What is Security Automation?
A Guide for an Evolving Landscape

OVERVIEW

Security automation is all the rage right now. According to a recent ESG survey, 91% of survey respondents said that their organization's spending on incident response automation will increase over the next two years. But with the popularity comes ambiguity—many vendors tout themselves as automation, but they all automate different facets of cyber analyst processes.

In this guide, we'll propose the ideal definition of security automation and its relevant requirements. We'll then review current solutions in the market to determine the pros and cons associated with automating the cyber incident response process.

Table of Contents

Defining Security Automation

Since security automation is a newly emerging market, definitions can vary significantly from one vendor or thought leader to the next. Barak Klinghofer, CPO at Hexadite, recently sat down with Lisa Musthaler from Network World for a deep dive into security automation. He defined security automation as the active process of the following:

1. **Mimicking the ideal steps a human would take to investigate a cyber threat:** Not simply providing insight or assisting, but truly mimicking the steps and logic a cyber analyst would take during an investigation.
2. **Determining whether the threat requires action:** Beyond just detonating something in a sandbox or running it against threat intelligence, automation will use these results to question the evidence and inform the investigation—just like a SOC analyst would
3. **Performing necessary remediation actions:** This is more difficult than it sounds, because there are many possible actions that could be taken. An automation solution must be able to handle as many use cases as possible in the same manner a human would.
4. **Deciding what additional investigations should be next:** Many automation tools stop after the first few steps, and it's up to a cyber analyst to go a step further and determine whether or not the threat was removed and if it's still a risk to the organization.

MIMICKING IDEAL STEPS A HUMAN WOULD TAKE TO INVESTIGATE CYBER THREATS

Whenever a detection system finds a potentially malicious threat, it kicks off an alert. In organizations not using automation, that alert is sent to a cyber analyst for follow-up. Unfortunately, most organizations receive 500 or more alerts per day, leaving analysts with no possible way to investigate all of them. In most cases, an analyst can perform roughly 8-10 full investigations per day, making analysts prioritize which alerts are worthy of attention.

In an ideal scenario, a cyber analyst would rigorously investigate every alert from all detection systems regardless of priority. In fact, looking at any of the high-profile data breaches in the past decade shows that in nearly all cases, a detection system created an alert about malicious activity but the company did not have the manpower to investigate. In our opinion, prioritization is just a conscious decision about what you are willing to ignore.

If we are to put prioritization and human capacity aside, the following are the ideal steps a cyber analyst would take to investigate a cyber threat:

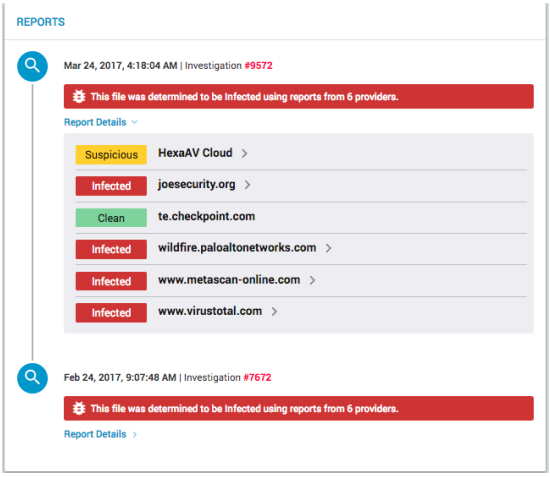
1. **Investigating the endpoint –** The first step after receiving an alert is to access the endpoint in question to determine whether the threat is still present. To use the most basic example – an AV alert about malware – the analyst would check the endpoint to see whether the detection system has eradicated the threat. While an antivirus application may have quarantined a file, there may still be running processes and loaded modules that remain active. The symptoms may have been resolved, but the cause of the infection may still be present.

   Investigating the endpoint brings its own set of challenges:

   a. **Permission to access –** The first challenge is having the requisite access rights to be able to get on the endpoint to begin investigating. In some cases, an analyst must seek permission to be able to begin an investigation based on access roles.
   b. **Remote users –** In an increasingly mobile world, users are no longer bound by physical locations or networks. As I write this, I am on a laptop on a train, not connected to a corporate network, accessing the internet through a hotspot. If an AV or EDR detected something suspicious on my machine and kicked off an alert to a security analyst, it would be very difficult for them to immediately access my laptop to begin investigating.
   c. **Endpoints that are powered off –** We recently spoke with a multinational with security operations in Australia and the majority of users in the United States. By the time they started to investigate an alert about a U.S. endpoint, the machine was off, causing massive delays.
   d. **Endpoints not in Active Directory –** Finally, when users work from a machine not in a directory service, finding and accessing that endpoint becomes nearly impossible.

2. **Gathering Additional Data –** Most companies have implemented a SIEM solution and a log repository to provide additional correlation and context around a potential threat. Once an analyst has accessed the endpoint to determine whether the threat is still active, they will then gather more data from the network resources to understand:
    a. Which user(s) were involved
    b. Which endpoints were affected
    c. The attack vector
    d. When and where the malicious activity took place

3. **Comparing Against Threat Intel -** After accessing the endpoint and gathering contextual information, the analyst will then need to determine whether the threat is known bad, known good, or unknown.



Any security automation solution must be able to perform the above steps consistently, with the requisite fallback mechanisms to anticipate any exceptions or failures. The security automation solution must be able to:

a. **Access the Endpoint –** Taking into account the potential that an endpoint may be remote, outside of a directory service, and perhaps even powered-off, the security automation solution must be able to reach the affected endpoint as soon as it is available.
b. **Gather Additional Data –** The security automation solution must have access to network resources, it must have the ability to query to get relevant data, and it must be able to compare and analyze that data to inform its investigation.
c. **Compare Against Threat Intel –** The security automation solution must have access to its own threat intelligence and be able to leverage the customer's own threat intel to determine what to do next.

DETERMINING WHETHER A THREAT REQUIRES ACTION

Once a cyber analyst has received an alert and accessed the endpoint, they need to determine whether a threat requires action. As the majority of alerts an analyst sees are false positive or benign, it's very common to fall victim to what is known as alert fatigue.

