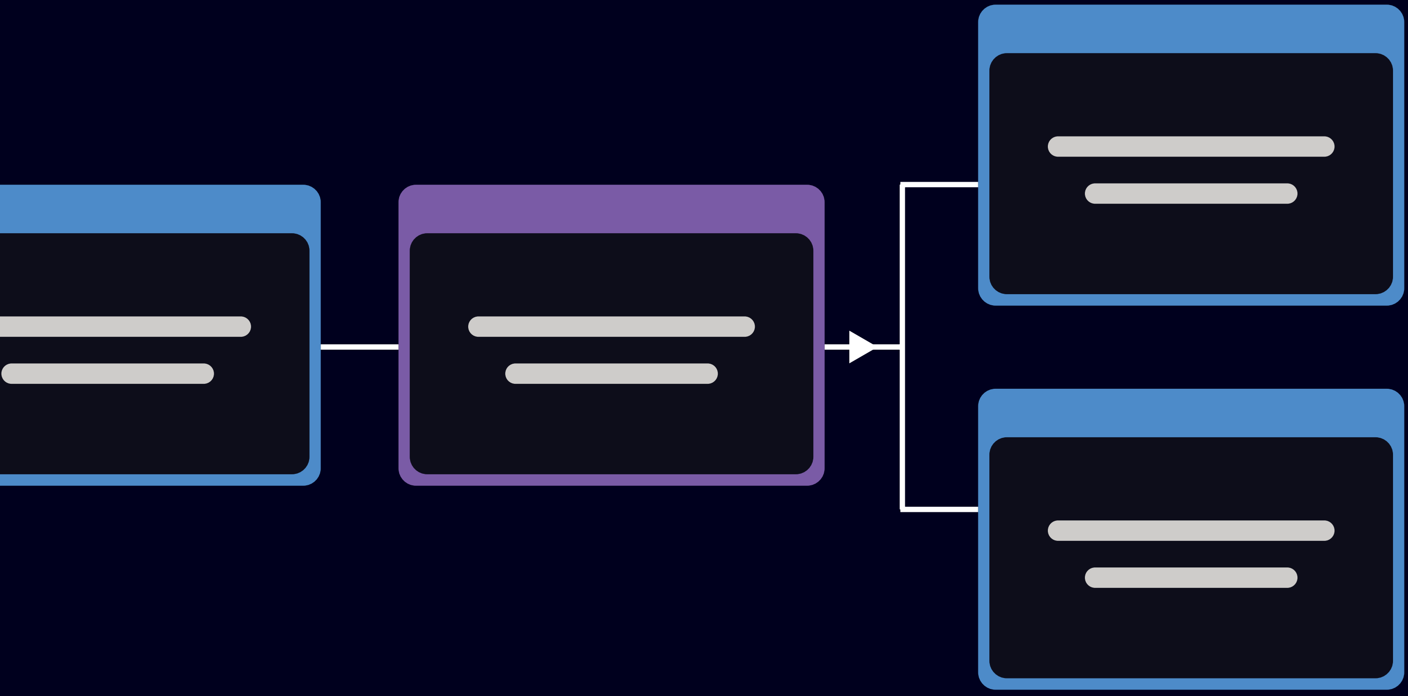
Siemplify



SOC Investigation and Response – Driven by Context

Top Security Playbooks for 2019

WHITE PAPER

INTRODUCTION

The security operations center (SOC), to borrow parlance from the legendary comedian Rodney Dangerfield, doesn't get the respect it deserves. But anyone who understands how the beating heart of your security program functions knows otherwise. The SOC is the regulator of the business, responsible for ensuring nothing disrupts it and that its proverbial kingdom keys and secret sauces stay protected.

But with that great responsibility comes great pressure for SOC inhabitants, as they must successfully follow security events from inception to resolution, while in the process overcoming key stressors endemic to a modern-day infosec command center: skills shortages, disparate detection tools and, of course, an abundance of threats amid an even greater number of false alarms.

Security analysts, engineers, architects and managers in the SOC are engaged in a zero-sum game where there can be only one winner. To give the SOC team the best chance to win, they must identify, investigate and respond to threats as quickly and consistently as possible. The key to fast and effective response is having processes documented in what is commonly referred to as playbooks (also known as runbooks).

Cybercriminals are sophisticated – but they're also business savvy, meaning they know what works and what doesn't and aren't keen on exerting unnecessary time and energy. In fact, security operations teams have seen many times before what cybercriminals can throw at them, but where they've stumbled is because of things like human error, poor prioritization or even burnout.

Playbooks help address each of these downsides by providing security teams with a single source of truth to turn to in high-pressure situations, helping to ensure response processes are executed systematically and repeatably. The purpose of this document is to provide security teams with a set of dependable playbooks targeted at the most common types of investigations undertaken by SOCs to drive down mean time to resolution. Added benefits include documenting so-called tribal knowledge, defined as unwritten information not commonly known by others within a business, and onboarding new analysts.

Siemplify, a leading provider of security orchestration, automation and response technology, provides these purpose-built playbook templates, and dozens more, in its Security Operations Platform with the goal of making analysts more efficient, engineers and architects more effective, and managers more informed. Since every organization has different needs, the Siemplify platform makes editing existing and creating new playbooks easy thanks to the drag-and-drop playbook editor. Now let's get into the playbooks!

> *Playbooks [provide] security teams with a single source of truth to turn to in high-pressure situations, helping to ensure response processes are executed systematically and repeatably.* "

THE CONTEXT X-FACTOR

But first, a note on context. Whether using the Siemplify Security Operations Platform or some other solution, modern SOCs must transition from investigations based on tribal knowledge to a well-documented context-driven approach that can be used by all analysts in the SOC.

