

## Siemplify Demo Information and Script

### Key Business Efficiency Improvement

- Time Saving: Workload reduction, automation of processes
- Empowering the Analysts: Noise reduction and focus on real threats, complete workbench
- Consistency: Orchestration of technical and human processes via playbooks
- SOC Management: A central workbench for the manager and the SOC team
- S.A Onboarding: Reduce time of training for new S.A, reduce the level of knowledge required from new S.A

### Key Competitive Differentiators

- Visual Contextual Analysis - Alerts, timeline, insights, explorer, and playbooks
- Our view on what is automation (grouping auto, prioritization auto, auditing auto, playbooks auto)
- Our view on processes (we go process first - make sure it works and then automate)
- Very clean and intuitive GUI that our customers praise us for!
- Very flexible and easy to use - both engineers and analysts can use it for alert response.

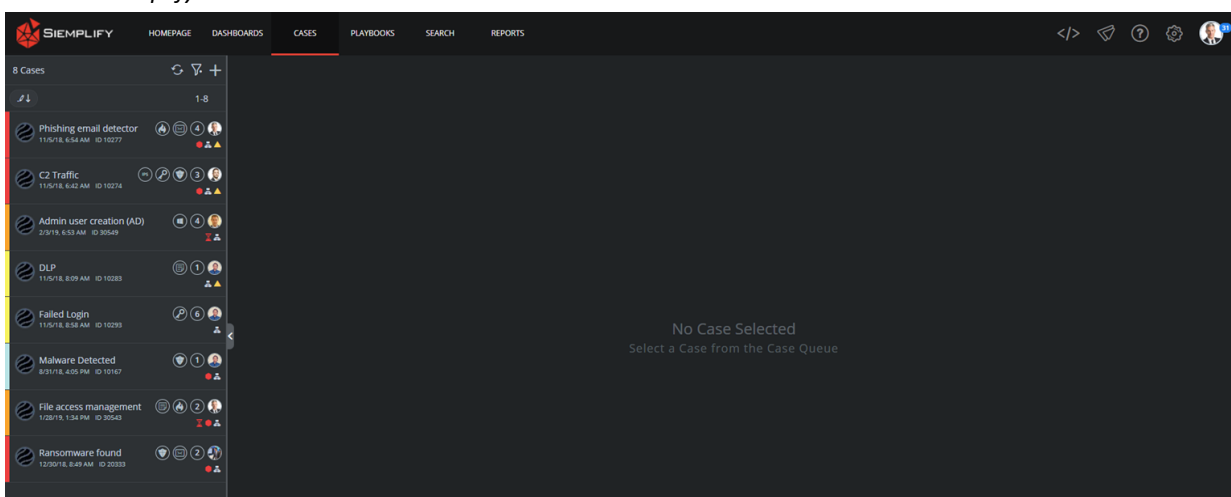
## Demo Script

### ■ Salesforce\HubSpot Analogy

Siemplify provides a central platform for the SOC. A platform where you orchestrate your security tools and the people who work in the SOC with processes that you can measure and improve. Just like sales team have Salesforce and marketing teams have HubSpot or Marketo, security teams use Siemplify.

### ■ Siemplify Cases

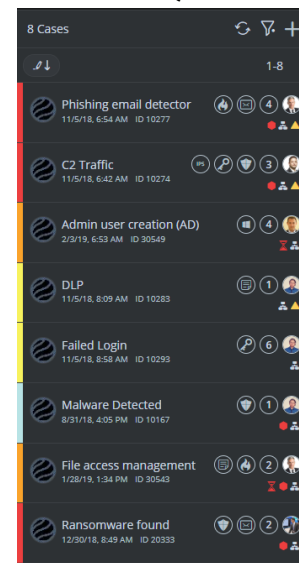
Table 1: Siemplify Cases



Case Name	Timestamp	ID
Phishing email detector	11/5/18, 6:54 AM	ID 10277
C2 Traffic	11/5/18, 6:42 AM	ID 10274
Admin user creation (AD)	2/3/19, 6:53 AM	ID 30549
DLP	11/5/18, 8:09 AM	ID 10283
Failed Login	11/5/18, 8:58 AM	ID 10293
Malware Detected	8/31/18, 4:05 PM	ID 10167
File access management	1/28/19, 1:34 PM	ID 30543
Ransomware found	12/30/18, 8:49 AM	ID 20333

