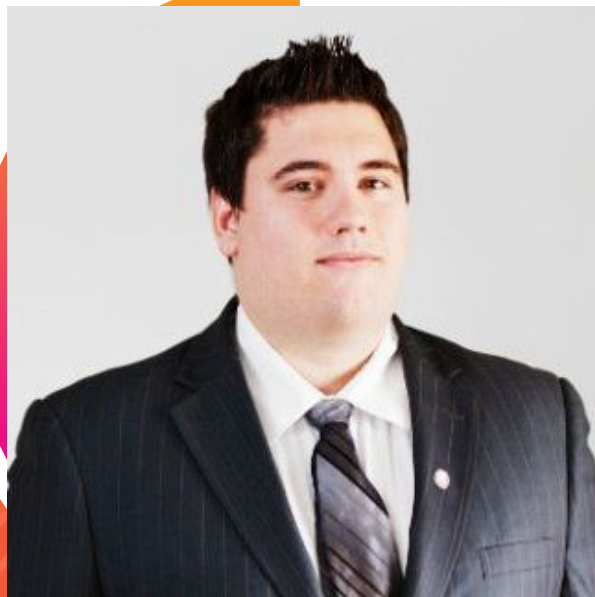


SEC1375 - Use Red Team Exercises to Build Alerts, Train Staff, and Drive Policies



Nate Piquette & Adam Parsons

October 22, 2019



Nate Piquette

Sr. Detection & Response Engineer
L3 Harris Technologies



Adam Parsons

Sr. Detection & Response Engineer
L3 Harris Technologies

npiquette@L3Harris:~# whoami

© 2019 SPLUNK INC.

Incident Response Engineer @ L3 Harris Technologies
Member of L3Harris' Threat Hunting, Deep Dive, and Architecture Teams

!~#history

Student > Intern > Hired! > SOC > Incident Response/Splunk Admin/Arch

!~#cat /etc/shadow

Credentials : GREM, Splunk Certified Arch. II, Lethal Forensicator

Hobbies : Family, Music, Video Games, Reading

Nathaniel.Piquette@L3Harris.com

aparsons@L3Harris:~# whoami

© 2019 SPLUNK INC.

Incident Response Engineer @ L3 Harris Technologies
Member of L3Harris' Threat hunting, Malware Analysis, and Red Teams

!~#history

Computer Operator > HelpDesk > Desktop > SysAdmin > Incident Response

!~#cat /etc/shadow

Credentials : GREM, OSCP, OSCE

Hobbies : Family, Hiking, Mountain Biking, Cyber Security

Adam.Parsons@L3Harris.com

Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Agenda

1. Intros
2. Quick Poll
3. Set the scene
4. Red team ready to strike
5. Evaluating our defeat
6. Come together, right now, as purple team
7. The All-In-One-Dashboard (AIOD)
8. Training day montage
9. No budget to red team, no problem
10. Lets wrap this up

Quick Poll

Who likes being hacked?

Who here learns a lot from post hack analysis?

The problem: How do we get that great post hack analysis step without actually being hacked?

Answer: Red Team!

Why Red Team?

Great way to test your current level of protection and alerts without having to alert the media

Takes out all the external hackers, replaces them with an internal team!

Know exactly what happened

Learn and adapt

Grow as a team!

We'll walk you through one such time we ran a red team exercise this past year!

Setting the Scene

Pre-merger

Week of December 17th, the perfect time to strike

Sysmon just rolling out

Whitelisting enabled

60+ alerts turned on

Monitoring at the lower level of the pyramid of pain primarily

Engagement Summary

L3 Harris Red Team's first engagement targeting L3 Harris infrastructure from the internet

Op Name: "Eat In"

Narrative: A server running a tomcat administrative panel with a weak password was exposed to the internet. An adversary bruteforced the password and compromised the Tomcat instance and thus the system running it.