From our whitepaper "Solving Alert Fatigue in Cyber Security: What Cyber Security Teams Can Learn from Healthcare Alarm Fatigue"

> Alarms and alerts are meant to signal a potential problem that needs immediate attention and action. However, when alarms are constant and have a high false positive percentage, they end up losing their meaning. Think of a nagging car alarm: what was meant to signal a theft in progress now just makes people think "somebody shut that off!"
>
> In today's Security Operations Centers (SOCs), cyber security incident response teams are dealing with their own version of alert fatigue. While they have invested millions in systems that detect and alert them to potential problems, the sheer volume and high rate of false positives undermine the value of the detection systems.

A cyber analyst must be able to respond to three distinct types of alerts to determine next steps.

- **Known Bad –** In the case of commodity malware, the analyst will need to check the hash against known threat sources. Common threats can be found in multi-AV sources like VirusTotal, letting the analyst know an IOC requires action.
- **Known Good –** When a detection system alerts on a benign entity, a whitelist or exception rule will let the analyst know there is no further investigation necessary.
- **Unknown –** These are threats not yet known, or are file-less and cannot be categorized by signature.

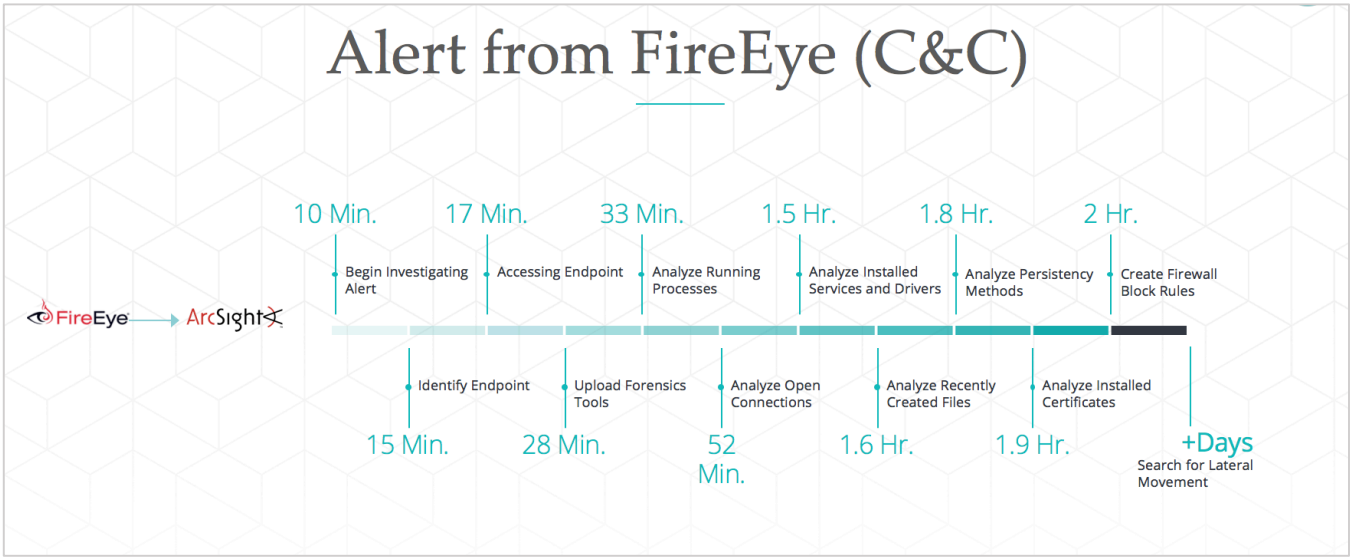
When a threat is known bad, an analyst is able to decide what to do next based on the type of malicious entity. When a threat is unknown, the analyst must take steps to understand the behavior of the entity before deciding the proper course of action.

A security automation solution must be able to determine the status of a potential threat in seconds by comparing with its own threat intelligence, threat intelligence supplied by the customer, and using its own codified logic to understand the behavior of the entity along with what to do next.

PERFORMING NECESSARY REMEDIATION ACTIONS

Once an analyst has deemed a threat to be malicious and requires remediation action, they must then determine the proper course of action based on the type of threat. Three examples follow:

Example 1: Connection to a C2

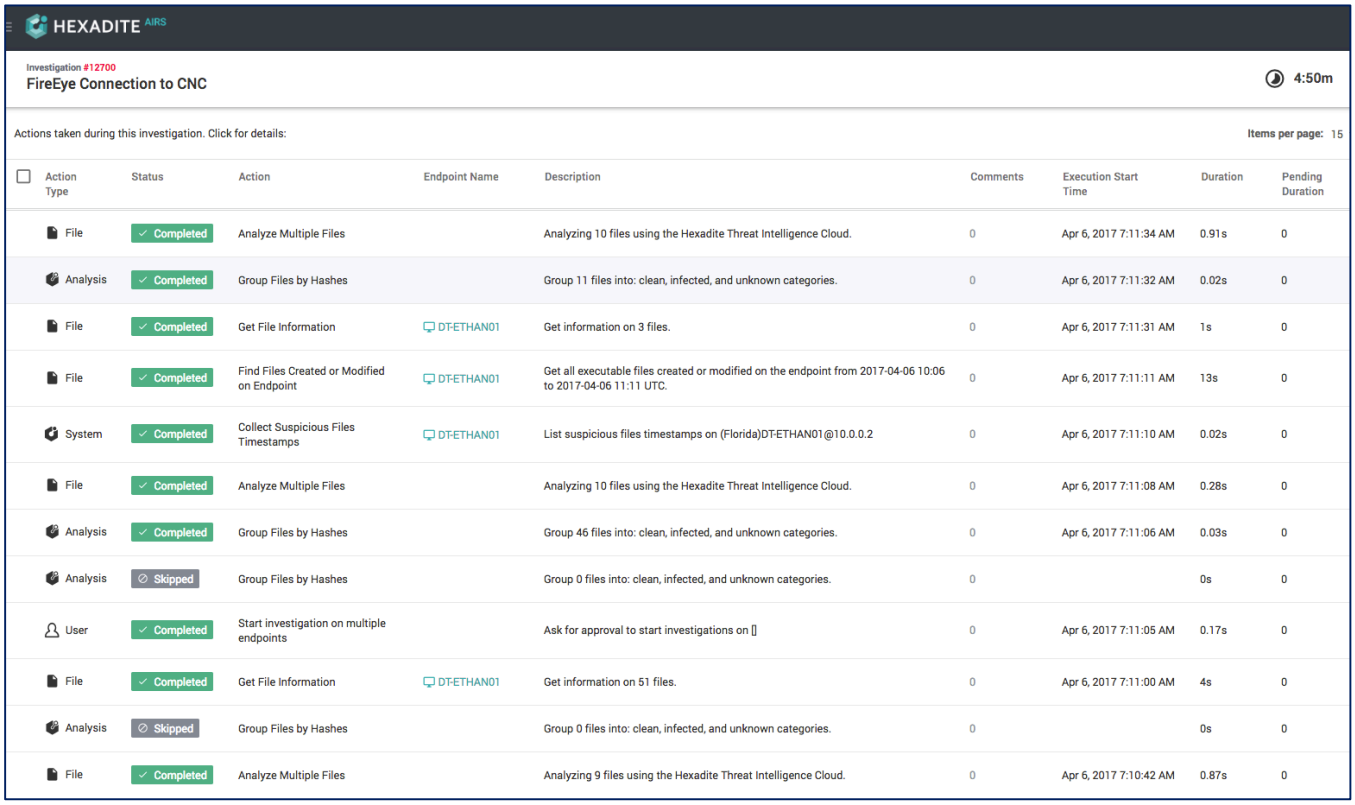


When an analyst receives an alert about a connection to a C&C, they need to analyze:

- **Running Processes**
- **Open Connections**
- **Installed Services and Drivers**
- **Recently Created Files**
- **Persistency Methods**
- **Installed Certificates**

These are a few examples of items that will need to be remediated on the endpoint before creating a firewall block rule to prevent other systems from contacting the malicious address.

A security automation solution must be able to perform these steps at machine speed:



HEXADITE AIRS

Investigation #12700
FireEye Connection to CNC

4:50m

Actions taken during this investigation. Click for details:

Items per page: 15

Action Type	Status	Action	Endpoint Name	Description	Comments	Execution Start Time	Duration	Pending Duration
File	Completed	Analyze Multiple Files		Analyzing 10 files using the Hexadite Threat Intelligence Cloud.	0	Apr 6, 2017 7:11:34 AM	0.91s	0
Analysis	Completed	Group Files by Hashes		Group 11 files into: clean, infected, and unknown categories.	0	Apr 6, 2017 7:11:32 AM	0.02s	0
File	Completed	Get File Information	DT-ETHAN01	Get information on 3 files.	0	Apr 6, 2017 7:11:31 AM	1s	0
File	Completed	Find Files Created or Modified on Endpoint	DT-ETHAN01	Get all executable files created or modified on the endpoint from 2017-04-06 10:06 to 2017-04-06 11:11 UTC.	0	Apr 6, 2017 7:11:11 AM	13s	0
System	Completed	Collect Suspicious Files Timestamps	DT-ETHAN01	List suspicious files timestamps on (Florida)DT-ETHAN01@10.0.0.2	0	Apr 6, 2017 7:11:10 AM	0.02s	0
File	Completed	Analyze Multiple Files		Analyzing 10 files using the Hexadite Threat Intelligence Cloud.	0	Apr 6, 2017 7:11:08 AM	0.28s	0
Analysis	Completed	Group Files by Hashes		Group 46 files into: clean, infected, and unknown categories.	0	Apr 6, 2017 7:11:06 AM	0.03s	0
Analysis	Skipped	Group Files by Hashes		Group 0 files into: clean, infected, and unknown categories.	0		0s	0
User	Completed	Start investigation on multiple endpoints		Ask for approval to start investigations on []	0	Apr 6, 2017 7:11:05 AM	0.17s	0
File	Completed	Get File Information	DT-ETHAN01	Get information on 51 files.	0	Apr 6, 2017 7:11:00 AM	4s	0
Analysis	Skipped	Group Files by Hashes		Group 0 files into: clean, infected, and unknown categories.	0		0s	0
File	Completed	Analyze Multiple Files		Analyzing 9 files using the Hexadite Threat Intelligence Cloud.	0	Apr 6, 2017 7:10:42 AM	0.87s	0