So, to understand how Siemplify works, let me first explain how data is ingested into Siemplify. As part of the Siemplify platform, there are components that we call connectors. A connector is an application that fetches alerts from data sources - SIEM products (ArcSight, QRadar, McAfee, AlienVault and several others), log repositories (like Splunk or ELK), various detection tools, monitored email boxes and more. Multiple connectors can be created in Siemplify to pull alerts from a variety of sources simultaneously, all consolidated in one queue (**show queue Reference Table 2**) presented in one language to the analysts regardless of the source product. As alerts are pulled into Siemplify they are wrapped in cases and placed into the queue that can be prioritized and filtered for different tiers and teams.

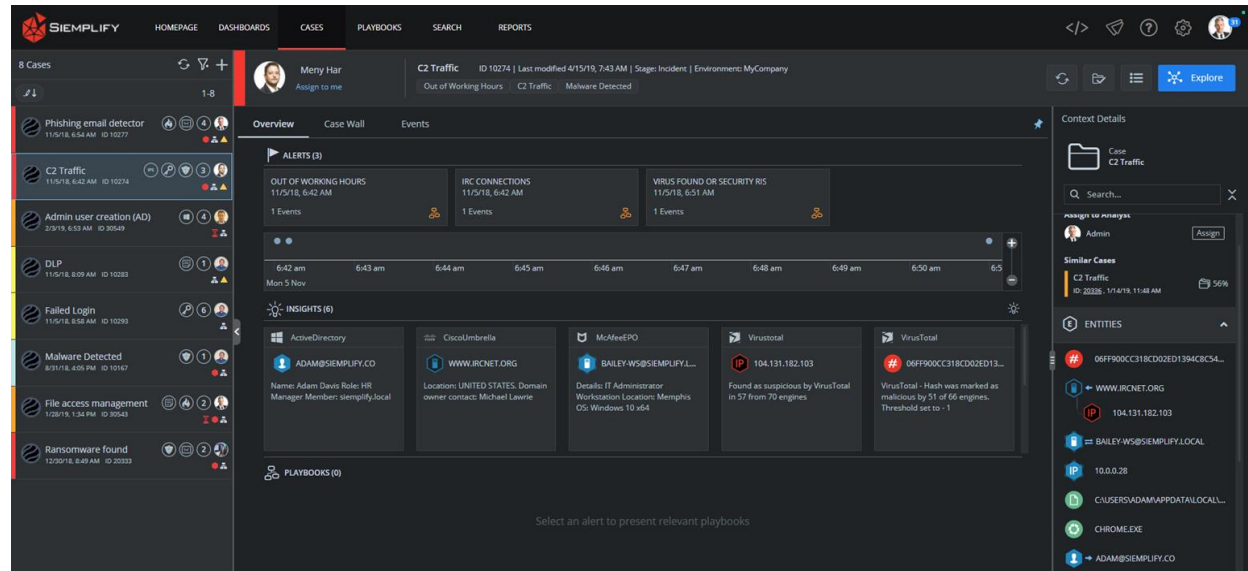
Table 2: Case Queue



Case Name	Timestamp	ID
Phishing email detector	11/5/18, 6:54 AM	ID 10277
C2 Traffic	11/5/18, 6:42 AM	ID 10274
Admin user creation (AD)	2/3/19, 6:53 AM	ID 30549
DLP	11/5/18, 8:09 AM	ID 10283
Failed Login	11/5/18, 8:58 AM	ID 10293
Malware Detected	8/31/18, 4:05 PM	ID 10167
File access management	1/28/19, 1:34 PM	ID 30543
Ransomware found	12/30/18, 8:49 AM	ID 20333