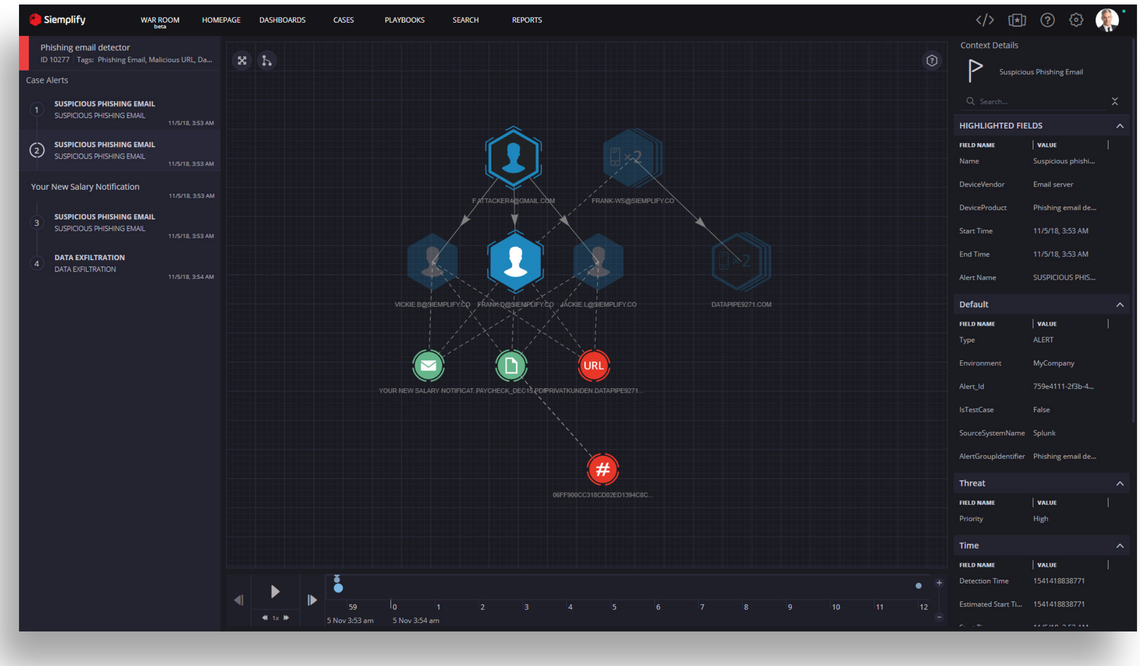
Before driving into the details of these context-driven playbooks, we first must define context in terms of security operation. Context is something that everyone deals with daily. The best example outside of security is text messaging. While texting is an effective way to quickly communicate with friends and family, even co-workers, one of the main issues is lack of context. Since text messages are just text, we miss a major piece of context vital to effective communication: tone and tenor.

Many disagreements or misunderstandings can come from this lack of context. The stakes, however, are quite low when it comes to text message misperceptions. The same can't be said when investigating a potential threat. Context in security means understanding how a single alert or incident fits into the overall threat landscape at any given point in time.

For instance, if an analyst investigated an alert of a failed login by User A on Computer X, they may quickly dismiss this as a false positive – to no fault of their own. After all, people make mistakes entering their credentials all the time. However, if the analyst had proper context that showed user A also attempted to login to 10 other machines within seconds of each other, they would realize that this single incident was part of a coordinated brute force attack against the organization.

With this proper context, the analyst now understands that a different response is required compared to the response that would come for a likely false positive alert. This example, while quite simple, illustrates the ultimate power of context in investigation and response. The remainder of this paper will keep context in mind as we discuss several common investigation types and describe the best practices regarding playbook creation and flow.

> *Context in security means understanding how a single alert or incident fits into the overall threat landscape at any given point in time.*



Phishing email detector
ID 10277 | Tags: Phishing Email, Malicious URL, Da...

Case Alerts

1. SUSPICIOUS PHISHING EMAIL
SUSPICIOUS PHISHING EMAIL
11/5/18, 3:53 AM

2. SUSPICIOUS PHISHING EMAIL
SUSPICIOUS PHISHING EMAIL
11/5/18, 3:53 AM

Your New Salary Notification
11/5/18, 3:53 AM

3. SUSPICIOUS PHISHING EMAIL
SUSPICIOUS PHISHING EMAIL
11/5/18, 3:53 AM

4. DATA EXFILTRATION
DATA EXFILTRATION
11/5/18, 3:54 AM

Context Details

Suspicious Phishing Email

Search...

HIGHLIGHTED FIELDS

FIELD NAME	VALUE
Name	Suspicious phishi...
DeviceVendor	Email server
DeviceProduct	Phishing email de...
Start Time	11/5/18, 3:53 AM
End Time	11/5/18, 3:53 AM
Alert Name	SUSPICIOUS PHIS...

Default

FIELD NAME	VALUE
Type	ALERT
Environment	MyCompany
Alert_Id	759e4111-2f3b-4...
IsTestCase	False
SourceSystemName	Splunk
AlertGroupIdentifier	Phishing email de...

