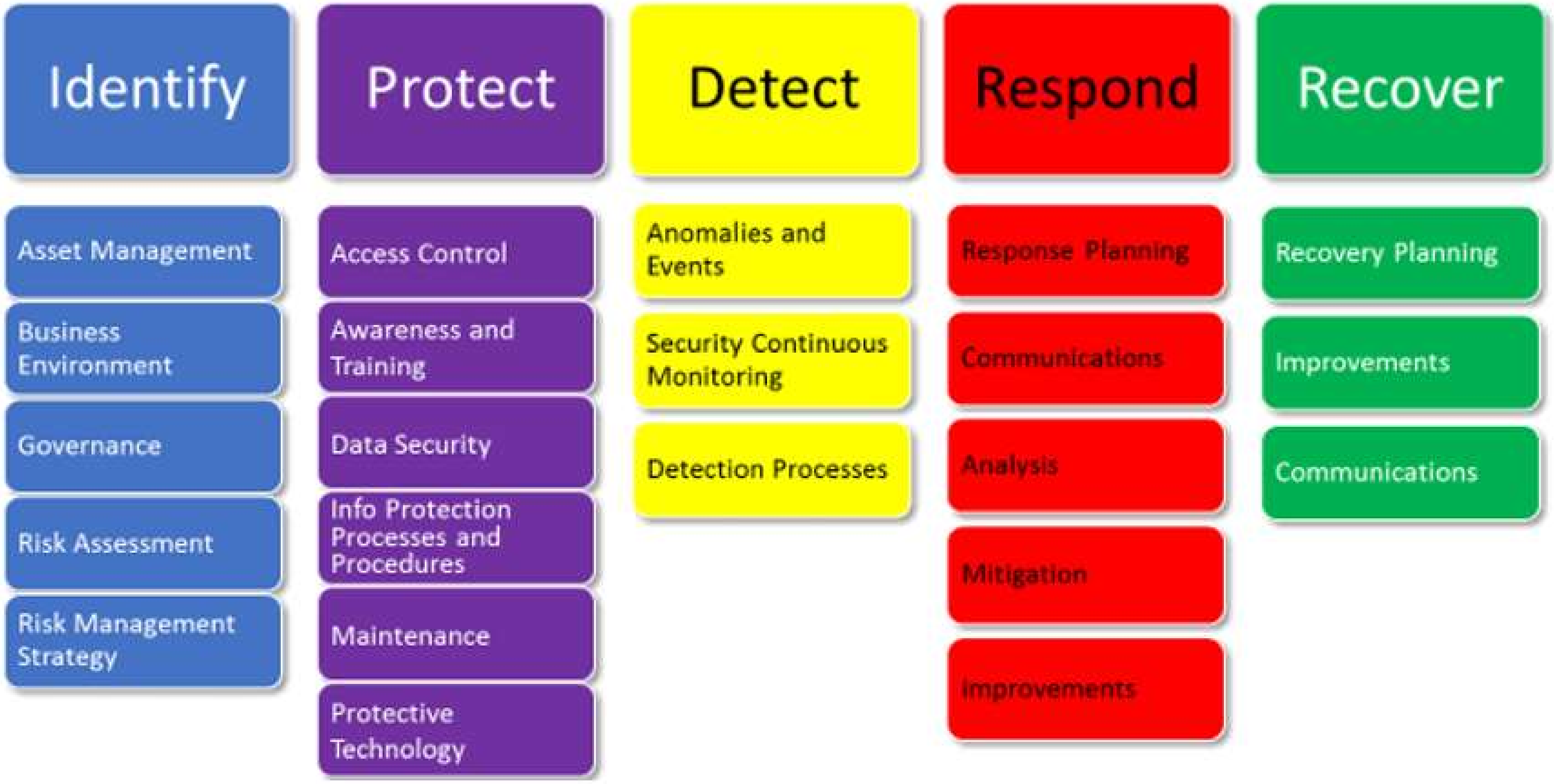
DAY 5

SOC INVESTIGATION PROCESS

- PRESENTED BY: ADITYA JAMKHANDE

NIST CYBER SECURITY FRAMEWORK



Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

CORE RESPONSIBILITIES

- A SOC team has two core responsibilities:
- **Maintaining security monitoring tools** – The team must maintain and update tools regularly. Without the correct and most up-to-date tools, they can't properly secure systems and networks. Team members should maintain the tools used in every part of the security process.
- **Investigate suspicious activities** – The SOC team should investigate suspicious and malicious activity within the networks and systems. Generally, your SIEM or analytics software will issue alerts which the team then analyzes and examines, triages, and discovers the extent of the threat.

STEPS FOLLOWED BY ANALYST

- Monitoring
- Triage
- Basic Investigation
- Deep Dive Investigation
- Remediation
- Closure

MONITORING

- Cybersecurity monitoring is the process of continuously observing what is happening in your organization's ecosystem with the aim of detecting cyber threats and data breaches.
- Done in the following way:
  - Monitor alerts, dashboards and reports
  - Identify Indicators of compromise or indicators of attack
  - Perform adhoc investigation

ALERTS, DASHBOARD AND REPORTS

Alerts

- An alert is based on a scheduled saved or real time search that whenever certain conditions are overcome, generates one or more actions to be executed