Reference Table 3 for this part of the demo

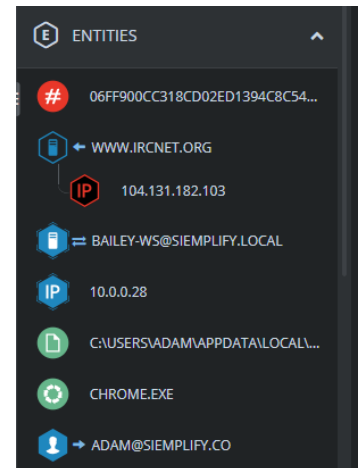
Table 3: Case Overview



## ■ Explain Cases

Each case is like a ticket. It can be closed/opened, assigned, escalated and much more. **[click case with one alert]** As an alert is pulled into Simplifi it will look like this **[point to case]** this gives you the information needed for your analysts to make a decision on what to do next. Simplifi doesn't just take the alerts from the SIEM and turn them into cases with one alert we also look at the information in the cases and we group cases into one cases giving you the complete view of the threat not just a single alert **[click case with multiple alerts]**. Within the case you are also able to see what is happening **[point to alerts in the case]** when it happened **[point to timeline]** and who was involved in the alert **[point to entities: reference table 4]**. The entities are not just a string of characters it is an object of information **[click hash entity]**.











Table 4: Entities



## Entity Benefit

When the hash entity is clicked *Reference Table 6*, I can see the historical details about the entity. You can see previous cases that this entity has been involved **[point to last cases section]** as well as analysis that may have been entered before. This allows me to be able to work more efficiently because I can re-use the analysis that was done in the past. The more the analysis use the system and store information the more powerful it becomes. An analysis can also use the contextual details that have been gathered from enrichment sources like VirusTotal, XForce, ThreatConnect or ActiveDirectory and others to make decisions. **[Use 'Case Screen' bottom right hand corner. Scroll to bottom of entity details - show information from a enrichment source]**






Table 5: Entity Details

<div>  06FF900C318C02ED1394C8C34A0066         </div> <div>           This entity was involved in 6 cases during the last 3 months           <span>0 Malicious Cases</span> </div> <div>           MyCompany         </div>															
<div> <div>ENTITY DETAILS</div> <div> <div>DEFAULT</div> <table> <thead> <tr> <th>FIELD NAME</th><th>VALUE</th></tr> </thead> <tbody> <tr> <td>Type</td><td>FILEHASH</td></tr> <tr> <td>Environment</td><td>MyCompany</td></tr> <tr> <td>IsInternalAsset</td><td>True</td></tr> <tr> <td>IsSuspicious</td><td>True</td></tr> <tr> <td>IsEnriched</td><td>True</td></tr> <tr> <td>IsVulnerable</td><td>False</td></tr> </tbody> </table> </div> </div>		FIELD NAME	VALUE	Type	FILEHASH	Environment	MyCompany	IsInternalAsset	True	IsSuspicious	True	IsEnriched	True	IsVulnerable	False
FIELD NAME	VALUE														
Type	FILEHASH														
Environment	MyCompany														
IsInternalAsset	True														
IsSuspicious	True														
IsEnriched	True														
IsVulnerable	False														
<div> <div>LINKED ENTITIES (2)</div> <div> <div>  PAYCHECK_DEC15.PDF           </div> <div>  CAUSERSADAMPAPPDATA\LOCAL\TEMP\SMON\1307961920\33095381194           </div> </div> </div>															
<div> <div>LAST CASES (5)</div> <div> <div>  symantecepriskfile 1/20/19, 9:59 AM <a href="#">ID: 20224</a> </div> <div>  symantecepriskfile 1/20/19, 9:58 AM <a href="#">ID: 20223</a> </div> <div>  symantecepriskfile 1/21/19, 4:57 AM <a href="#">ID: 20249</a> </div> <div>  symantecepriskfile 1/20/19, 10:40 AM <a href="#">ID: 20285</a> </div> <div>  symantecepriskfile 1/20/19, 10:39 AM <a href="#">ID: 20283</a> </div> </div> </div>															
<div> <div>CASE DISTRIBUTION</div> <div> <div>Product</div> <div>  symantecepriskfile           </div> </div> </div>															
<div> <div>ENTITY LOG</div> <div> <div>  This is a new note Youn B.           </div> <div>             3/18/19, 7:30 AM           </div> </div> </div>															