Threat

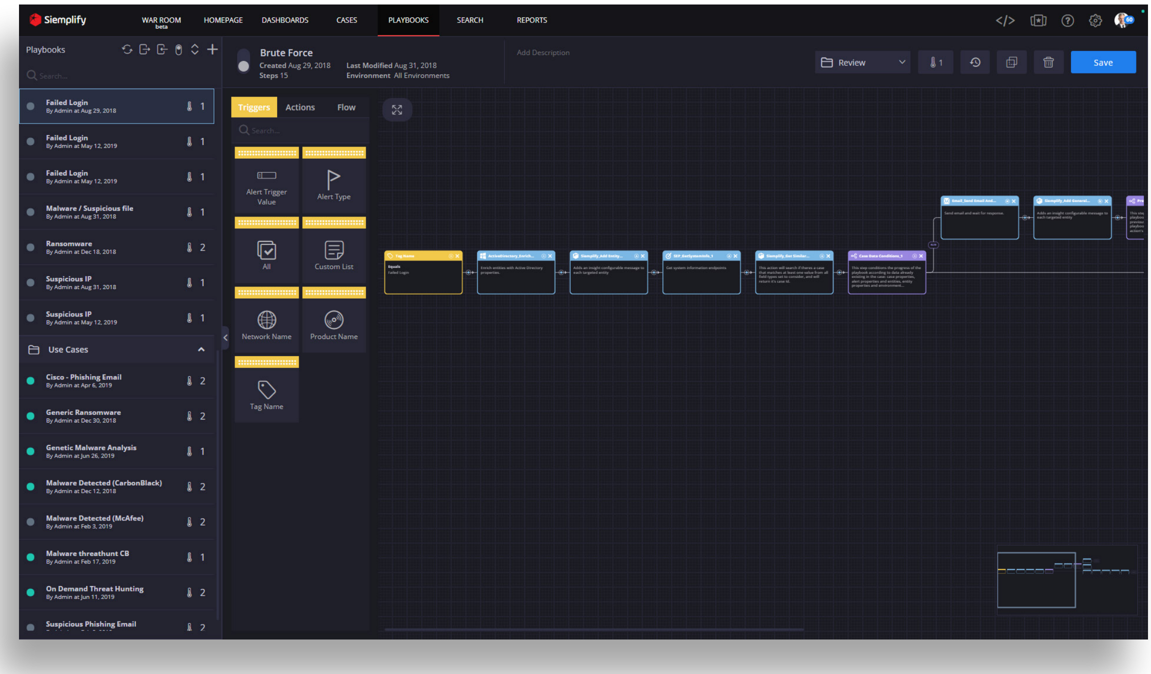
FIELD NAME	VALUE
Priority	High

Time

FIELD NAME	VALUE
Detection Time	1541418838771
Estimated Start Ti...	1541418838771

Playbooks

Brute Force Attacks


Siemplify
WAR ROOM beta
HOMEPAGE
DASHBOARDS
CASES
PLAYBOOKS
SEARCH
REPORTS
Playbooks
Search...
Failed Login By Admin at Aug 29, 2018 1
Failed Login By Admin at May 12, 2019 1
Failed Login By Admin at May 12, 2019 1
Malware / Suspicious file By Admin at Aug 31, 2018 1
Ransomware By Admin at Dec 18, 2018 2
Suspicious IP By Admin at Aug 31, 2018 1
Suspicious IP By Admin at May 12, 2019 1
Use Cases
Cisco - Phishing Email By Admin at Apr 6, 2019 2
Generic Ransomware By Admin at Dec 30, 2018 2
Genetic Malware Analysis By Admin at Jun 26, 2019 1
Malware Detected (CarbonBlack) By Admin at Dec 12, 2018 2
Malware Detected (McAfee) By Admin at Feb 3, 2019 2
Malware threathunt CB By Admin at Feb 17, 2019 1
On Demand Threat Hunting By Admin at Jun 11, 2019 2
Suspicious Phishing Email 2
Brute Force
Created Aug 29, 2018
Steps 15
Last Modified Aug 31, 2018
Environment All Environments
Add Description
Review
Save
Triggers
Actions
Flow
Alert Trigger Value
Alert Type
All
Custom List
Network Name
Product Name
Tag Name

As mentioned previously, a brute force attack occurs when an attacker attempts to break into an environment by repeatedly attempting to login to a system or systems. Generally, the attacker has either reverse engineered or purchased on the dark web legitimate usernames and applies a vast library of potential passwords to gain access to a system. While IT departments can implement a policy that locks out users after a given number of failed attempts, many organizations do not take this approach as they are concerned about remote and in-the-field employees being frozen out of their computers, causing business disruption.

Details & Workflow

Enrichment & Context

- Source IP address –is it internal or external
- Target IP and OS information

Investigation

1 Is the source IP internal or external?

Is the source IP internal or external?

a) If internal: Search of any previous alerts raised on the entity (source IP). The machine might be already compromised and might still be compromised.

I) If the alerts are involving a malware alert, escalate the case to Tier 2.

II) Tier 2: Block the traffic from the source IP, disinfect the machine, verify the source of the malware and unblock the machine once no threats are found.

b) If external: Search the IP using IP reputation sites and act accordingly (continue the next steps of this playbook to gather information for Tier 2).

2

Determine which data source was used to trigger the alert. Is the alert based on network logs or actual on-host login information?

3

Network based logs: Here we assume that the product triggering the alert cannot be sure about the traffic it monitors, as it might be encrypted. In this case, we only try to find out indicator of failure.

a) Find out which ports were used for the brute force.

b) Search the IP using IP reputation sites and act accordingly (continue the next steps of this playbook to gather information for Tier 2).

c) If the attack port does not match any listening service or and previously running service, mark the case as a 'false positive' (since there is no chance of success without a service listening on the port). Escalate the source IP's information to Tier 2 for further hunting, as this is still considered an indication of a malicious presence trying its 'luck' around the network.

4

Host-based logs (or logs from the last step of the previous section)

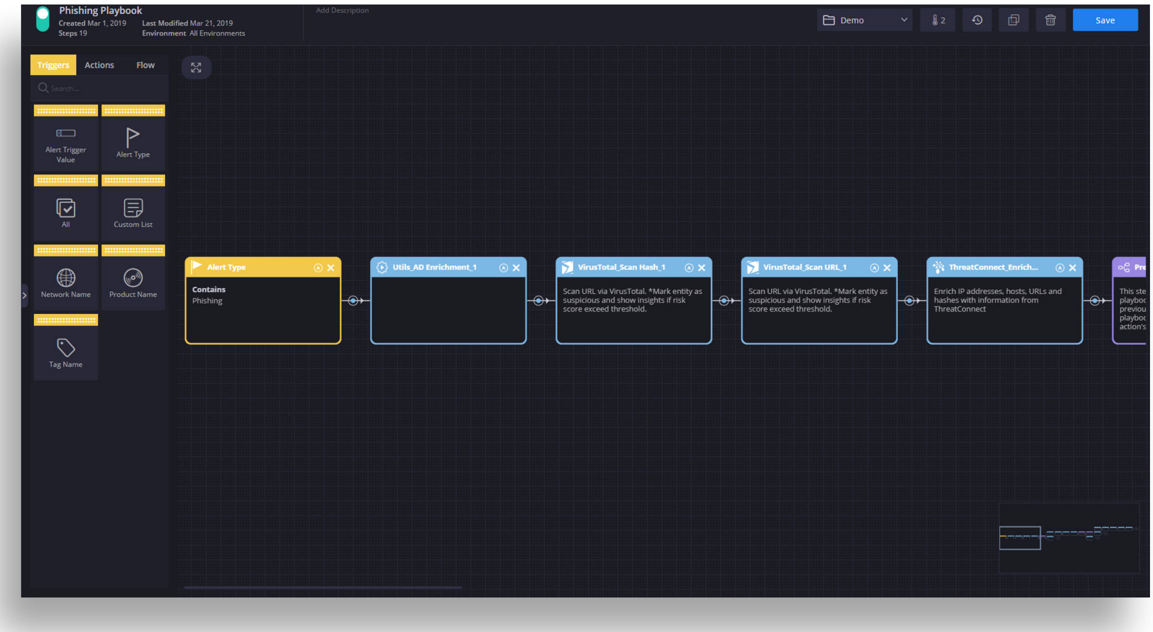
a) Search the logs for events indicating a 'failure to login' or 'user does not exist' (depends on the attacked service). If such logs exist, measure the time span during which they occurred. If the time span is very short, aka mere seconds between attempts, escalate the case to Tier 2, an indication of a malicious presence trying its 'luck' around the network.