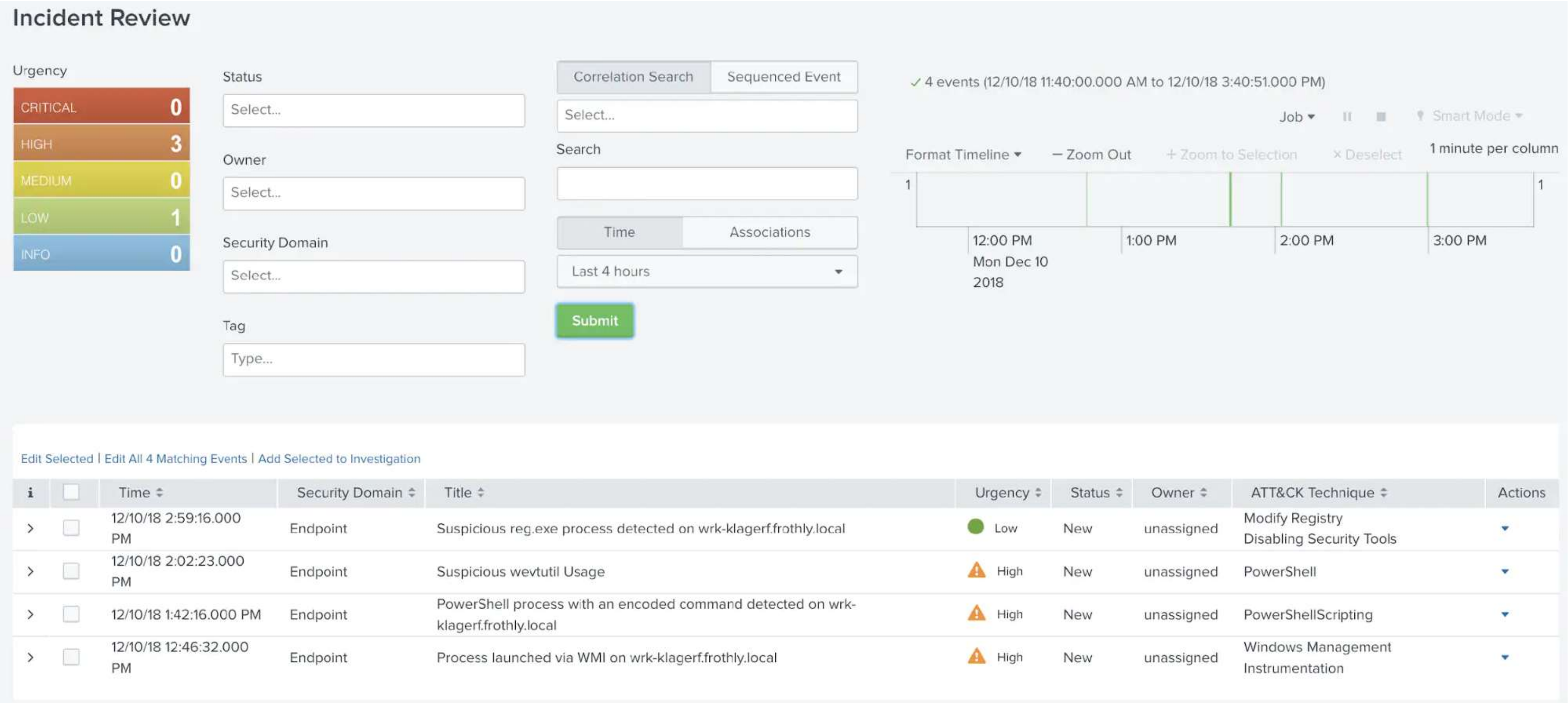
Dashboards

- A dashboard is a visual display of all of your data. While it can be used in all kinds of different ways, its primary intention is to provide information at-a-glance, such as KPIs

Reports

- A cybersecurity report presents critical information about cybersecurity threats, risks within a digital ecosystem, gaps in security controls, and the performance of security programs at regular intervals

SPLUNK NOTABLES (ALERTS) EXAMPLE



Incident Review

Urgency

CRITICAL	0
HIGH	3
MEDIUM	0
LOW	1
INFO	0

Status: Select...

Owner: Select...

Security Domain: Select...

Tag: Type...

Correlation Search | Sequenced Event: Select...

Search:

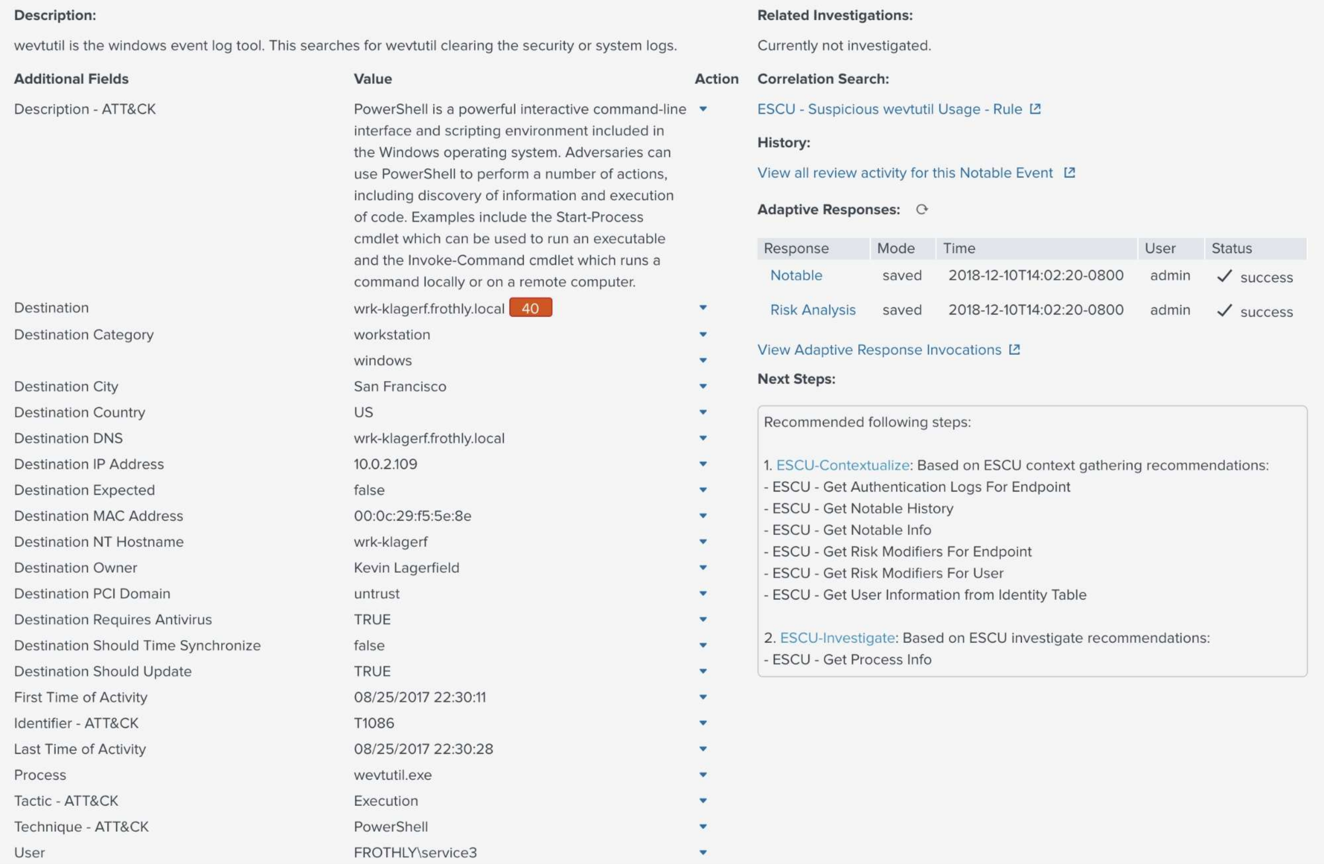
Time | Associations: Last 4 hours

✓ 4 events (12/10/18 11:40:00.000 AM to 12/10/18 3:40:51.000 PM)

Edit Selected | Edit All 4 Matching Events | Add Selected to Investigation

i	□	Time	Security Domain	Title	Urgency	Status	Owner	ATT&CK Technique	Actions
›	□	12/10/18 2:59:16.000 PM	Endpoint	Suspicious reg.exe process detected on wrk-klagerf.frothly.local	● Low	New	unassigned	Modify Registry Disabling Security Tools	▾
›	□	12/10/18 2:02:23.000 PM	Endpoint	Suspicious wevtutil Usage	⚠ High	New	unassigned	PowerShell	▾
›	□	12/10/18 1:42:16.000 PM	Endpoint	PowerShell process with an encoded command detected on wrk-klagerf.frothly.local	⚠ High	New	unassigned	PowerShellScripting	▾
›	□	12/10/18 12:46:32.000 PM	Endpoint	Process launched via WMI on wrk-klagerf.frothly.local	⚠ High	New	unassigned	Windows Management Instrumentation	▾

SPLUNK NOTABLES (ALERTS) EXAMPLE



Description:

wevtutil is the windows event log tool. This searches for wevtutil clearing the security or system logs.