Duration of prep: ~3 months from request to server build to service deployment to firewall rule push

Duration of engagement: ~26 hours

Team members involved:

Red Team: 4

Purple Team: 7

Human Proxies used: 1

Objectives

Test IT and Security processes for gaps and weaknesses

- Network and firewall modifications
- Request standard server build
- Create publicly available website
- SOC / IRT Escalation Plan

Test and Improve Detection and Response Capabilities

- Identify weakness in tools
 - SIEM, Threat Intel, App Whitelisting, Anti-Virus(A/V), Web Application Firewall(WAF), Intrusion Protection System(IPS), Endpoint Detection & Response(EDR)
 - Identify new alerting opportunities and/or gaps
 - SIEM, EDR, Sysmon



Preparation

Established Narrative

Tested vulnerabilities for exercise

Identified Human Proxy

Human proxy:

- Submitted requests for server build
- Submitted firewall requests

Configured Webserver

Check firewall is configured as requested

Wiped SIEM of logs that tied L3 Harris Red Team to attack infrastructure

Configured Kali VM in Azure Commercial

And so it begins...



Exercise ran

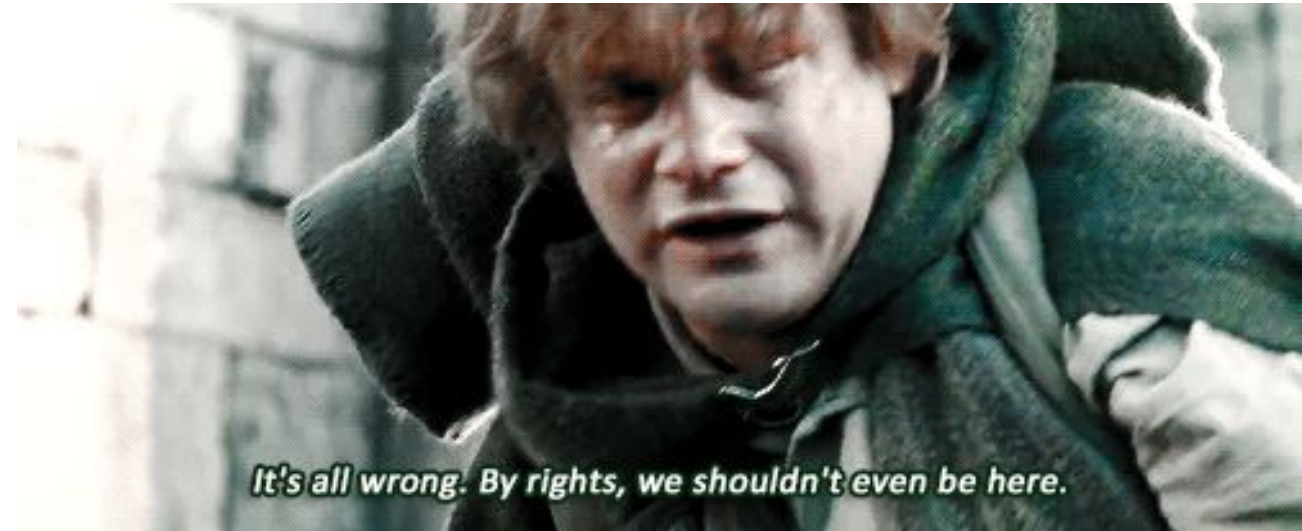
Recon performed via Burp Suite, Nikto, and Nmap

Compromised via “bruteforcing” Tomcat admin portal account – IRL a complex password was used

Uploaded Tomcat Web shell

Enumerated host

Gained interactive access by changing RDP port to an open/unused port on host



Banging pots and pans



Meanwhile in the SOC...



Detection & Response

SOC and IRT response

11:45AM: SOC analyst identified alert and notified SOC Manager of the activity

- Alert came in from EDR solution to ES Notable Event

12:09PM: SOC Manager notified IRT Manager of activity requesting IRT analyst to review.

12:58PM: SOC Manager recommended to IRT Manager that the Incident Response Plan be implemented.