b) Search the logs for a successful login log entry. If such entry is found, escalate the case to Tier 2 for further vestigation.

Containment & Remediation

1. Find out all users that were used in the brute force attack. Look for any suspicious username from this list and search for other hosts that these usernames were used on.
2. Notify the owners of the legitimate accounts and the owners of the targeted machines that a brute force attempt was made on their assets.
3. Perform a more thorough investigation on the possibly affected hosts and act accordingly.
4. If the attacker is an external IP, block it and ensure that the firewall is configured to prevent remote login attempts for the specific port in the case it was unnecessarily open to the public.
5. If the attacker is an internal IP, search for any malware infections and past malware alerts on the source host to see if the host is vulnerable.

Phishing Attacks



Phishing Playbook

Created Mar 1, 2019 Last Modified Mar 21, 2019

Steps 19 Environment All Environments

Alert Type — Contains Phishing

Utils_AD Enrichment_1

VirusTotal_Scan Hash_1 — Scan URL via VirusTotal. *Mark entity as suspicious and show insights if risk score exceed threshold.

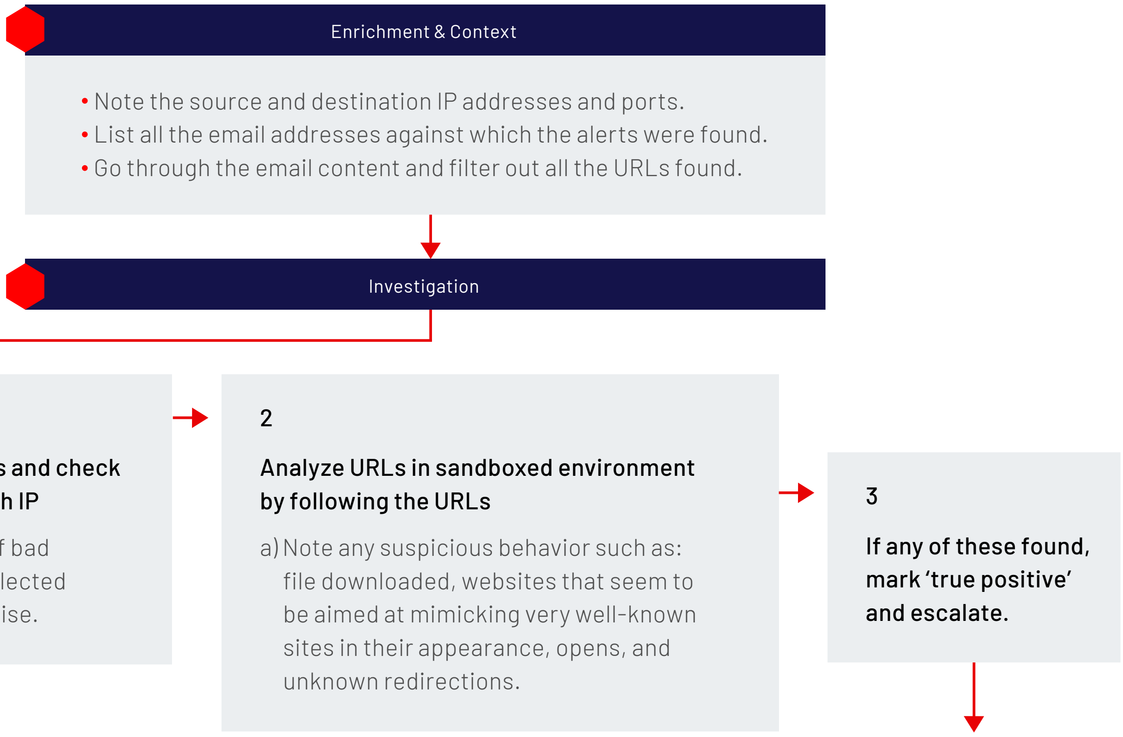
VirusTotal_Scan URL_1 — Scan URL via VirusTotal. *Mark entity as suspicious and show insights if risk score exceed threshold.

ThreatConnect_Enrich... — Enrich IP addresses, hosts, URLs and hashes with information from ThreatConnect

Phishing is one of the most prevalent attack types organizations experience across all industries and size and has been the source of some of the most prolific breaches of all time. It's also the type of attack that your CEO is familiar with and comfortable enough asking you about in the hallway. In a typical scenario, an attacker attempts to trick an unsuspecting employee to divulge sensitive information. In the early days of phishing, the attackers would send seemingly legitimate emails to employees with the hopes the worker would click on a link in the message and subsequently provide the proverbial keys to the kingdom.

Today, phishing attacks are more sophisticated, ranging from email, text message, and even company executive and cloud-based file storage/sharing site impersonation. Given the large set of threat vectors associated with phishing attacks, many SOCs cite phishing investigations as among their largest consumers of available resources.