Additional Fields	Value	Action
Description - ATT&CK	PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer.	▾
Destination	wrk-klagerf.frothly.local 40	▾
Destination Category	workstation	▾
	windows	▾
Destination City	San Francisco	▾
Destination Country	US	▾
Destination DNS	wrk-klagerf.frothly.local	▾
Destination IP Address	10.0.2.109	▾
Destination Expected	false	▾
Destination MAC Address	00:0c:29:f5:5e:8e	▾
Destination NT Hostname	wrk-klagerf	▾
Destination Owner	Kevin Lagerfield	▾
Destination PCI Domain	untrust	▾
Destination Requires Antivirus	TRUE	▾
Destination Should Time Synchronize	false	▾
Destination Should Update	TRUE	▾
First Time of Activity	08/25/2017 22:30:11	▾
Identifier - ATT&CK	T1086	▾
Last Time of Activity	08/25/2017 22:30:28	▾
Process	wevtutil.exe	▾
Tactic - ATT&CK	Execution	▾
Technique - ATT&CK	PowerShell	▾
User	FROTHLY\service3	▾

Related Investigations:

Currently not investigated.

Correlation Search:

ESCU - Suspicious wevtutil Usage - Rule

History:

View all review activity for this Notable Event

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2018-12-10T14:02:20-0800	admin	✓ success
Risk Analysis	saved	2018-12-10T14:02:20-0800	admin	✓ success

View Adaptive Response Invocations

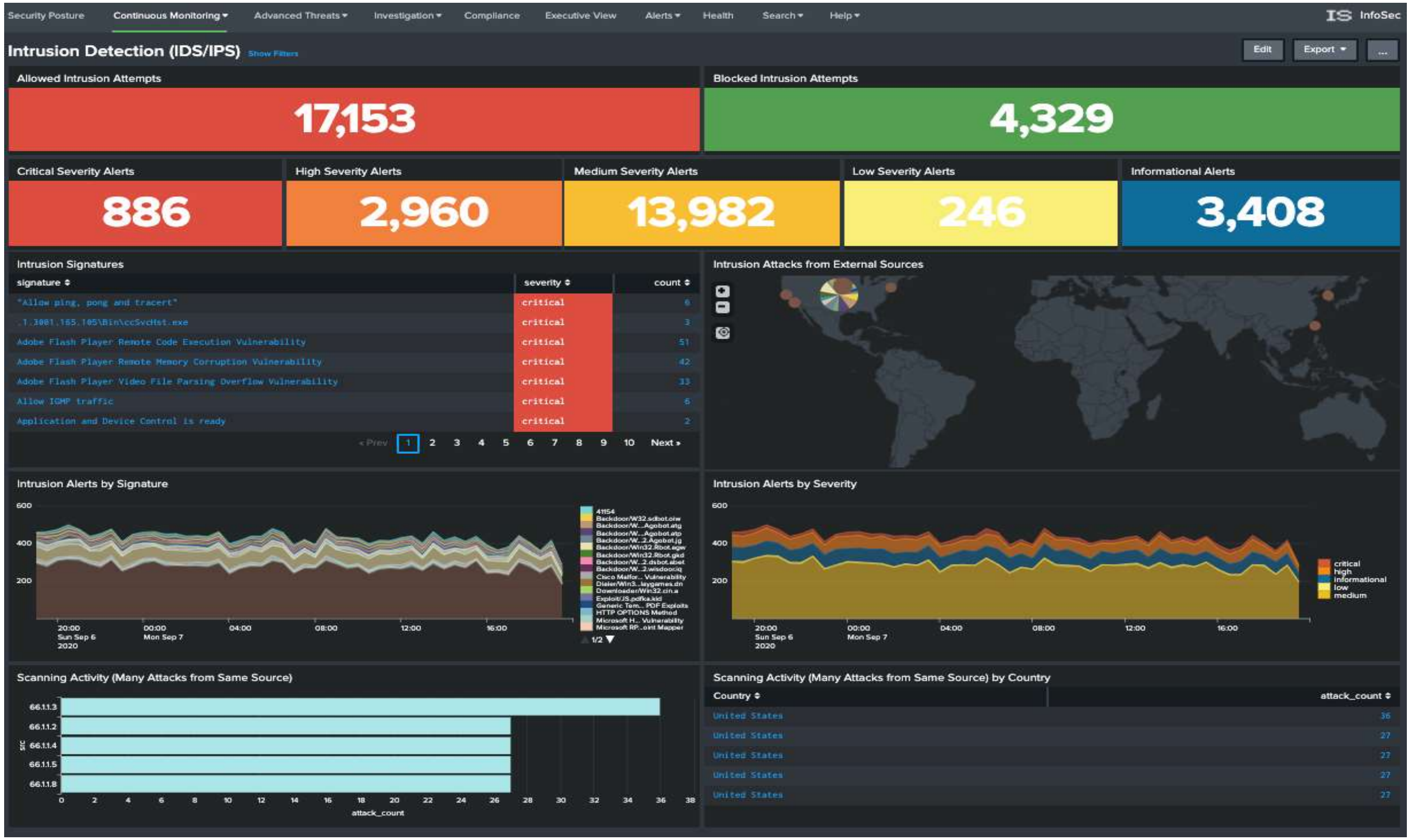
Next Steps:

Recommended following steps:

1. ESCU-Contextualize: Based on ESCU context gathering recommendations:
- ESCU - Get Authentication Logs For Endpoint
- ESCU - Get Notable History
- ESCU - Get Notable Info
- ESCU - Get Risk Modifiers For Endpoint
- ESCU - Get Risk Modifiers For User
- ESCU - Get User Information from Identity Table

2. ESCU-Investigate: Based on ESCU investigate recommendations:
- ESCU - Get Process Info

SPLUNK DASHBOARD EXAMPLE



Intrusion Detection (IDS/IPS)