1:00PM: TMT notified that this was a Red Team exercise

2:00PM: IRT and SOC provided debrief of engagement



Detection and Response

Due to the logs we collect from servers all of our analysis was able to be conducted in Splunk

Event ID 4688 in the Security Logs helped identify malicious use of PowerShell being executed

- Used a local copy of Cyberchef to decode the base64 command string and pivot from indicators found there

Began to pivot to network indicators found

Identified system was running TomCat and found web shell

Evaluating our Defeat

Our time to detect was outside what was expected

Had to “bang pots and pans” to get detected

Found out log forwarding agent misconfigured

Operational processes not followed causing increased security risk

SIEM alerts not properly working after log source format changes

Server admin uninstalled EDR unaware it was containing the server

ES instance was healthy



Red Team Mistakes

Triggered A/V twice

Triggered App Whitelisting multiple times

Left “Attacker” hostname as “kali”



Purple Team

Assigned members from SOC and IRT to work Purple Team looking for alert opportunities and SOP shortcomings

Installed Sysmon with a verbose config on server

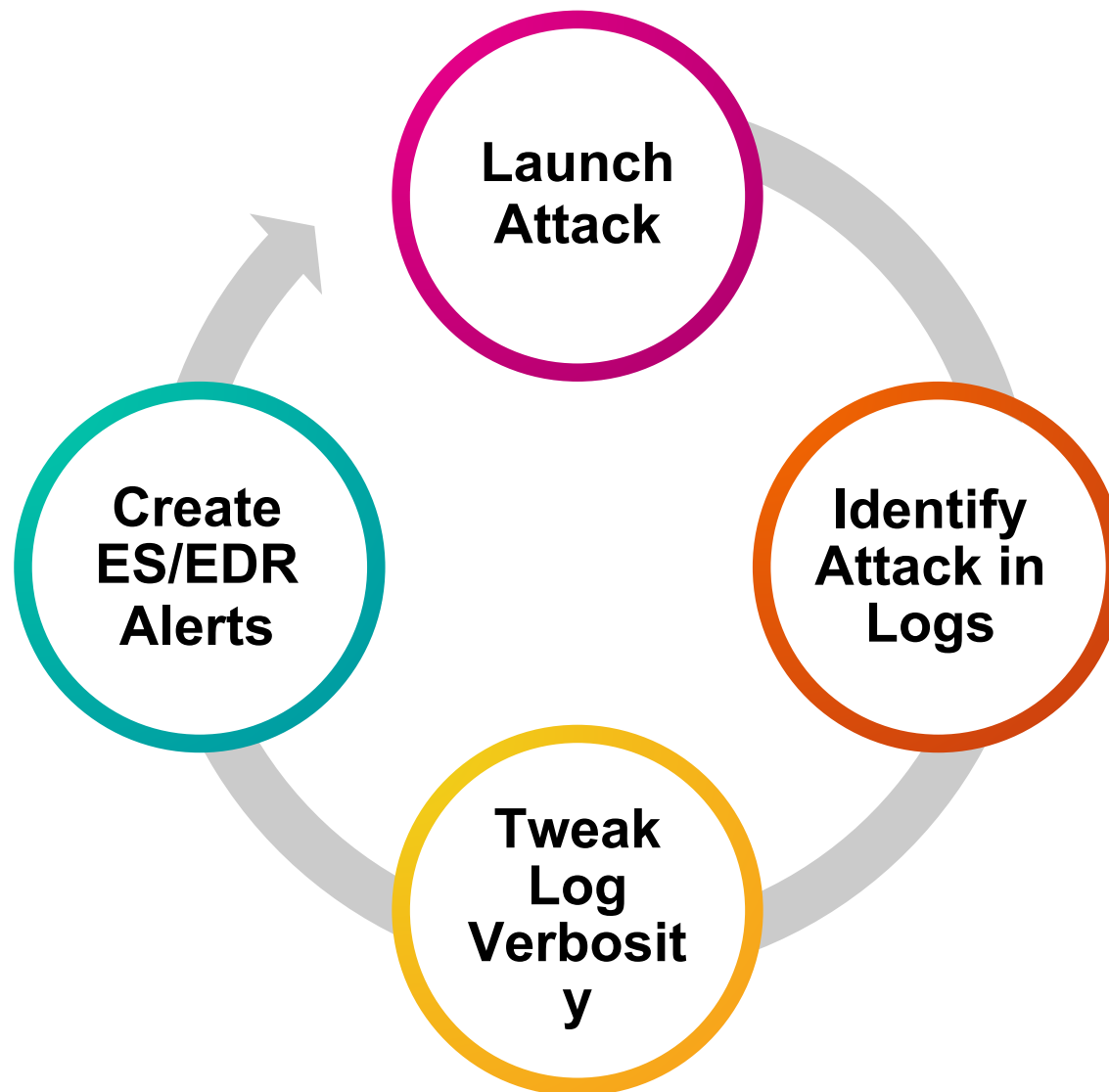
Fixed Log forwarding agent

Re-ran exercise sharing and recording screen of “attacker”