Details & Workflow



Enrichment & Context

- Note the source and destination IP addresses and ports.
- List all the email addresses against which the alerts were found.
- Go through the email content and filter out all the URLs found.

Investigation

1

Resolve all URLs to IPs and check the reputation for each IP

a) Mark 'true positive' if bad and escalate the collected information, otherwise.

2

Analyze URLs in sandboxed environment by following the URLs

a) Note any suspicious behavior such as: file downloaded, websites that seem to be aimed at mimicking very well-known sites in their appearance, opens, and unknown redirections.

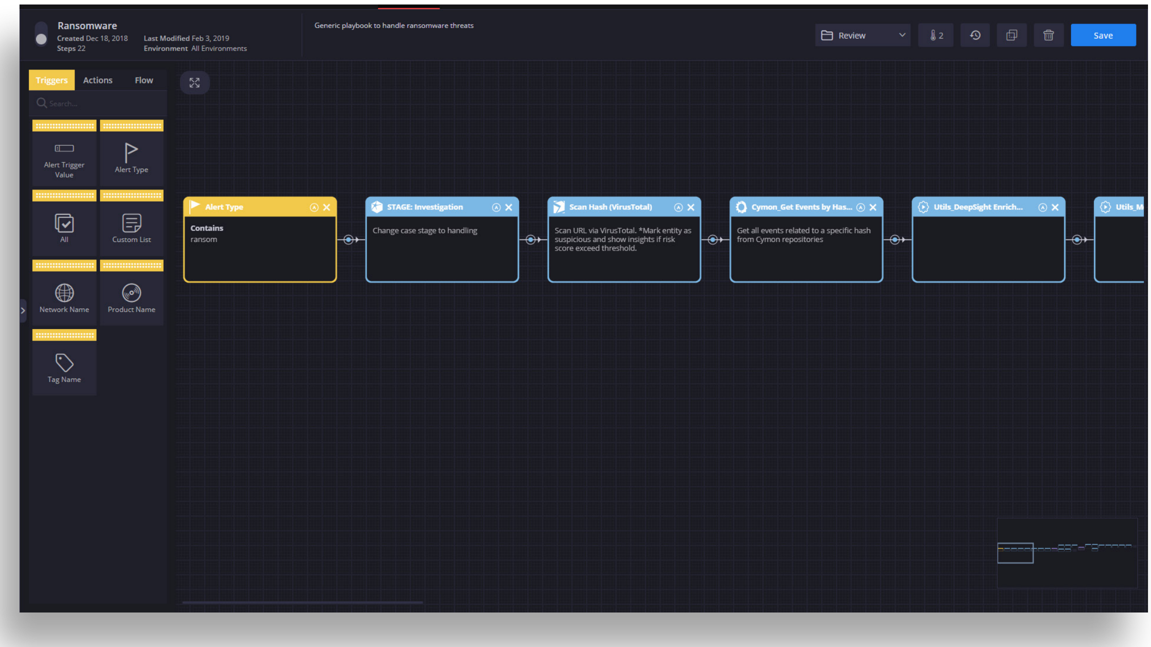
3

If any of these found, mark 'true positive' and escalate.

Containment & Remediation

1. Once phishing is confirmed, send a security alert email to entire organization, notifying them about the targeted activity going on.
2. Block all the malicious URLs found in the alerts (and IP addresses) with firewall.
3. Run thorough anti-malware scans against the users who received the emails (found in alerts).

Ransomware


Ransomware
Created Dec 18, 2018 Steps 22
Last Modified Feb 3, 2019 Environment All Environments

Generic playbook to handle ransomware threats

Alert Type
Contains
ransom

STAGE: Investigation
Change case stage to handling

Scan Hash (VirusTotal)
Scan URL via VirusTotal. *Mark entity as suspicious and show insights if risk score exceed threshold.

Cymon_Get Events by Has...
Get all events related to a specific hash from Cymon repositories

Utils_DeepSight Enrich...

Utils_M

Ransomware is a popular attack vector that involves holding an organization’s data hostage and threatening destruction unless a ransom is paid. The threat moved into the mainstream in 2016 with the WannaCry outbreak, which affected companies around the world.

When the victim employee accidentally installs the malicious payload, the ransomware begins to encrypt all the data on the drive and can only be decrypted with the attacker’s key. If the victim organization pays the ransom – as many companies have been forced to do, fearing capitulation as their only option – the attacker will provide the key to decrypt the data. However, once the ransom is paid, the attackers may decide to stick around and target the victim again through backdoor they created. (Digital crooks aren’t exactly known for keeping their word.)

Details & Workflow

Enrichment & Context

- Verify the log source (network based, anti-virus, host-based or threat intel) and locate/extract the actual suspicious file

Investigation

1

Search third party sources for information on malware and its associated variants to determine the severity and impact of the specific threat.

2

Upload the suspicious binary to VirusTotal and examine the detection ratio.

3

If the detection ratio indicates a malicious signature, escalate to Tier 2 with the gathered information.

4

If the detection ratio indicates of a clean file, make the case 'false positive' and close.

5

If the case was escalated to Tier 2, supply Tier 2 with the following extra information:

a) Binary file (for static/dynamic analysis.

b) Any infected files to determine whether business critical data was affected.

c) Victim's IP and source IP (if the source is known – in case the alert originated from a network-based product).