Allowed Intrusion Attempts: 17,153

Blocked Intrusion Attempts: 4,329

Critical Severity Alerts: 886

High Severity Alerts: 2,960

Medium Severity Alerts: 13,982

Low Severity Alerts: 246

Informational Alerts: 3,408

Intrusion Signatures

signature ⇕	severity ⇕	count ⇕
"Allow ping, pong and tracert"	critical	6
.1.3001.165.105\Bin\ccSvcHst.exe	critical	3
Adobe Flash Player Remote Code Execution Vulnerability	critical	51
Adobe Flash Player Remote Memory Corruption Vulnerability	critical	42
Adobe Flash Player Video File Parsing Overflow Vulnerability	critical	33
Allow IGMP traffic	critical	6
Application and Device Control is ready	critical	2

Intrusion Attacks from External Sources

Intrusion Alerts by Signature

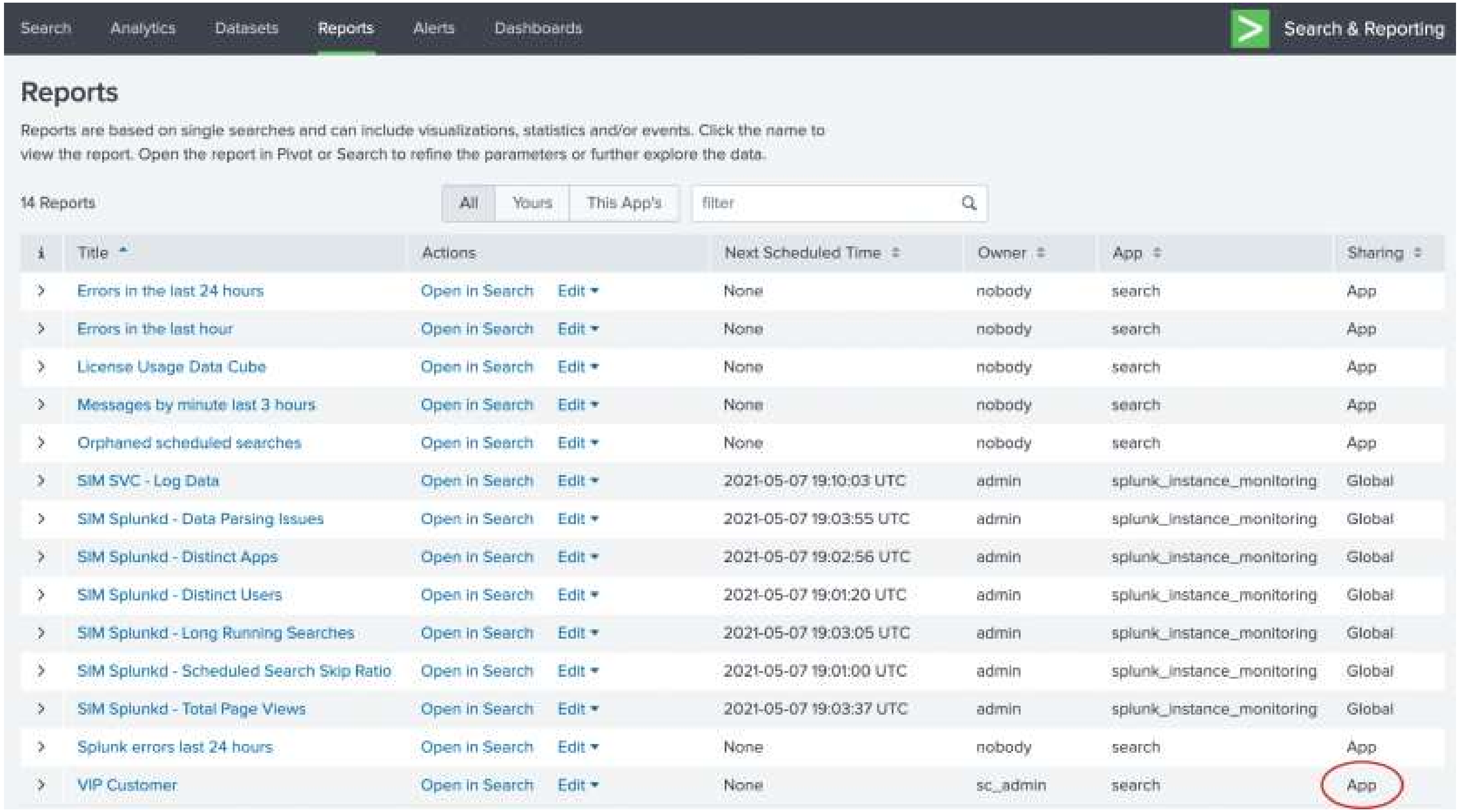
Intrusion Alerts by Severity

Scanning Activity (Many Attacks from Same Source)

Scanning Activity (Many Attacks from Same Source) by Country

Country ⇕	attack_count ⇕
United States	36
United States	27
United States	27
United States	27
United States	27

SPLUNK REPORTS EXAMPLE



Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

14 Reports

i	Title ▲	Actions		Next Scheduled Time ⇕	Owner ⇕	App ⇕	Sharing ⇕
›	Errors in the last 24 hours	Open in Search	Edit ▾	None	nobody	search	App
›	Errors in the last hour	Open in Search	Edit ▾	None	nobody	search	App
›	License Usage Data Cube	Open in Search	Edit ▾	None	nobody	search	App
›	Messages by minute last 3 hours	Open in Search	Edit ▾	None	nobody	search	App
›	Orphaned scheduled searches	Open in Search	Edit ▾	None	nobody	search	App
›	SIM SVC - Log Data	Open in Search	Edit ▾	2021-05-07 19:10:03 UTC	admin	splunk_instance_monitoring	Global
›	SIM Splunkd - Data Parsing Issues	Open in Search	Edit ▾	2021-05-07 19:03:55 UTC	admin	splunk_instance_monitoring	Global
›	SIM Splunkd - Distinct Apps	Open in Search	Edit ▾	2021-05-07 19:02:56 UTC	admin	splunk_instance_monitoring	Global
›	SIM Splunkd - Distinct Users	Open in Search	Edit ▾	2021-05-07 19:01:20 UTC	admin	splunk_instance_monitoring	Global
›	SIM Splunkd - Long Running Searches	Open in Search	Edit ▾	2021-05-07 19:03:05 UTC	admin	splunk_instance_monitoring	Global
›	SIM Splunkd - Scheduled Search Skip Ratio	Open in Search	Edit ▾	2021-05-07 19:01:00 UTC	admin	splunk_instance_monitoring	Global
›	SIM Splunkd - Total Page Views	Open in Search	Edit ▾	2021-05-07 19:03:37 UTC	admin	splunk_instance_monitoring	Global
›	Splunk errors last 24 hours	Open in Search	Edit ▾	None	nobody	search	App
›	VIP Customer	Open in Search	Edit ▾	None	sc_admin	search	App

