchestration

In the end, best practices don't revolve around whether you can automate or orchestrate operations. It's when you choose to automate and orchestrate operations and how you go about doing so.

Because of the initial investment required, you must choose your battles carefully and expend your resources deliberately.

- Bring all your information, capital and human resource together so you can establish what you have to work with.
- Clearly identify high-value, frequently repeated tasks for automation so you can free your experts to focus on more important, non-automatable tasks
- Ensure that you are detailing outcomes to work towards when orchestrating activities, so that you pursue simplification and optimization as well as automation.

Be strategic and practical about what to automate.

Integrating automation requires that a task be broken down, analyzed and codified. When selecting tasks to automate, choose wisely and avoid tasks that are unnecessary or require human know-how to drive each successive step. Such tasks are often not worth prioritizing for automation. Instead, focus on tasks that deliver high-value output and are either repeated often or have a repetitive steps.

Focus on tasks that deliver high-value output and are either repeated often or have a repetitive steps

Ensure that your data is compatible and meaningful when it is brought together.

As organizations attempt to centralize their security intelligence and operations, it is not enough to simply feed the data from existing tools to a central location. In fact, simply bringing all your data feeds together may exacerbate the decision making process. It is far more effective to gather, correlate and integrate data from different sources for correlation and analysis using playbooks. These playbooks, which document processes programmatically and accommodate contingencies, must be designed to generate decisions as outcomes or shrink the problem to be solved.

Vet your security processes before pursuing efficiencies

Optimizing operations requires that we ask questions such as:

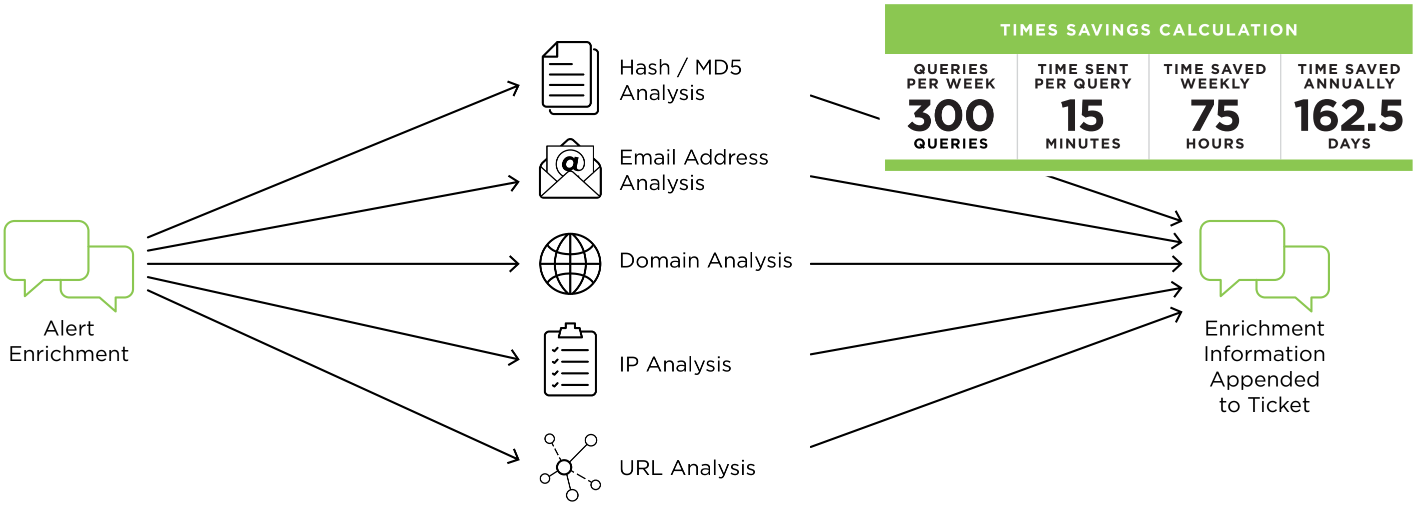
- When, if ever, should we perform the task?
- What is the eventual outcome of the task?
- How will we use the output of the task to achieve the outcome?
- How else might we achieve the outcome?
- Are we using the least possible number of steps to achieve the outcome?

Core orchestration use cases

Alert enrichment

Because most security teams receive a large volume of alerts from their installed base of security products, they need to prioritize their efforts. Ideally, they would focus their attention on alerts that represent a greater risk.

The most common approach they take is to conduct a quick alert analysis to determine if an alert contains email address, domain, IP, URL or other indicators that are known to be malicious. Immediately after receiving an alert, they usually rely on a consistent, repeatable sequence of queries and actions. These steps can be easily automated before a human actually needs to be involved in the process.