***Example**: Hexadite AIRS investigation of a C2, going from alert to remediation in under 5 minutes.*

Example 2: Phishing Attacks

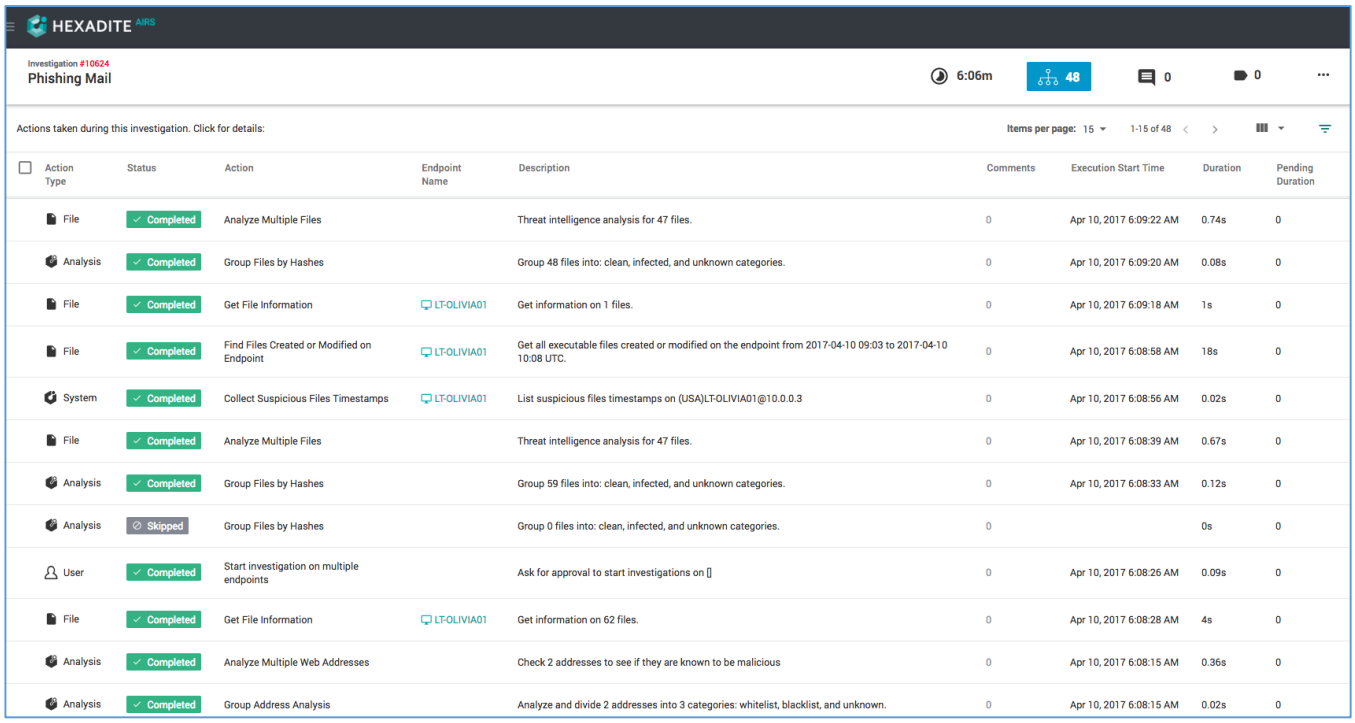
Phishing emails continue to be a problem for enterprises, as phishing is now the #1 delivery vehicle for ransomware and malware[i]. Consider the following statistics:

- 85% of organizations have suffered phishing attacks[ii]
- 30% of phishing emails get opened[iii]
- The number one delivery vehicle for malware is email attachments
- A 250% surge in phishing was detected in Q1 2016[iv]
- 9 out of 10 phishing emails carried ransomware in March 2016[v]

To remediate a phishing attack, an analyst must first:

- **Investigate attachments**
- **Find all endpoints that received the email**
- **Determine whether the attachments were executed**
- **Investigate endpoints for infection**
- **Review installed services, drivers and recently created files**
- **Quarantine files, kill processes and create a firewall block rule**

These are just a few examples of items that need investigation and remediation when a phishing attack has occurred.



HEXADITE AIRS

Investigation #10624
Phishing Mail

6:06m | 48 | 0 | 0

Actions taken during this investigation. Click for details:

Items per page: 15 | 1-15 of 48

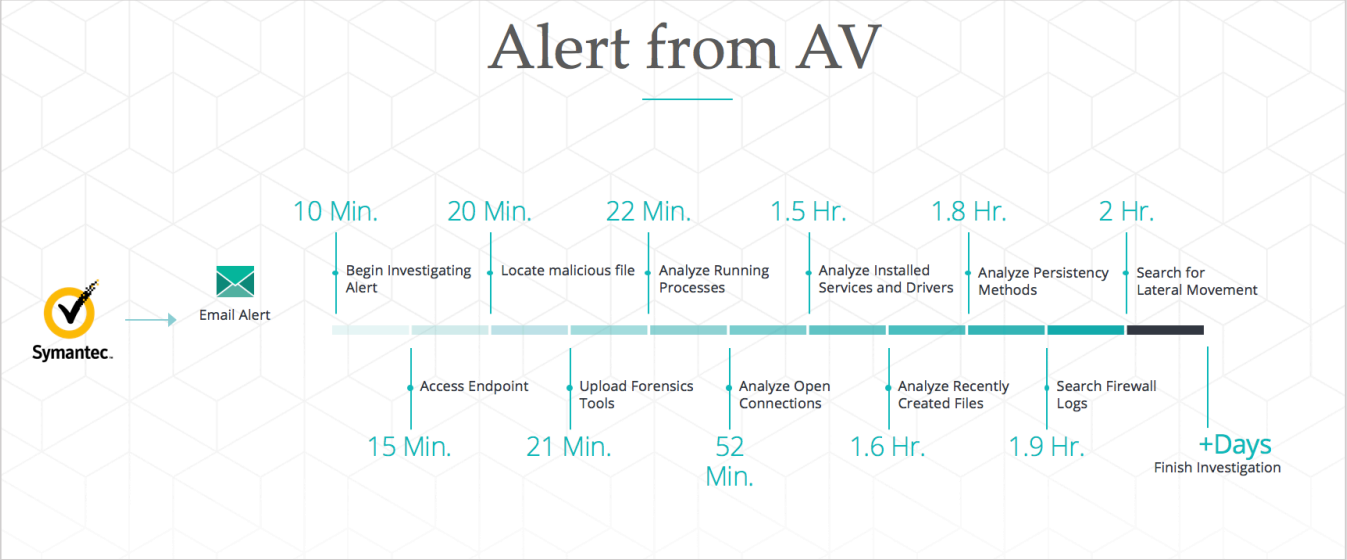
Action Type	Status	Action	Endpoint Name	Description	Comments	Execution Start Time	Duration	Pending Duration
File	Completed	Analyze Multiple Files		Threat intelligence analysis for 47 files.	0	Apr 10, 2017 6:09:22 AM	0.74s	0
Analysis	Completed	Group Files by Hashes		Group 48 files into: clean, infected, and unknown categories.	0	Apr 10, 2017 6:09:20 AM	0.08s	0
File	Completed	Get File Information	LT-OLIVIA01	Get information on 1 files.	0	Apr 10, 2017 6:09:18 AM	1s	0
File	Completed	Find Files Created or Modified on Endpoint	LT-OLIVIA01	Get all executable files created or modified on the endpoint from 2017-04-10 09:03 to 2017-04-10 10:08 UTC.	0	Apr 10, 2017 6:08:58 AM	18s	0
System	Completed	Collect Suspicious Files Timestamps	LT-OLIVIA01	List suspicious files timestamps on (USA)LT-OLIVIA01@10.0.0.3	0	Apr 10, 2017 6:08:56 AM	0.02s	0
File	Completed	Analyze Multiple Files		Threat intelligence analysis for 47 files.	0	Apr 10, 2017 6:08:39 AM	0.67s	0
Analysis	Completed	Group Files by Hashes		Group 59 files into: clean, infected, and unknown categories.	0	Apr 10, 2017 6:08:33 AM	0.12s	0
Analysis	Skipped	Group Files by Hashes		Group 0 files into: clean, infected, and unknown categories.	0		0s	0
User	Completed	Start investigation on multiple endpoints		Ask for approval to start investigations on []	0	Apr 10, 2017 6:08:26 AM	0.09s	0
File	Completed	Get File Information	LT-OLIVIA01	Get information on 62 files.	0	Apr 10, 2017 6:08:28 AM	4s	0
Analysis	Completed	Analyze Multiple Web Addresses		Check 2 addresses to see if they are known to be malicious	0	Apr 10, 2017 6:08:15 AM	0.36s	0
Analysis	Completed	Group Address Analysis		Analyze and divide 2 addresses into 3 categories: whitelist, blacklist, and unknown.	0	Apr 10, 2017 6:08:15 AM	0.02s	0