TRIAGE

- To triage means to assign a level of importance or urgency to incidents, which then determines the order in which they will be investigated
- Done in the following way:
  - Review the alerts by actively investigating the trigger
  - Close an alert if it is qualified as false positive
  - Park the alert if same offense triggered multiple time to understand it is false positive or legit one
  - Categorize the alerts based on severity and impact

BASIC INVESTIGATION

- It is the process of investigating, analyzing and gathering relevant evidences about the security incident
- Done in the following way:
  - Identify which Rule triggered an alert
  - Try to collect as much information as possible.
  - Identify which log sources & systems triggered the alert
  - Identify users or potential actors involved in the an incident
  - Search past alerts/incidents
  - Understand attack vectors
  - Use the available threat intelligence
  - Search related events, flows, vulnerabilities and active exploits

DEEP DIVE INVESTIGATION

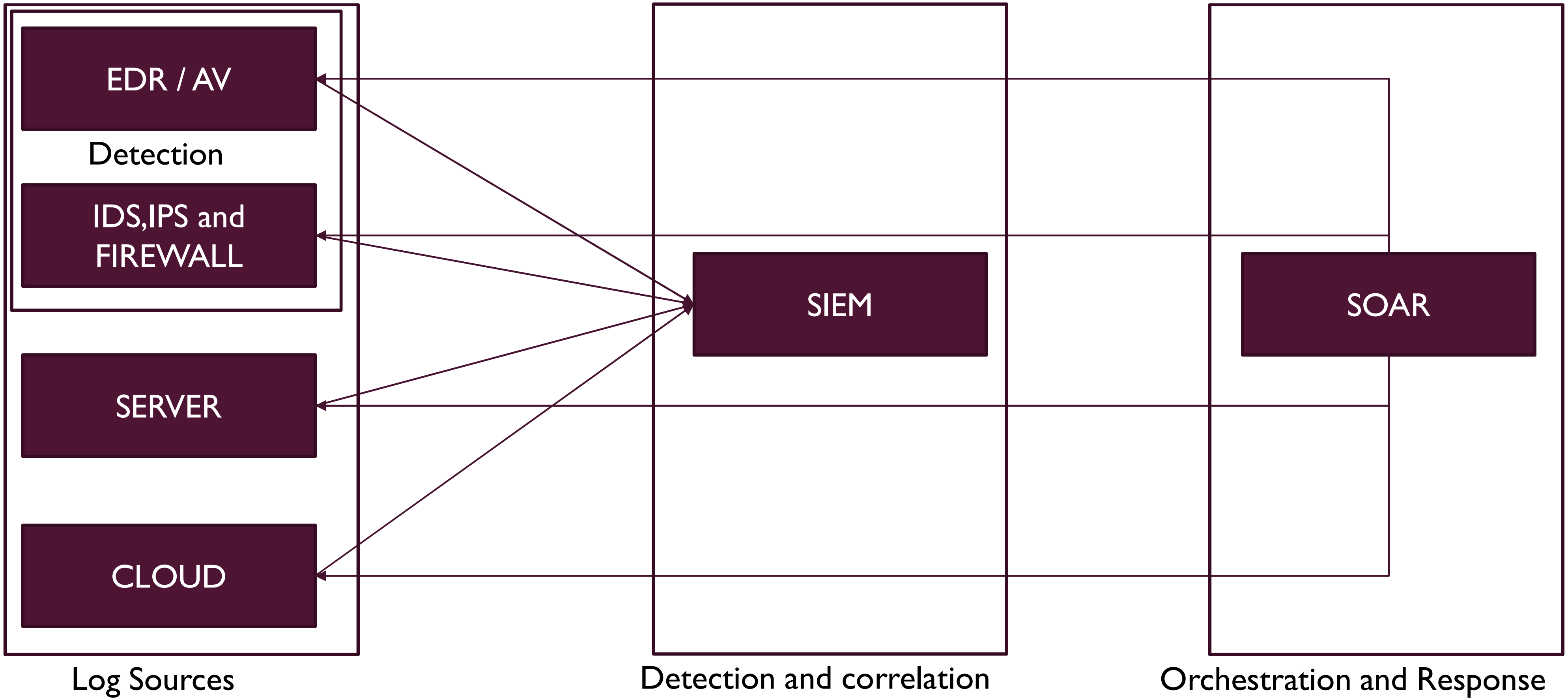
- Perform threat hunting based on the IOC’s and IOA’s
- Identify the related activity during the given timeline
- Try to correlate the actions and identify the source of infection or the root cause of the activity
- Use advanced detection and remediation mechanisms like EDR

REMEDIATION

- Gather incident information as below and forward it to respective teams
  - List of affected hosts
  - Potentials Actors / users
  - attack vector information

- If the incident is a false positive – create tuning request and send to SOC Admin Team

