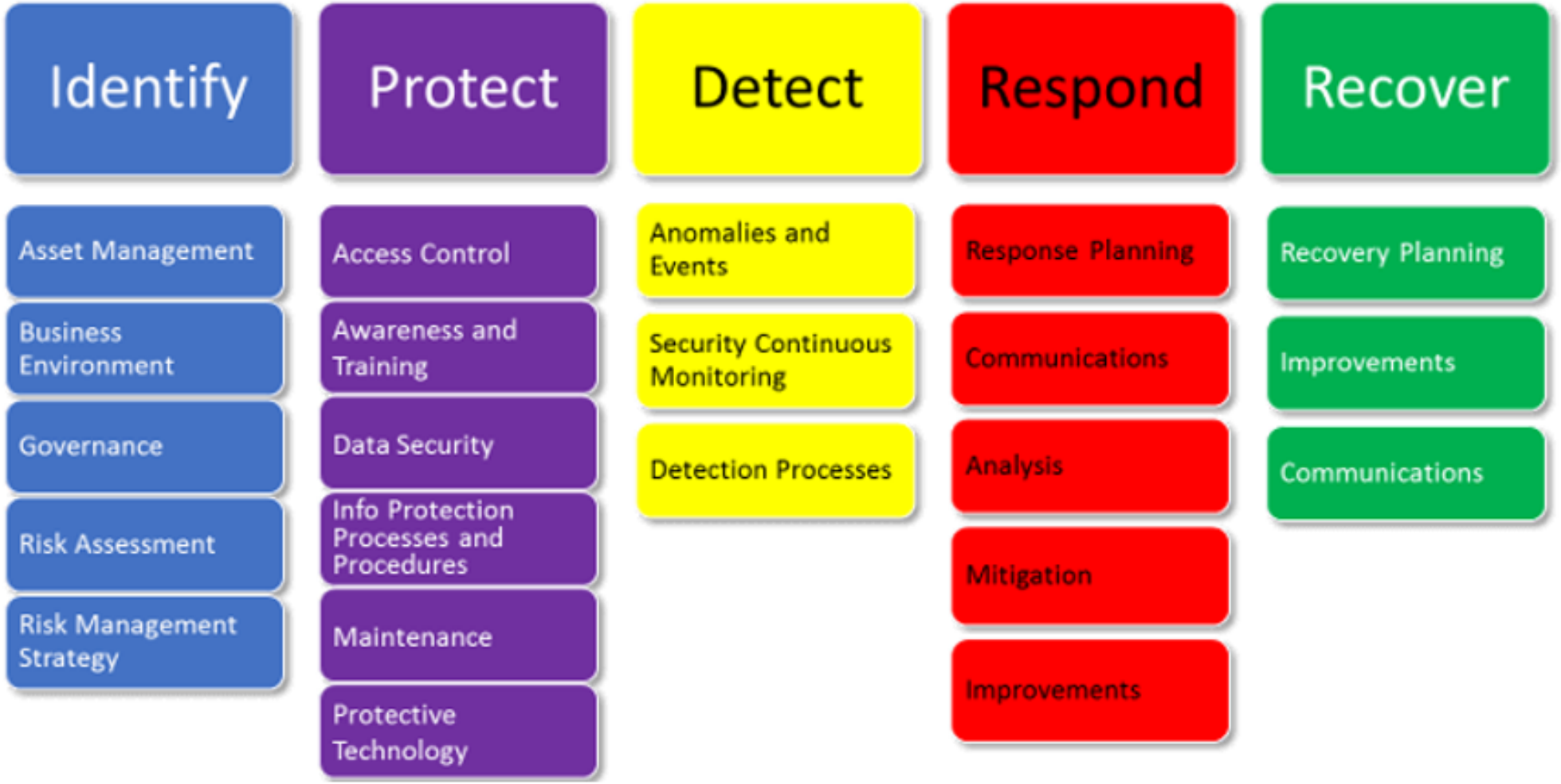
DAY 5

SOC INVESTIGATION PROCESS

- PRESENTED BY: ADITYA JAMKHANDE

NIST CYBER SECURITY FRAMEWORK



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

Submit

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

Job | Smart Mode

Format Timeline | – Zoom Out | + Zoom to Selection | × Deselect | 1 minute per column

1 — 12:00 PM Mon Dec 10 2018 — 1:00 PM — 2:00 PM — 3:00 PM — 1

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

SPLUNK REPORTS EXAMPLE

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Search & Reporting

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 | All | Yours | This App's | filter

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

THANK YOU

HAVE A HAPPY WEEKEND