## ▪ Insights

**[click back to cases - select C2 case]** I talked about how you can see what's happening, when it happened, who was involved. You are also able to see key information about the cases so the analyst can make faster decisions and we show this to you as an insight. Within each of the cases in order to understand what is happening with in the case you need to click through several screens to get to the right information. Siemplify believes in getting analysts the information faster, insights are used to provide the details of the information that was needed to understand what was going on within the case. We bring those to the forefront so that the analysts can get to the answer faster and be able to decide on what to do next without having to click through several screens. **[point to insights]**

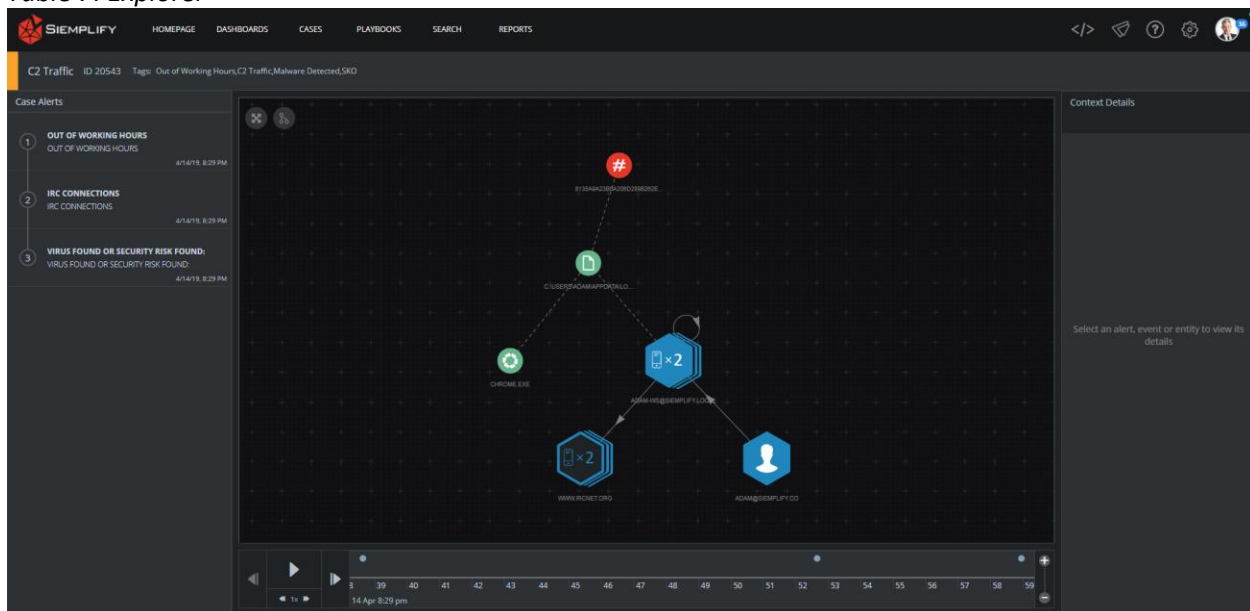
Table 6: Insights

INSIGHTS (6)				
<b>ActiveDirectory</b>  ADAM@SIEMPLIFY.CO Name: Adam Davis Role: HR Manager Member: siemplify.local	<b>CiscoUmbrella</b>  WWW.IRCNET.ORG Location: UNITED STATES, Domain owner contact: Michael Lawrie	<b>McAfeeEPO</b>  BAILEY-WS@SIEMPLIFY.L... Details: IT Administrator Workstation Location: Memphis OS: Windows 10 x64	<b>VirusTotal</b>  104.131.182.103 Found as suspicious by VirusTotal in 57 from 70 engines	<b>VirusTotal</b>  06FF900CC318CD02ED13... VirusTotal - Hash was marked as malicious by 51 of 66 engines. Threshold set to - 1