***Example**: Hexadite AIRS investigation of a Phishing attack, going from alert to remediation in under 7 minutes.*

Example 3: Investigating an AV Alert and Verifying Results

In most scenarios, an incident response team will receive an alert from AV, and will do a quick verification check to make sure that the file in question has been removed/quarantined by AV. However, stopping an investigation after verifying file deletion is like making sure one symptom is gone without addressing the core problem.

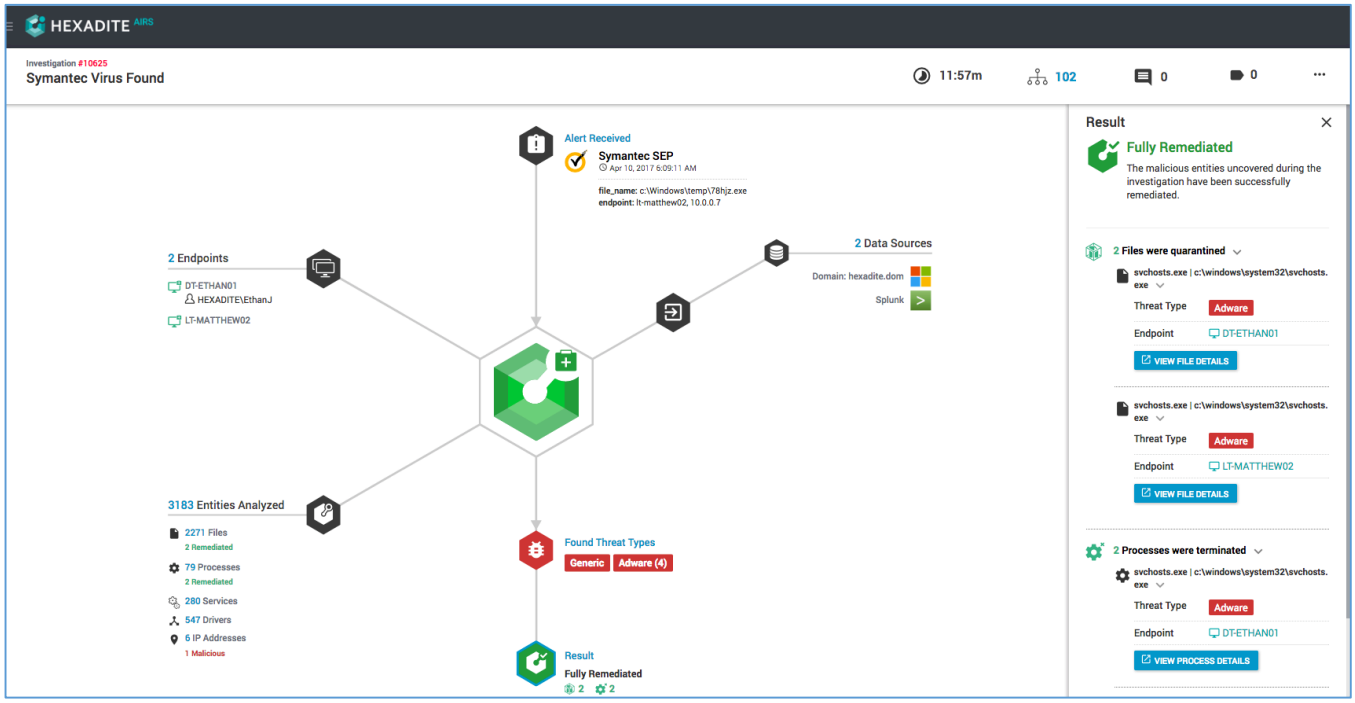
In the case where a cyber analyst receives an alert from AV, the following process would be followed:



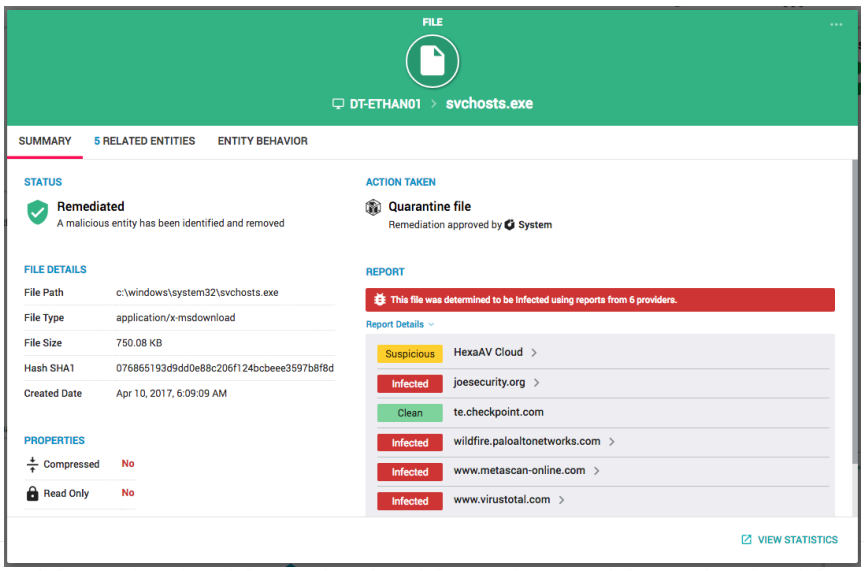
To investigate and verify results of an AV alert, an analyst must first:

- **Access the endpoint**
- **Locate the malicious file(s)**
- **Analyze running processes, open connections, installed services and drivers, recently created files, persistency methods**
- **Search firewall logs**
- **Search for lateral movement**
- **Quarantine files, kill processes and create a firewall block rule**

These are just a few examples of items that need investigation and remediation when following up on an AV alert.



***Example**: Hexadite AIRS investigation of an AV alert, uncovering 2 infected endpoints with adware, and fully remediating both systems in under 12 minutes.*

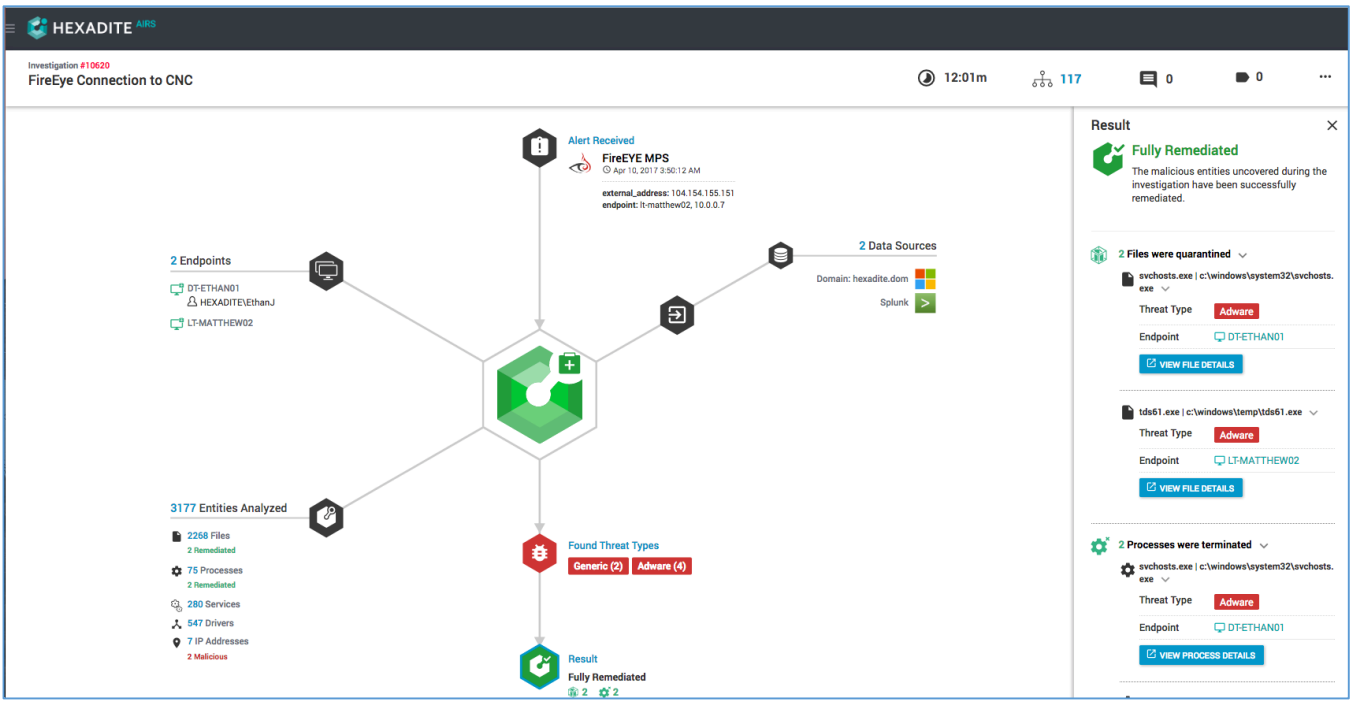


Detailed view of the quarantined file.

DECIDING WHAT ADDITIONAL INVESTIGATIONS SHOULD BE NEXT

After taking steps to remediate a threat and verifying all traces are accounted for, most cyber analysts will move on to the next alert. Faced with an overwhelming volume of threats and alerts, they simply do not have the time required to go beyond eliminating the most pressing items.

A security automation solution, however, is able to constantly ask "what's next?", as performing vigorous investigations at machine speed enables the system to pivot and launch parallel investigations.



***Example**: Hexadite AIRS receives an alert about a malicious IP address, and in the process of investigating finds another endpoint contacting the same IP.*

The speed and repeatability of a security automation solution enables organizations to go beyond a linear approach to investigation and remediation, and instead continuously spawn parallel investigations to always look for what can be done next.

5 Approaches to Security Automation

While the market for security automation has seen a dramatic increase in attention, investment, and budget, there is a vast difference in how security automation vendors define what they mean by "security automation." We've been able to identify five distinct approaches to security automation. What follows is a review of the approaches vendors call security automation.

Note: We believe that of these automation approaches are valid and there are excellent vendors in each of these categories. While we are partial to our own approach over the others, customers can find value any of these approaches.

#1 WORKFLOW TOOLS

Workflow tools are solutions that gather and enhance alert data, and automate the communication process of sending instructions to analysts and auditors. Workflow tools provide a standard framework to better organize incident response flows with built-in ticketing, instructions on how to react to certain alerts, and user roles.

Problems Solved

Streamlining communications and IR flow is crucial to having an efficient SOC. When an organization has a mature, fully-staffed SOC, increasing the team's communications efficiency will certainly provide value.