INCIDENT DETECTION AND RESPONSE – COMPLETE PICTURE



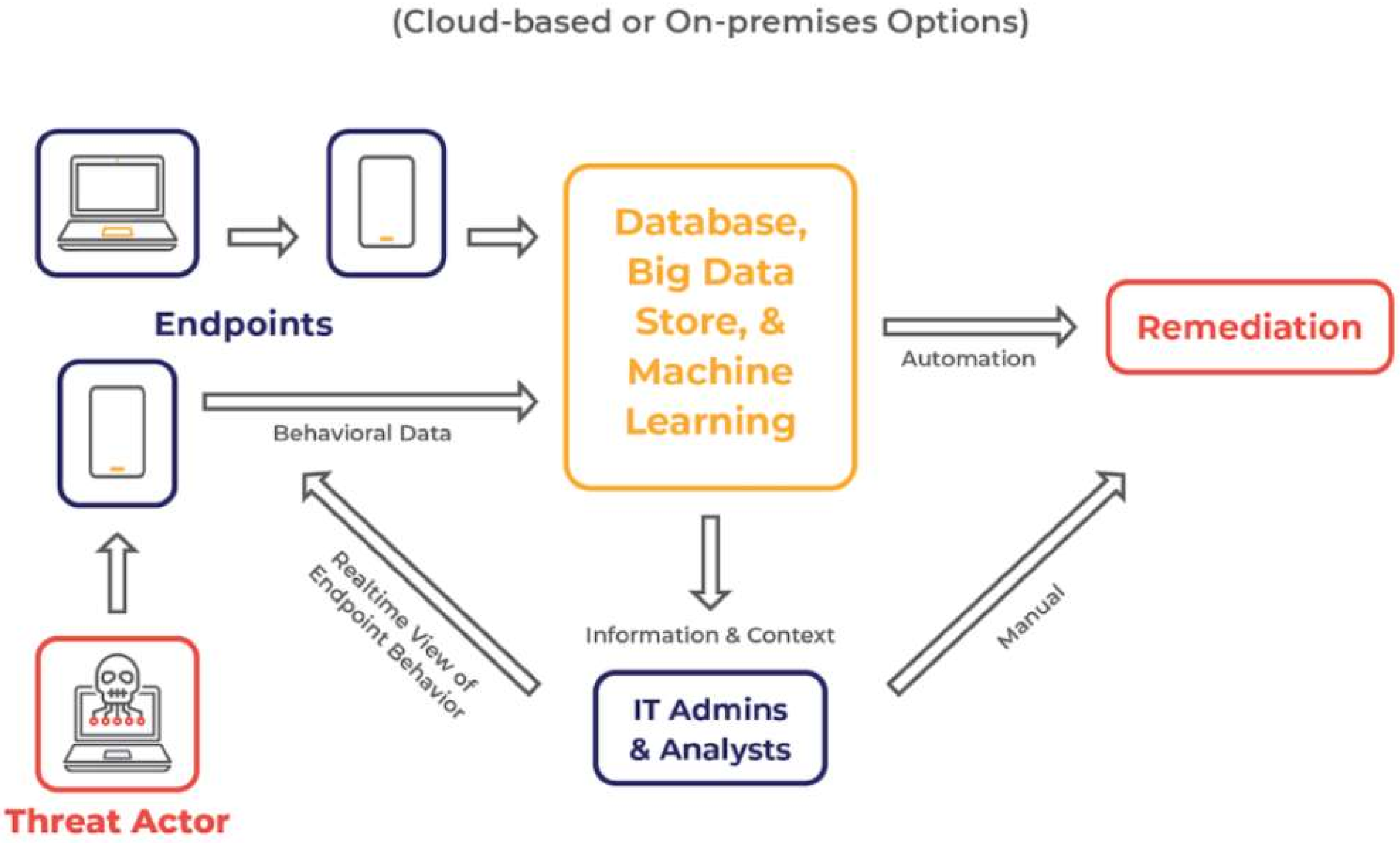
WHAT IS AN EDR

- Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

- The primary functions of an EDR security system are to:
  - Monitor and collect activity data from endpoints that could indicate a threat
  - Analyze this data to identify threat patterns
  - Automatically respond to identified threats to remove or contain them, and notify security personnel
  - Forensics and analysis tools to research identified threats and search for suspicious activities

Credits: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html

HOW EDR WORKS


(Cloud-based or On-premises Options)
Endpoints
Database, Big Data Store, & Machine Learning
Automation
Remediation
Behavioral Data
Realtime View of Endpoint Behavior
Information & Context
Manual
IT Admins & Analysts
Threat Actor

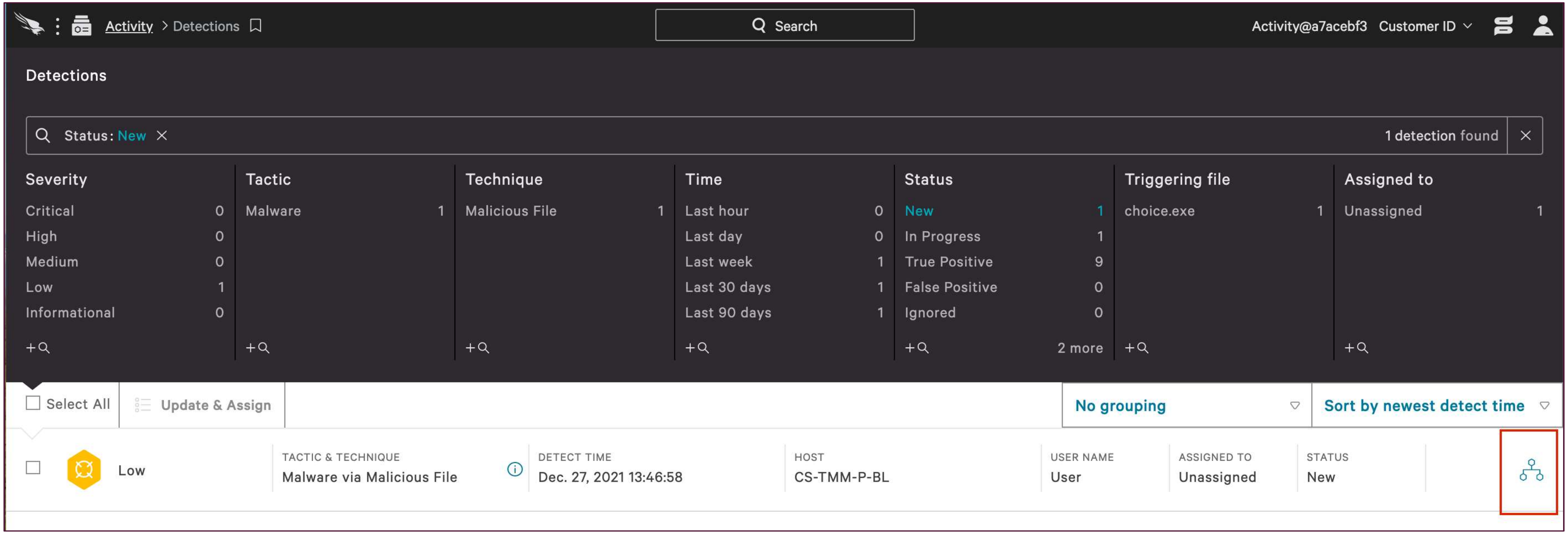
KEY COMPONENTS OF EDR SECURITY

- EDR security provides an integrated hub for the collection, correlation, and analysis of endpoint data, as well as for coordinating alerts and responses to immediate threats. EDR tools have three basic components:
- **Endpoint data collection agents:** Software agents conduct endpoint monitoring and collect data—such as processes, connections, volume of activity, and data transfers—into a central database
- **Automated response:** Pre-configured rules in an EDR solution can recognize when incoming data indicates a known type of security breach and triggers an automatic response, such as to log off the end user or send an alert to a staff member

- **Automated response:** Pre-configured rules in an EDR solution can recognize when incoming data indicates a known type of security breach and triggers an automatic response, such as to log off the end user or send an alert to a staff member