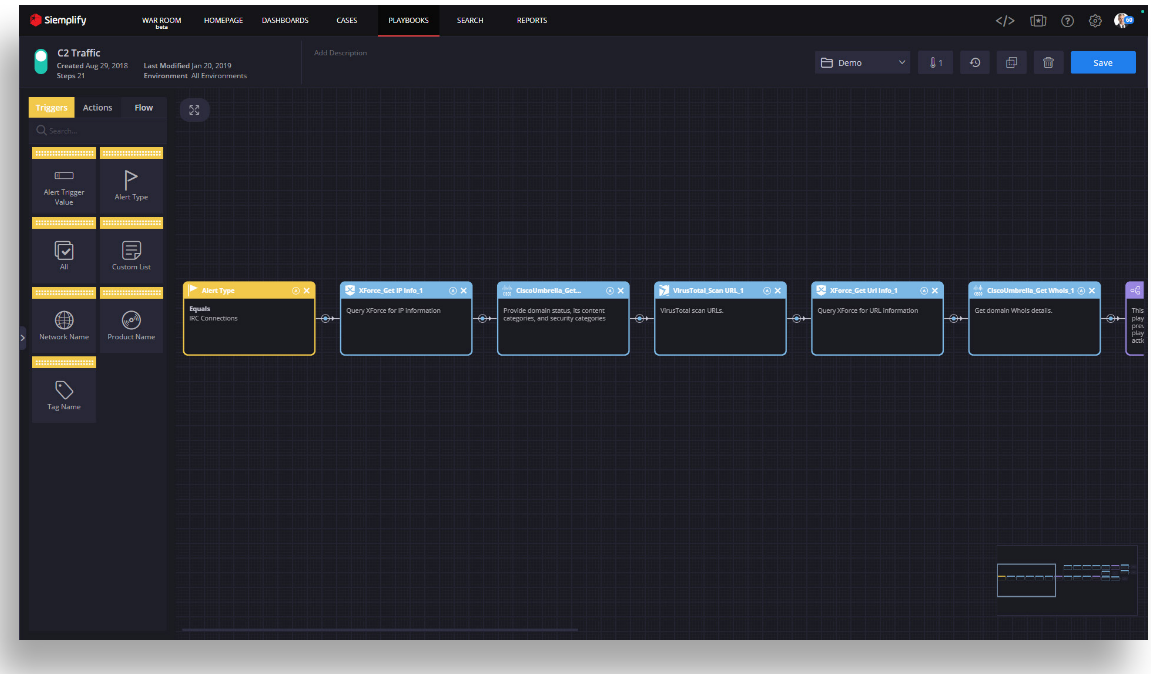
d) Initial information gathered about the malware type/family.

e) Potential impact on victim.

Containment & Remediation

1. If there is a source to the file, block it.
2. Disinfect the affected hosts that were found during the enrichment of Tier 1.
3. Determine the ransomware used to see if recovery will be possible and the way it works.
4. Determine the source of ransomware infection to patch it.
5. If asset value is high:
   a) Is high, recover the data if data decryption tools available for ransomware.
   b) If low, reimage the machine.

C2 Traffic



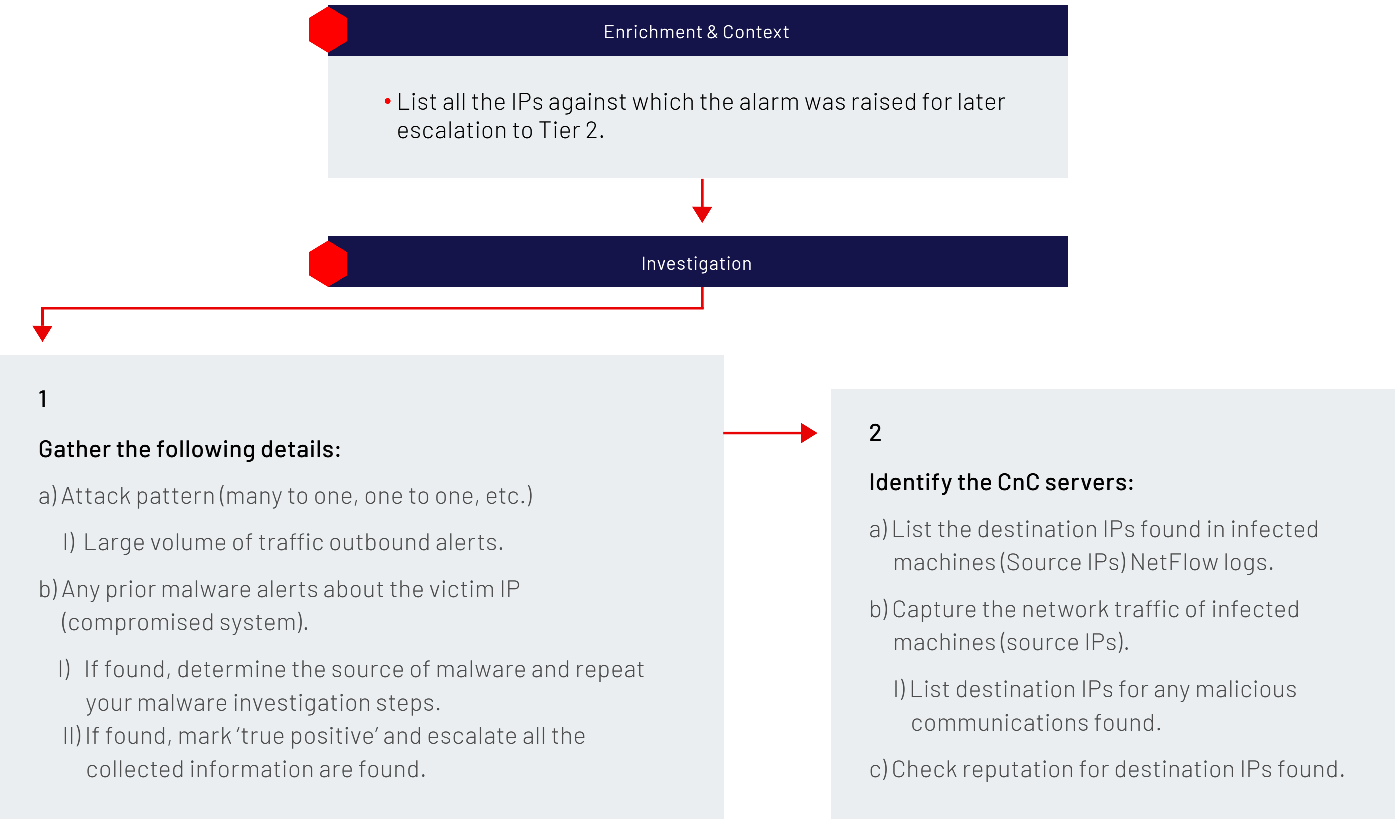
C2 Traffic
Created Aug 29, 2018 Last Modified Jan 20, 2019
Steps 21 Environment All Environments

Alert Type – Equals IRC Connections
XForce_Get IP Info_1 – Query XForce for IP information
CiscoUmbrella_Get... – Provide domain status, its content categories, and security categories
VirusTotal_Scan URL_1 – VirusTotal scan URLs.
XForce_Get Url Info_1 – Query XForce for URL information
CiscoUmbrella_Get WhoIs_1 – Get domain WhoIs details.