Challenges

When the issue at hand is the inability to investigate and remediate threats, workflow tools will only help with context and communications— relying on people to do the work.

#2 ORCHESTRATION TOOLS

Orchestration is probably the most pervasive buzzword in cybersecurity right now—but what is it, exactly?

Orchestration is the practice of connecting existing security tools together through APIs in order to streamline incident response processes.

Problems Solved

If an organization already has a full stack of point solutions that simply need to be connected together, an orchestration layer can be the connective fabric to make the tools work together.

Challenges

While orchestration can be powerful, one must ask: am I connecting tools for the sake of connecting them? What am I actually accomplishing by allowing my existing security tools to talk to each other? Is it saving time? Am I getting value? Orchestration is means to an end, and relies solely on the tools the customer already has.

#3 SCRIPTING TOOLS

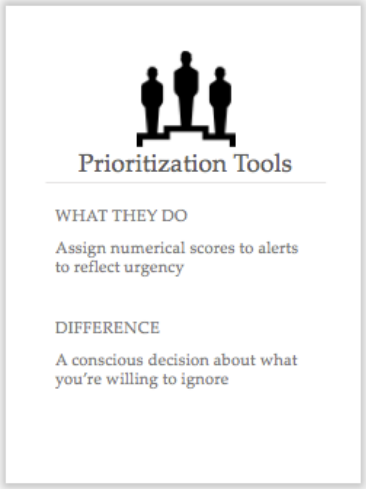
Scripting tools are another hot category in security automation, and rightly so—they allow SOCs to do literally anything they want by writing code and configuring all of the playbooks.

Problems Solved

If an organization has developer resources that can consistently write and maintain code to perform in-depth investigations for all use cases, and simply need an engine to execute code, then scripting tools are a great choice.

Challenges

When organizations do not have the resources to investigate and remediate threats, it is unlikely that they have the development resources necessary to use a scripting tool. When budget and resources are an issue, using scripting tools to automate become a non-starter.



#4 PRIORITIZATION TOOLS

The most basic form of automation is the ability to assign a priority score to security alerts. In many cases, organizations simply tune their detection systems to match their capacity so that only critical alerts are sent to analysts. The rest of the alerts are ignored. This approach is necessary, but it's far, far from ideal.

Problems Solved

Teams that are overwhelmed need help deciding where to focus their scarce resources can be helped by prioritization. Priority scores attempt to categorize by severity, giving them notification of what is deemed critical.

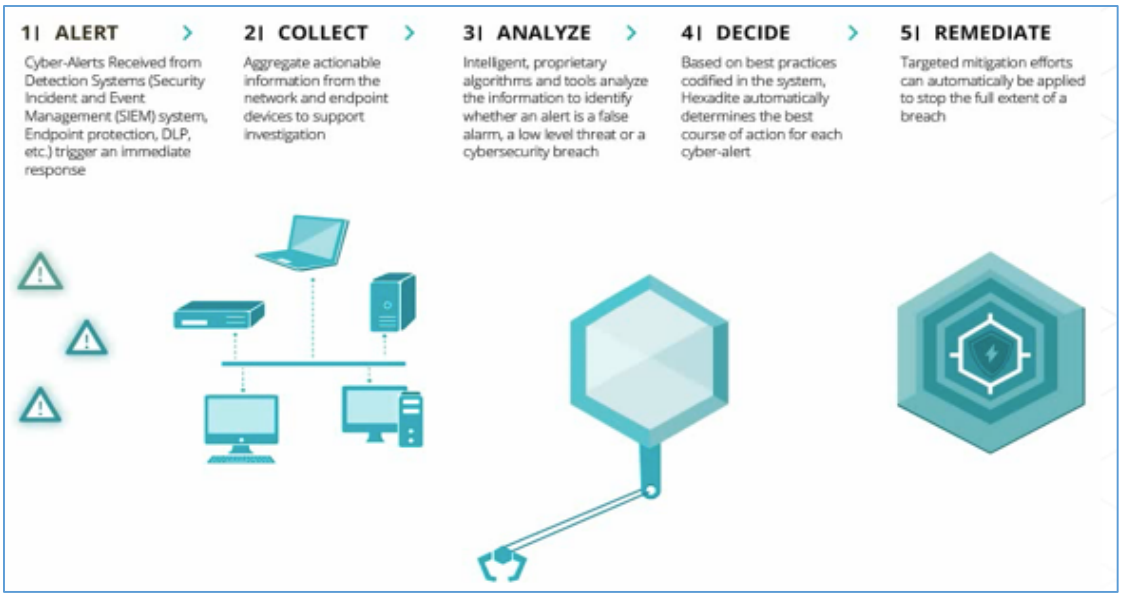
Challenges

Prioritization is akin to saying "ignore anything with a score below 80." But why 80? Because 81 is worse. How is that threshold determined? Additionally, nearly every headline-grabbing data breach over the last decade wasn't due to threats being missed. Instead, in every case a detection system produced an alert, but the organization in question did not have the capacity to follow up on what wasn't deemed critical.

#5 INTELLIGENT SECURITY AUTOMATION

Intelligent security automation means automation that does exactly what a cyber analyst would do, but at machine speed. This approach must have the following five following qualities in order to be considered intelligent security automation:

1. **Connect with any detection system that can produce an alert.**
2. **Be able to query data from relevant sources to start an investigation. Sources include SIEMs, log repositories, network appliances, and endpoints.**
3. **Have the ability to compare information against threat intelligence and determine whether a threat is a known bad, known good, or unknown.**
4. **Be able to make decisions about what steps to take next. This includes quarantining a file, terminating a process, adding a firewall block rule, and dozens of other remediation actions.**
5. **Be able to execute remediation actions automatically or semi-automatically to allow humans to approve actions and work within the policies of an organization.**



If an organization's analysts are buried in alerts and do not have the developer resources to build automation that automatically investigates and remediates, then intelligent security automation is the best approach.

The 5 Prerequisites for Enterprises to Trust Security Automation

Addressing the trust factor in security automation

Any conversation about using automation in cybersecurity inevitably wanders into "can I trust automation" territory. And while some vendors choose to pit automation vendors against human cyber analysts in an all or nothing battle royal, the reality of how automation can complement human intelligence is a bit more nuanced and subtle.