Credits: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html

SAMPLE EDR DETECTION



Detections

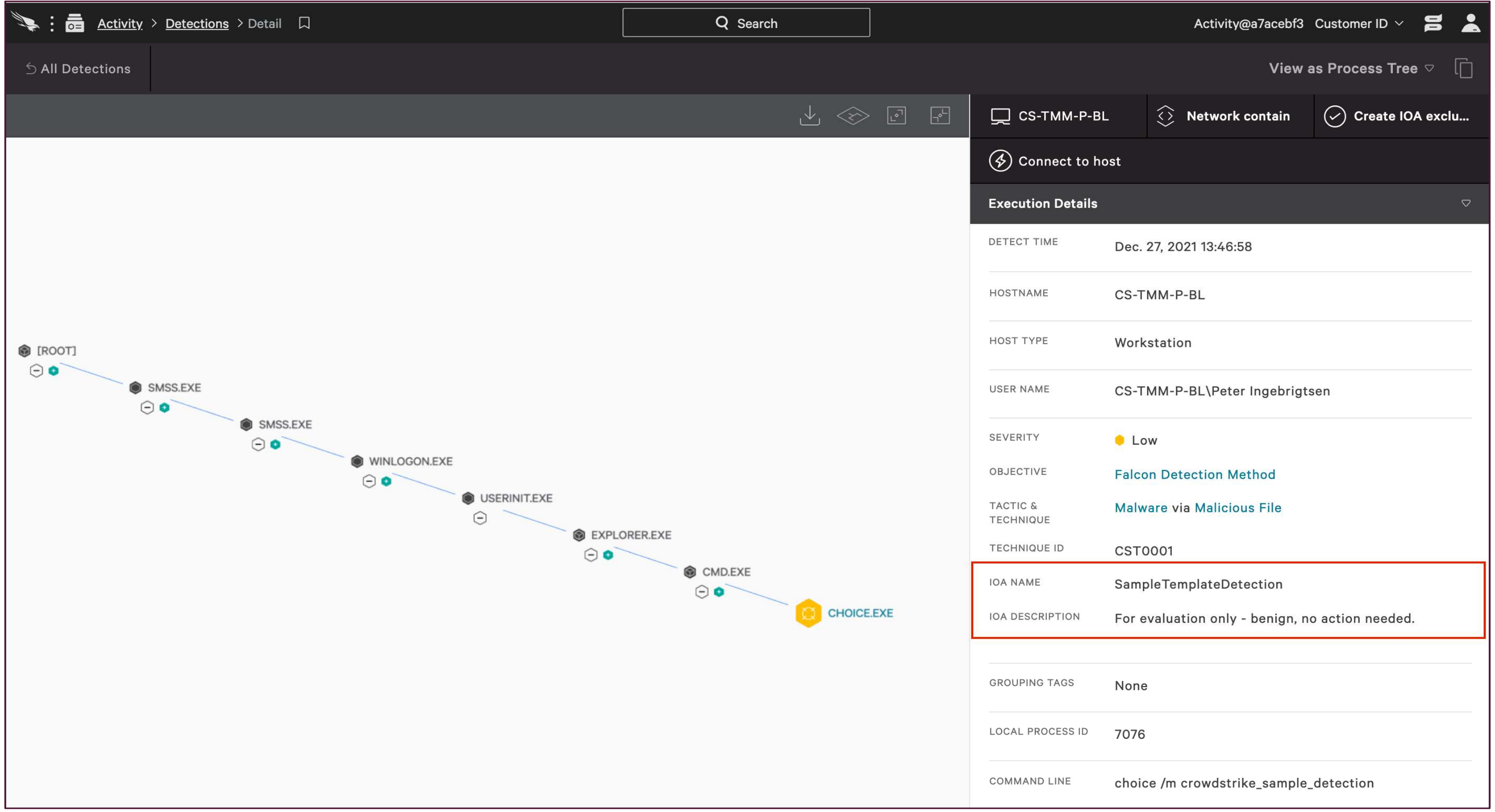
Status: New ✕ — 1 detection found ✕

Severity		Tactic		Technique		Time		Status		Triggering file		Assigned to	
Critical	0	Malware	1	Malicious File	1	Last hour	0	New	1	choice.exe	1	Unassigned	1
High	0					Last day	0	In Progress	1				
Medium	0					Last week	1	True Positive	9				
Low	1					Last 30 days	1	False Positive	0				
Informational	0					Last 90 days	1	Ignored	0				
								2 more					

	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
□ Low	Malware via Malicious File	Dec. 27, 2021 13:46:58	CS-TMM-P-BL	User	Unassigned	New

Credits: https://www.crowdstrike.com/blog/tech-center/generate-your-first-detection/