Command-and-control (C2) traffic confirms your worst nightmare: that your environment has one, or more, compromised systems. If an attacker can penetrate the network and establish a communication channel to a remote server, they can exfiltrate data in seconds.

Unfortunately, detection of C2 traffic can be difficult, especially when the adversary understands how to remain covert. For instance, advanced attackers will limit the bandwidth and duration of communications so not to alert network monitoring systems. Additionally, attackers may encrypt their communications, making it virtually impossible to discern the type of data moving across – and out of – the network.

Details & Workflow



Enrichment & Context

- List all the IPs against which the alarm was raised for later escalation to Tier 2.

Investigation

1

Gather the following details:

a) Attack pattern (many to one, one to one, etc.)

I) Large volume of traffic outbound alerts.

b) Any prior malware alerts about the victim IP (compromised system).

I) If found, determine the source of malware and repeat your malware investigation steps.

II) If found, mark 'true positive' and escalate all the collected information are found.

2

Identify the CnC servers:

a) List the destination IPs found in infected machines (Source IPs) NetFlow logs.

b) Capture the network traffic of infected machines (source IPs).

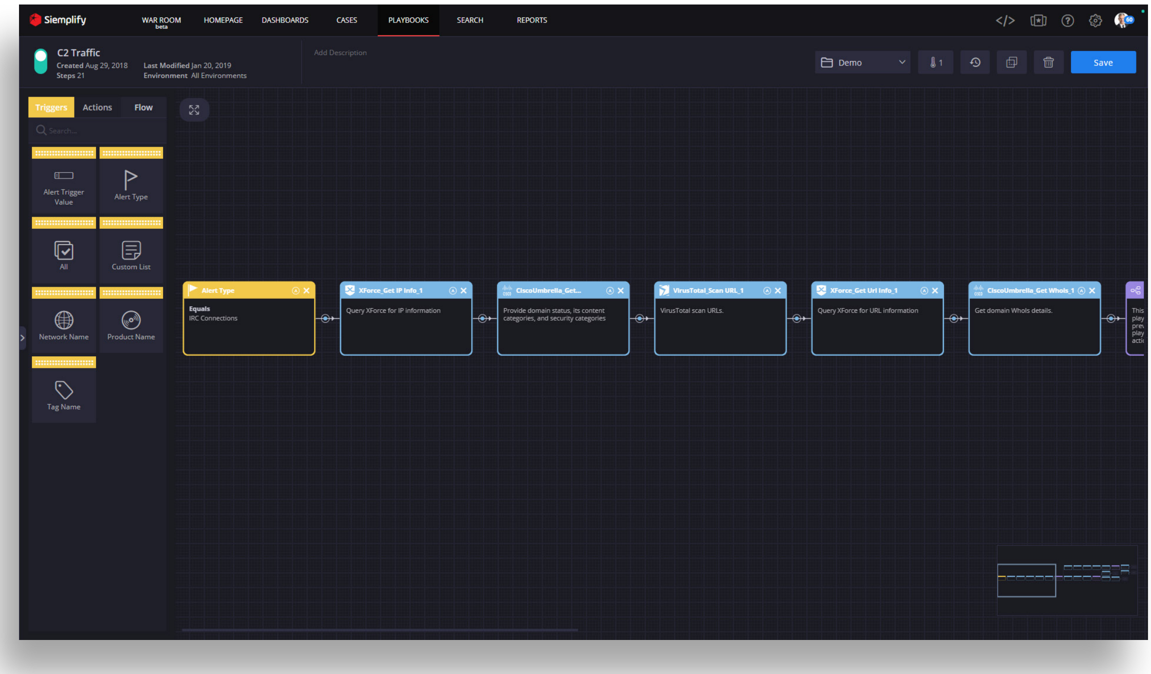
I) List destination IPs for any malicious communications found.

c) Check reputation for destination IPs found.

Containment & Remediation

1. Blacklist all the identified CnC servers with firewall.
2. Hunt for any backdoors on affected hosts and remove them.
3. Hunt for the origin of attack.
   a) Look for any previous alarms for the affected hosts and use corresponding playbook

Insider Threat (Data Leakage)



C2 Traffic
Created Aug 29, 2018
Steps 21
Last Modified Jan 20, 2019
Environment All Environments

Equals
IRC Connections

Query XForce for IP information

Provide domain status, its content categories, and security categories

VirusTotal scan URLs.

Query XForce for URL information

Get domain WhoIs details.