But the question of whether automation can be trusted is a valid one and when it comes to automating any aspect of information security, being skeptical is understandable. There are 5 prerequisites that must be satisfied before any enterprise can trust security automation.

Prerequisite #1: Security Automation Must Be Repeatable

Without predictability, there is no trust. In order to believe that an automation tool will perform as intended, there needs to be a demonstrated record of repeatability. Think of every meal you've ever eaten in a restaurant: a server is willing to take your order and bring you drinks and the chef is willing to cook your food all without demanding you pay up front in full. Why would they take that risk? Because thousands of transactions have proven that customers will pay.

Prerequisite #2: Auditable

While some think of automation as a "black box" comprised of a mixture of magic and alchemy, true automation must be repeatable and visible to the user. Every action taken and every decision made must be auditable. A good example is online banking. In the early days of online banking, people were justifiably confused by the idea that all transactions would happen automatically without a person being involved. But the fact that a searchable record exists showing every dollar going in and out of the account allowed for the trust needed to make the switch from paper and trips to see the teller.

Prerequisite #3: Reversible

Any time a system has access to a company's data and the ability to take action, there must also be a process in place to reverse those actions. Without a way to reverse a course of action, automation will be too much of a risk for large scale adoption.

Prerequisite #4: Kill Switch / Interrupt

To fully trust automation, there must be a way to stop it. If you look to the world of driverless cars, you'll note that any driverless vehicle is equipped with an override that allows the driver to take control. It is only when you have the capability to take the reins that a person can have enough trust in an automated system to hand over the controls.

Prerequisite #5: Learn/Adapt

Finally, an automation solution must be able to learn and adapt for enterprises to be willing to invest the time and resources to get up and running. Without the ability to get better with time and more data, you're only able to automate what you know today. But tomorrow is coming, and you can bet it will bring with it new challenges that are impossible to predict today.

Return on Investment

As with any security purchase, the capabilities added must justify the dollars spent and time invested. The following requirements should be considered when evaluating a solution.

SPEED OF INTEGRATION

Once purchased, how quickly can you be up and running? Will the integration involve paid hours of professional services, and custom code? Determine whether the solution has been built to immediately integrate with your current security toolset to understand just how long the integration process will take.

SPEED OF DEPLOYMENT

Once connected to alert sources, how quickly can you start automatically investigating alerts? While some approaches require you to write and maintain custom code to execute investigation actions, others favor an out-of-the-box approach that begins investigating immediately after receiving the first alert.

NO ADDITIONAL RESOURCES

If the goal of automating incident response is to free up security resources, your security automation solution should not require additional headcount to develop and maintain custom code in order for the system to run. Requiring more people defeats the purpose and the value.

PREDICTABLE COST STRUCTURE

Without predictability, it's impossible to determine value. As some solutions charge a cost per investigation, cost per remediation action, and cost for additional support hours, it can be futile to project yearly costs. This makes ROI a guess at best.

Evaluation Checklist

Use the following checklist to evaluate security automation solutions.

Feature	Description	Requirement Met?
Immediate Integration with Existing Security Toolset	The automation solution integrates with my detection systems (SIEM, AV, EDR, etc.) out of the box.	☐ Yes ☐ No
Operating System Coverage	The solution can work with my Windows, Mac, and Linux servers, desktops, and laptops.	☐ Yes ☐ No
Automatic Investigation Capabilities	The solution does not require customization in the target environment to perform investigations.	☐ Yes ☐ No
Automated Remediation of Confirmed Threats	Automatic remediation methods must include removing malicious objects on the endpoint as well as dynamically reconfiguring network security devices.	☐ Yes ☐ No
Integrated Threat Intelligence	Including provider's own threat data, for analysis of suspicious objects, as well as provide dynamic analysis of files and URL objects using multiple sandbox technologies	☐ Yes ☐ No
Deploy as VM	Ability to deploy as a virtual appliance into a standard VM environment.	☐ Yes ☐ No
Autonomous Remediation	Ability to complete incident response flow from alert to remediation without human interaction.	☐ Yes ☐ No
Custom Approval Levels	Ability to pause automation for human approval.	☐ Yes ☐ No
Rapid Investigation Trigger	Ability to initiate an investigation within less than 30 seconds after an alert is received.	☐ Yes ☐ No
Immediate Results	Ability to complete investigations and provide a finding within 15 minutes or less on average.	☐ Yes ☐ No
Parallel Investigations	Ability to conduct at least 50 parallel automated investigations with default hardware specification.	☐ Yes ☐ No

Evaluation Checklist (Continued)

Feature	Description	Requirement Met?
Large Scale Coverage	Ability to scale up with additional hardware resources.	☐ Yes ☐ No
Manual Investigation Capability	Ability to launch a manual investigation on any supported object.	☐ Yes ☐ No
Coverage Customization	Ability to dynamically limit investigations to pre-defined asset groups based on Active Directory OUs.	☐ Yes ☐ No
3rd Party Ticketing Integration	Ability to push alert events back to a SIEM platform or log repository using standard formats	☐ Yes ☐ No
No Additional Resources	The solution does not require additional headcount or professional services to write and maintain custom code	☐ Yes ☐ No
Predictable Cost Structure	The solution is priced predictably, and I understand my yearly cost and can calculate ROI.	☐ Yes ☐ No

About Hexadite

Hexadite AIRS is the first agentless intelligent security automation platform. By easily integrating with customers' existing security technologies and harnessing artificial intelligence that automatically investigates every cyber alert and drives remediation actions, Hexadite enables security teams to mitigate cyber threats in real-time. For more information, follow @Hexadite on Twitter or visit www.hexadite.com.

---

[i] Phishing by the Numbers: Must-Know Phishing Statistics 2016

[ii] Wombat 2016 State of the Phish

[iii] Verizon 2016 DBIR

[iv] APWG Phishing Activity Trends Report

[v] PhishMe Q1 2016 Malware Review