Leveraging Breach Detection Systems within SOAR

HOW TO BECOME PROACTIVE BEFORE INCIDENTS HAPPEN

Agenda

- Intro
- SOAR
- BDS
- Scenarios

Intro

Intro

- Jeremy “Howie” Howerton
- Global Solutions Architect @ Trend Micro
- 17 years in security
- Specialized in BDS and IPS/IDS
- Recently introduced to SOAR

SOAR

What is SOAR?

- Security Orchestration and Automated Response
- Primary Goal: Reduce manual steps in response to security alerts
- Playbooks/Runbooks – Ready-made “scripts” to take action based on input/alerts
- Supports multiple technologies from multiple vendors

BDS

What is BDS?

- Breach Detection System
- Primary Goal: Discover stealthy malware threats that evade other detection technologies
- Virtual Analysis / Sandboxing
- Produce:
  - Alerts/Reports
  - IOCs
  - Signatures

Why SOAR + BDS

Why SOAR + BDS?

- Not limited to just BDS, of course
- Enrichment of Alert data
- Shorten dwell time
- Respond proactively
- Get better ROI from your security investments

Scenarios

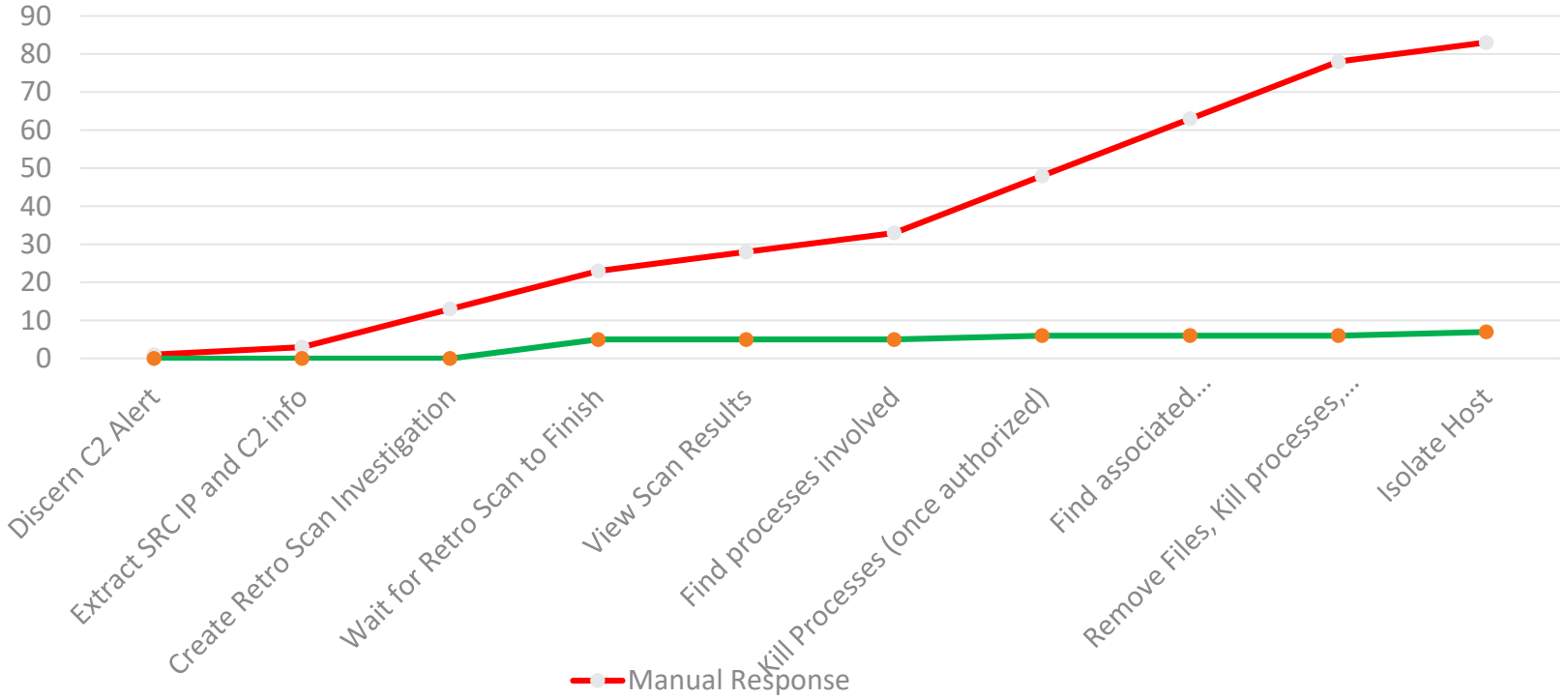
Scenario 1 - C2 “Seek and Destroy”

- Trigger: A C2 Alert is received from BDS
- Response: We want to identify the process behind the C2 communication on the source host involved in the event and take action

C2 “Seek and Destroy” - Manual Steps

Manual Steps	Approximate Time
Discern C2 Alert (from other types of alerts received from BDS)	If staffed 24x7x365… and assuming not busy with other tasks...1 minute
Extract the SRC IP and C2 IP/URL/Domain from the alert	2 minutes
Login to Endpoint Detection and Response Console and create a new Scan/Sweep	10 minutes
Wait for the investigation to finish	5– 15 minutes
View the results of the scan	5 minutes
Determine the process responsible for the communications	5 minutes
Determine if there's any reason why we shouldn't kill the process	5 minutes+ (depending on time needed for approval)
if not, kill the process on the host	5 – 15 minutes
Determine if there are any other related files/processes/registry keys that need to be killed/removed	5-15 minutes (for each object)
Determine if there's any reason why we shouldn't kill the processes or remove the files/registry keys	5 min for each object
if we can't kill processes and remove files/registry keys, can we isolate the host (via OSCE FW)?	5 minutes
Total Approximate Time (assuming green light approval):	Over an hour

Response Time – Manual vs Automation



Scenario 2 – 3rd Party Intel Sweep

- Trigger: File Hash intel received via 3rd party intel subscription
- We want to place the file hash into all BDS/EDR/etc products that can accept it in order to:
  - See if the malware is present on endpoints
  - Remove/Isolate the threat if discovered on an endpoint
  - Prevent further damage

Use Case: C2 “3rd Party Intel”

Manual Steps	Approximate Time
Monitor 3rd party notifications for Malicious SHA1	If staffed 24x7x365… and assuming not busy with other tasks...1 minute
Get info about SHA1 from BDS, EDR, others..	20 minutes
Create list of endpoints where malware matching the SHA1 is present	15 – 30 minutes
Block and remove the threat from each affected endpoint	Depends on breadth of infection. Estimated 10 minutes per infection.
Total Approximate Time (assuming green light approval):	over an hour. Possibly several hours with multiple infections.

Response Time – Manual vs Automation

Q & A

THANKS!!!