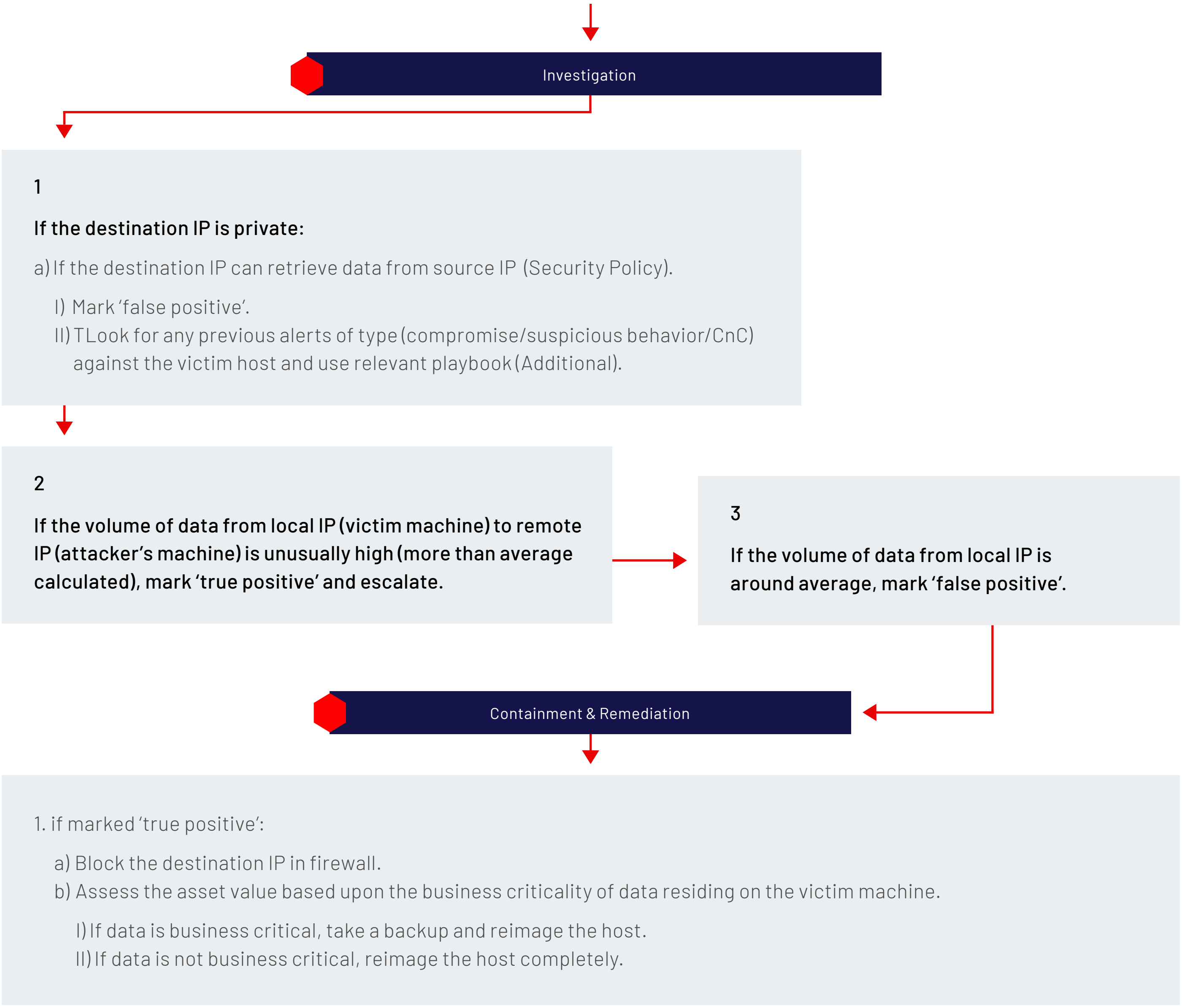
While conceiving that a trusted user could become a threat to the business may be difficult, many examples exist in which a rogue insider got the better of their employer. While most of your security controls are likely geared toward halting external threats, the insider threat can be equally, or even more, damaging. That's because malicious insiders don't need to coax anyone into giving them access to the environment. They're already in and have free run of the network under the guise of routine behavior.

This means they have access to a treasure trove of sensitive data and with a simple USB device can move potentially millions of dollars' worth of data off the network in the snap of a finger – and without raising an eyebrow.

Details & Workflow

Enrichment & Context

- Note the host IP against which the alert was raised (victim machine, source).
- Note the suspicious attacker IP (attacker, destination).
- Study the rule against which the alarm was raised and note the signature/checks in the rule.
- Note the outbound traffic volume of the host within the respective time
- Calculate/extract average traffic per host before the time of alert (from NetFlow).



Investigation

1

If the destination IP is private:

a) If the destination IP can retrieve data from source IP (Security Policy).

I) Mark 'false positive'.
II) TLook for any previous alerts of type (compromise/suspicious behavior/CnC) against the victim host and use relevant playbook (Additional).

2

If the volume of data from local IP (victim machine) to remote IP (attacker's machine) is unusually high (more than average calculated), mark 'true positive' and escalate.

3

If the volume of data from local IP is around average, mark 'false positive'.

Containment & Remediation

1. if marked 'true positive':

a) Block the destination IP in firewall.
b) Assess the asset value based upon the business criticality of data residing on the victim machine.

I) If data is business critical, take a backup and reimage the host.
II) If data is not business critical, reimage the host completely.

CONCLUSION

The key to driving efficient SOC investigation and response is to understand how individual alerts relate to each other. By adopting a context-driven approach, security analyst efficiency and effectiveness will dramatically increase, with cases being closed faster than ever before.

While these gains are obviously desirable, the real added value to the organization comes from limiting an attacker's ability to remain hidden in the shadows because the SOC team is buried under an avalanche of alert data.

Context-driven investigation and response is the future of modern security operations, and these top playbooks will act as an optimal first step for putting alerts and incidents into their proper context.

Playbooks are, of course, valuable even if they are just in flowcharts that you can manually apply to your activities, as they provide a definitive and reliable sequence to shadow during security incidents and investigations, when time is of the essence.

But there is a way to formalize and execute these playbooks using security automation, orchestration and response (SOAR) technology, which can ensure consistency, save you time, track and measure your progress, and provide you with machine learning-based recommendations for best courses of action.

Siemplify playbook capabilities offer the best of both worlds: a simple user interface that makes building and editing actions, triggers, and flows flexible, while incorporating a powerful IDE that delivers virtually unlimited customizability.

For more information, visit siemplify.co.

Siemplify

About Siemplify

Siemplify is a security orchestration, automation and response (SOAR) provider that is redefining security operations for enterprises and MSSPs worldwide. Its holistic security operations platform is a simple, centralized workbench that enables security teams to better investigate, analyze, and remediate threats. And, using automated, repeatable processes and enhanced measurement of KPIs, Siemplify empowers SOC teams to create a culture of continuous improvement. Siemplify's patented context-driven approach reduces caseload and complexity for security analysts, resulting in greater efficiency and faster response times. Founded by Israeli Defense Forces security operations experts with extensive experience running and training numerous SOCs worldwide, Siemplify is headquartered in New York with offices in Tel Aviv.

siemplify.co