SAMPLE EDR DETECTION

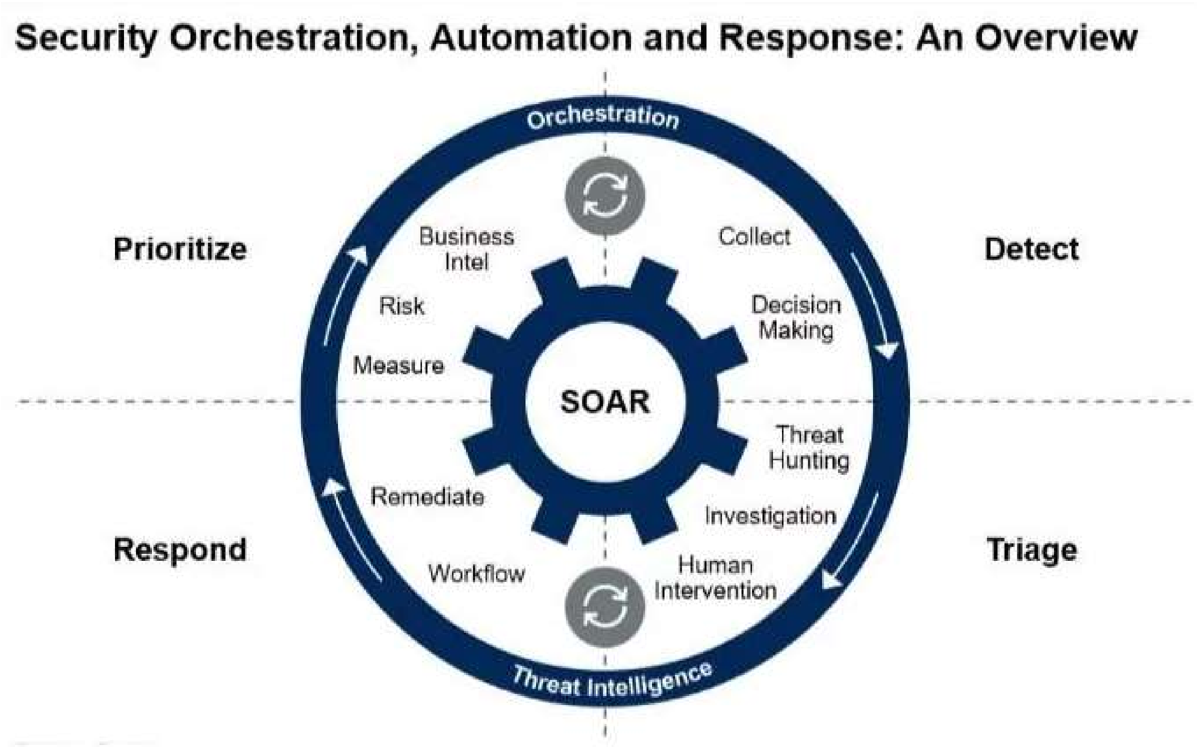


DETECT TIME	Dec. 27, 2021 13:46:58
HOSTNAME	CS-TMM-P-BL
HOST TYPE	Workstation
USER NAME	CS-TMM-P-BL\Peter Ingebrigtsen
SEVERITY	● Low
OBJECTIVE	Falcon Detection Method
TACTIC & TECHNIQUE	Malware via Malicious File
TECHNIQUE ID	CST0001
IOA NAME	SampleTemplateDetection
IOA DESCRIPTION	For evaluation only - benign, no action needed.
GROUPING TAGS	None
LOCAL PROCESS ID	7076
COMMAND LINE	choice /m crowdstrike_sample_detection

Credits: https://www.crowdstrike.com/blog/tech-center/generate-your-first-detection/

WHAT IS A SOAR

- SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team



Credits: https://www.ibm.com/security/digital-assets/soar/how-to-be-a-soar-winner/

THE ABC'S OF SOAR

- **Automation**
  - The ability to perform functions without human intervention. These functions may be internal
- **Orchestration**
  - The creation of a sequence of multiple steps and/or actions that drive a particular process or response
  - Orchestration typically involves human action as well as automated steps
- **Case/Incident**
  - This refers to the end-to-end process of investigation, containment and remediation
  - A case/incident may include multiple workflows, depending on how an attack evolves

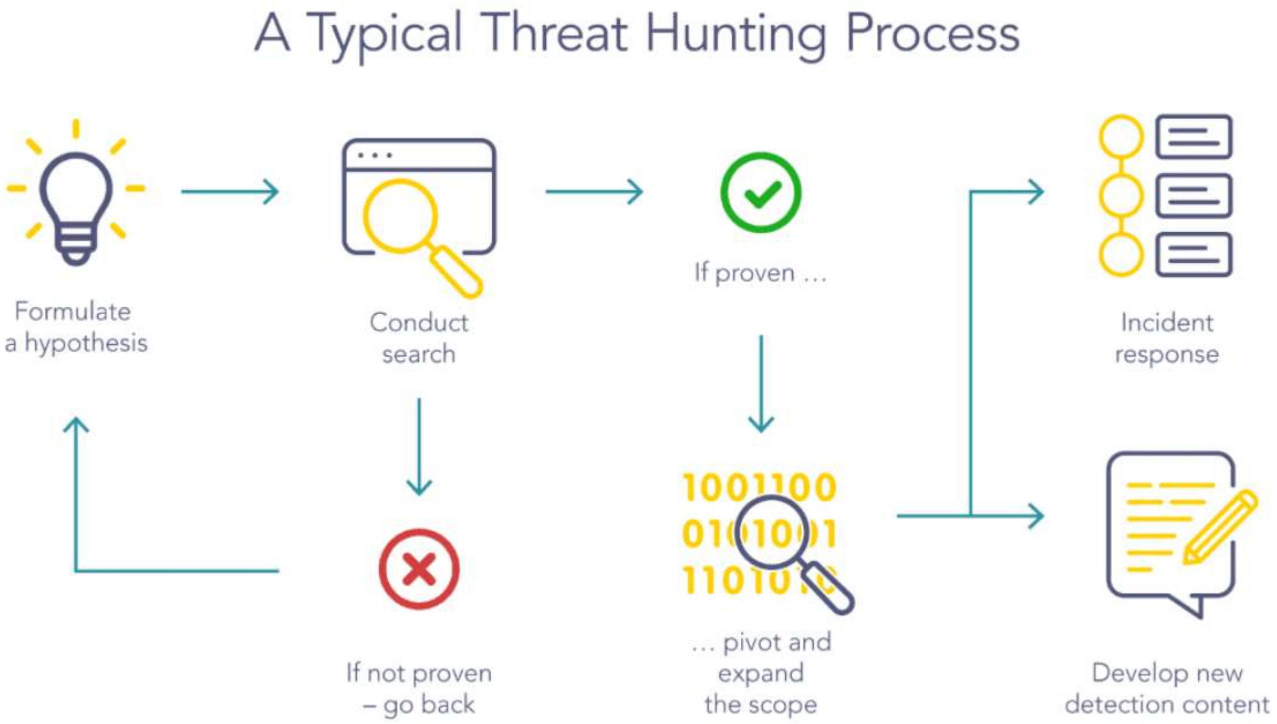
Credits: https://www.ibm.com/security/digital-assets/soar/how-to-be-a-soar-winner/

THE ABC'S OF SOAR

- **Playbook**
  - A set of tasks that may or may not include external automation, which is associated with a specific threat type such as phishing or network intrusion
  - A playbook determines the organizational response to a particular threat and should include business processes as well as technical tasks
  - Playbooks are additive, such that a complex incident may consist of multiple playbooks
- **Workflow**
  - A workflow describes a specific set of actions around a particular security process. A playbook is made up of multiple workflows
- **App/Integration**
  - An Application (App) or Integration is a packaged set of functions, rules, scripts and workflows that links the y SOAR API to third-party security
  - It can also be IT ops tools in order to leverage that external tools capabilities as part of the incident response process

Credits: https://www.ibm.com/security/digital-assets/soar/how-to-be-a-soar-winner/

CYBER THREAT HUNTING



THREAT HUNTING METHODOLOGIES

- In proactive threat hunting, the initiation of investigation typically falls into three main categories:
- **Hypothesis-driven investigation**
  - Hypothesis-driven investigations are often triggered by a new threat that's been identified through a large pool of crowdsourced attack data, giving insights into attackers' latest tactics, techniques, and procedures (TTP)
  - Once a new TTP has been identified, threat hunters will then look to discover if the attacker's specific behaviors are found in their own environment
- **Investigation based on known IOC and IOA**
  - This approach to threat hunting involves leveraging tactical threat intelligence to catalog known IOCs and IOAs associated with new threats
  - These then become triggers that threat hunters use to uncover potential hidden attacks or ongoing malicious activity
- **Advanced analytics and machine learning investigations**
  - The third approach combines powerful data analysis and machine learning to sift through a massive amount of information in order to detect irregularities that may suggest potential malicious activity
  - These anomalies become hunting leads that are investigated by skilled analysts to identify stealthy threats

Credits: https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

THANK YOU

HAVE A HAPPY WEEKEND