QUERIES PER WEEK	TIME SENT PER QUERY	TIME SAVED WEEKLY	TIME SAVED ANNUALLY
300 QUERIES	15 MINUTES	75 HOURS	162.5 DAYS

Figure 1. Alert enrichment

Threat intelligence, gathered from multiple disparate sources, is at the heart of alert analyses. Domain research may use WhoIs lookups. Threat intelligence such as VirusTotal or FireEye iSIGHT Intelligence may be a first stop for malware or attacker information. IPs and email addresses may have to be checked against threat libraries.

These aren't necessarily complex searches, but they take time. Normally, analysts must manually log into each site and conduct the research themselves.

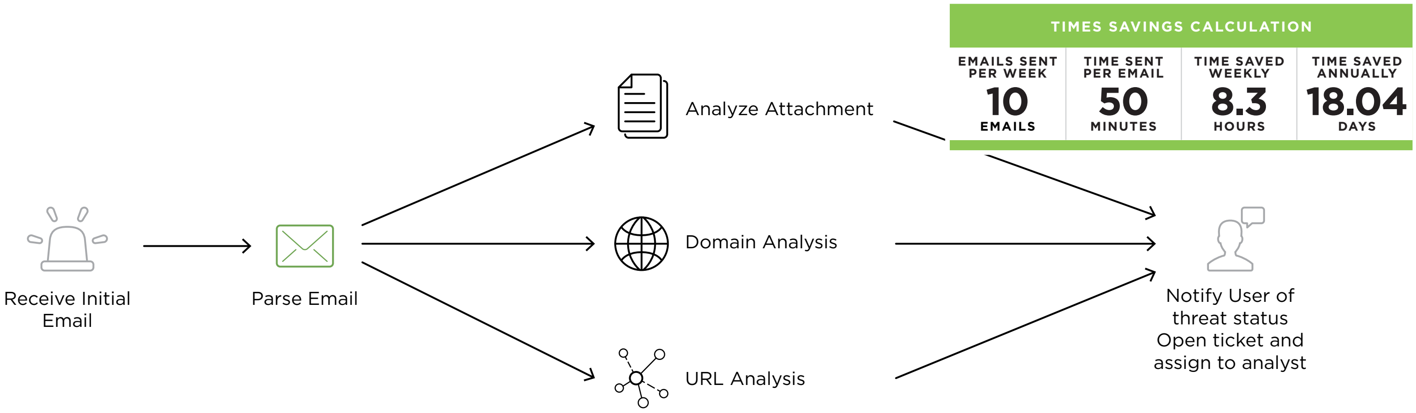
As part of the orchestration process, automation can allow a machine to receive an alert, access the appropriate database, conduct an automated search and finally bring normalized data together on a single screen for an analyst to review and synthesize. These tasks, when automatically performed and centralized, can take seconds instead of minutes.

If we assume IT must fulfill 300 queries per week at 15 minutes per query, that's 75 hours saved per week. This means that orchestration in such circumstances can allow teams to retask up to two analysts to higher value activities.

Alert analysis steps can be easily automated before a human actually needs to be involved.

Suspicious email management

Most organizations allow their employees and network users to report potentially suspicious users to an email alias. A security analyst then conducts an analysis to determine whether the email actually represents a threat. They must often parse the email and then analyze individual components. For most organizations, the immediate steps after a suspicious email is received are identical and repeatable. These steps can be easily automated before a human actually needs to be involved in the process.



TIMES SAVINGS CALCULATION			
EMAILS SENT PER WEEK	TIME SENT PER EMAIL	TIME SAVED WEEKLY	TIME SAVED ANNUALLY
10 EMAILS	50 MINUTES	8.3 HOURS	18.04 DAYS

Figure 2. Abuse mailbox

An analyst can take 20 or more minutes to dissect the email, analyze its source, links and attachments and then take any corrective action. Users at larger organizations can report hundreds or even thousands of email messages every week to their IT department as spam or phishing attempts. Clearly, it's not possible or practical for the IT security function to analyze this volume of work, let alone maintain communication with the end user to reward their participation in the security process.

The process of optimization might require analysts to document the process in detail, identify all intelligence sources used to assess threats and provide context, provide a library of email templates to support user communication and codify any new threat intelligence to help analyze future emails. Then they would need to prioritize and properly sequence these activities to generate a more automatable process:

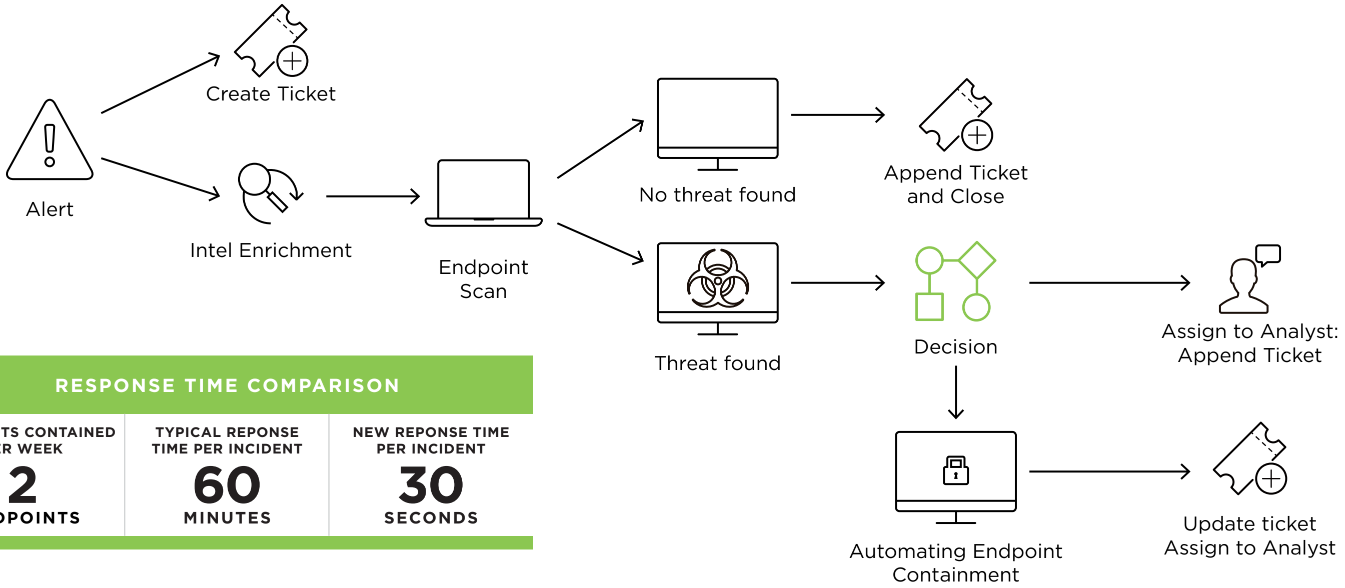
- End user submits suspicious email to IT for review.
- Orchestration engine picks up suspect email. Sends a thank you notification to submitter to acknowledge investigation has started. Orchestration engine parses email and begins to check URLs, IPs and attachments.
- If a known threat is identified, the system sends a thank-you to the user and begins to take steps to automate the process of quarantining such messages before they reach other users.
- If a potential or unknown threat is identified, an analyst is alerted to follow up.

This can save analysts an average of 50 minutes per email. Every 10 emails the system analyzes converts to a full workday saved.

By using orchestration, an IOC that might take 60 minutes to investigate manually can be researched in 30 seconds

Endpoint containment

Alerts require immediate host context. An analyst will normally examine the alert to determine the presence of any indicators of compromise at the endpoint. Then they determine whether the endpoint should be quarantined to mitigate further risk. The queries used by the analyst are repeatable and the expected responses are limited. Performing them manually extends the time that a risk remains active. These steps can be easily automated before a human actually needs to be involved in the process.



RESPONSE TIME COMPARISON		
ENDPOINTS CONTAINED PER WEEK	TYPICAL REPONSE TIME PER INCIDENT	NEW REPONSE TIME PER INCIDENT
2 ENDPOINTS	60 MINUTES	30 SECONDS

Figure 3. Endpoint containment

Indicators of compromise (IOCs) can be generated by multiple sources — network, email and other security products — and there are many such indicators. Multiply these by the hundreds or hundreds of thousands of endpoints in an organization and the task of correlating alerts with IOCs at the speed required to respond to threats becomes undeniably daunting.

With task automation, when an IOC alert is generated, the orchestration process can instantly compare the alert to the available library of IOCs and determine whether:

- There is no threat
- The endpoint should be contained
- The issue should be escalated to an analyst with full context for further action.

By using orchestration, an IOC that might take 60 minutes to investigate manually can be researched in 30 seconds — leaving sufficient time to mitigate any potential damage from a genuine threat.

Your level of orchestration

Orchestration can significantly benefit your security program, regardless of its level of maturity. Many basic, accessible and common orchestration opportunities exist. As you pursue them, several best practices will become apparent. You must achieve a deep understanding of your security environment, resources, risks and security goals. By bringing this knowledge together, it becomes easier to identify high-priority tasks that you can easily automate. This automation generates high-value outcomes such as reclaiming time for your security experts and reducing the dwell time of dangerous cyber attacks. And as you get better at selecting your outcomes strategically, you can simplify and optimize your security program to improve your overall security maturity.

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,600 customers across 67 countries, including more than 40 percent of the Forbes Global 2000.

© 2017 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc.
All other brands, products, or service names are or may be trademarks
or service marks of their respective owners. WP.ASO.EN-US.042017