## ▪ Explorer

In order to better understand the case, the explorer button allows you to preset the case in a graphical representation so that you can more easily understand what is going on. This also allows your tier 2 tier 3 analysts to come in and start to take action manually on things that Siemplify has found to be malicious.

Table 7: Explorer



- Case Wall (Optional)

Also, everything that has been done within a case is automatically documented within the case wall. This is like a chain-of-custody of everything that has been done within a case. Everything from case creation to case closure is documented and can be reported on.

Table 8: Case Wall

Overview

Case Wall

Events

🕒

🗨

📄

📋

🔍

⚙️

👤

All Alerts

⌵

☆

🔍

4/14/19, 8:30 PM

🔍

Action Name

Simplify\_Case Comment

Alert Name

Irc Connections

Playbook Name

C2 Traffic

Action Status

Completed

Result

Comment added to case:  
nothing suspicious or malicious ...

📄

Show More ⌵

🔍

System

⚙️

4/14/19, 8:31 PM

Entity Insight

🔍

VirusTotal

8135A9A23...

#

VirusTotal - Hash was marked as malicious by 50 of 64 engines. Threshold set to - 1

Alert Name

Virus Found Or Security Risk Found:

🔍

4/14/19, 8:31 PM

🔍

Action Name

VirusTotal\_Scan Hash

Alert Name

Virus Found Or Security Risk Found:

Playbook Name

Malware - Detected

Action Status

Completed

Result

The following hashes were subm...

📄

\*Check online report for full det...

Show More ⌵

🔍

System

🔍

4/14/19, 8:31 PM

🔍

Action Name

VirusTotal\_Scan IP

Alert Name

Virus Found Or Security Risk Found:

Playbook Name

Malware - Detected

Action Status

Completed

Result

The following IPs were submitte...

📄

\*Check online report for full det...

Show More ⌵

🔍

System

- Playbooks

When looking at automation it is important to first start with a process that has been well defined and then start to add automated steps. Building a playbook is very simple to do we provide a drag and drop designed that allows easy modification and create of playbooks.

Table 9: Playbook Designer

The screenshot displays the SIMPLIFY Playbooks interface. The top navigation bar includes links for HOMEPAGE, DASHBOARDS, CASES, **PLAYBOOKS**, SEARCH, and REPORTS. The left sidebar contains a 'Playbooks List' with a search bar and a list of playbooks, including 'Failed Login' (selected), 'Malware / Suspicious file', 'Malware', 'Phishing VI', 'Suspicious IP', 'Usecases', 'Default', and 'Use Cases'. The main workspace is titled 'Failed Login' and shows a flowchart in 'Review' mode. The flowchart starts with a 'Tag Name' trigger, followed by actions: 'Enrich entities', 'Add Entity Info', 'Get Cybereason ID', 'Get Similar Cases', and 'Save into cybereason'. The 'Review' tab is active, showing a 'Description' field and a 'Save' button.

## ■ Dashboards

We take the data that we are collecting and give you the ability to measure key KPIs. Everything we are collecting can be filtered and measured with the Dashboards allowing high-level management to get a good glimpse into how the SOC is performing. Siemplify also provides the data to giving you the ability to drill down the incidents and measure efficiency.

Table 10: Dashboard



## Optional

- Click Homepage

We want analysts have a good view into what they have to do for the data so we provide them a screen that they can go to in order to respond to tasks and see the cases that have been assigned to them.

Table 11: Homepage