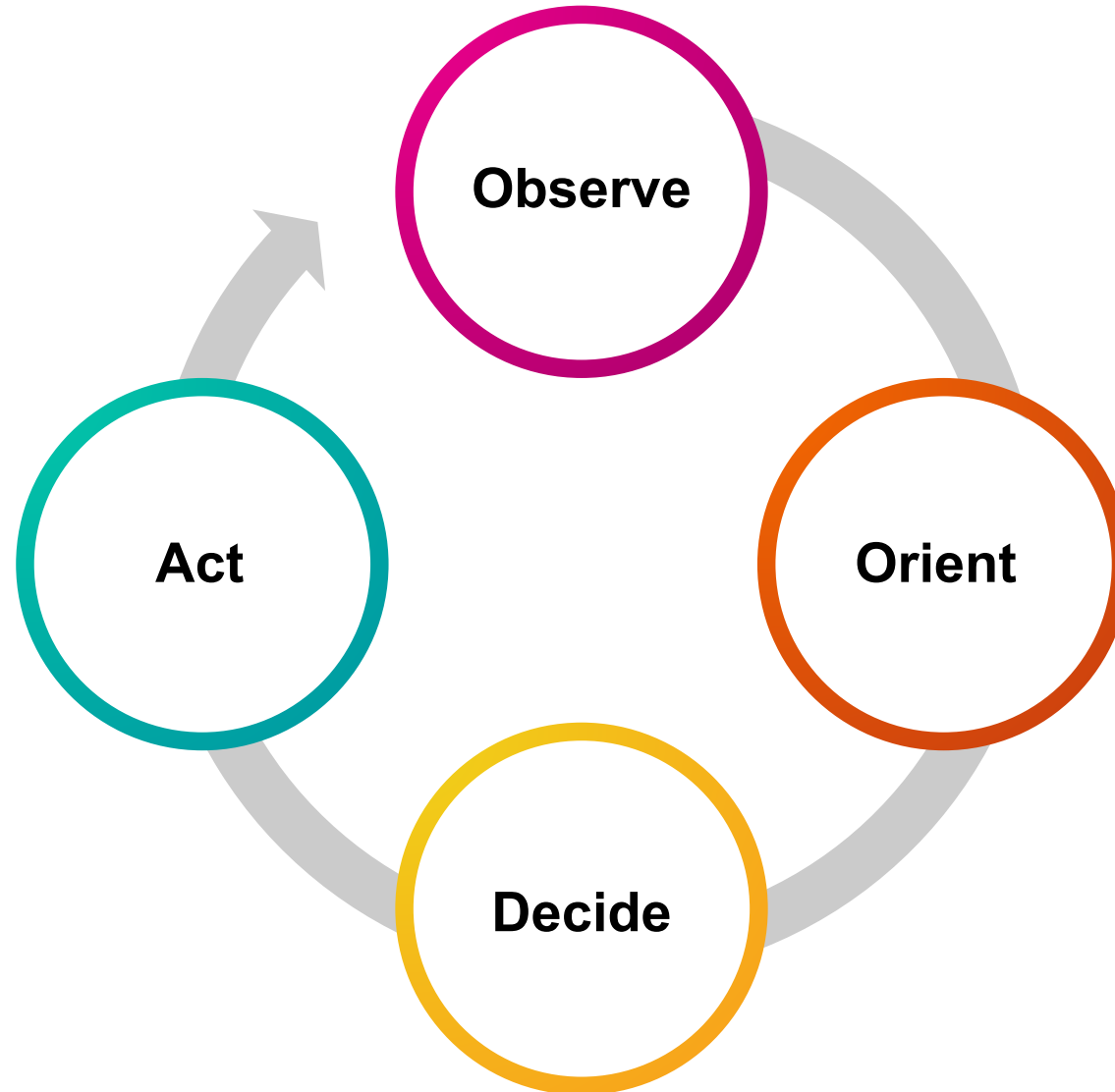
Notified Server team this time

Goal: Work with the red team to run through the operation again, this time monitoring each step of the journey to identify places of improvement.

Come together, right now, as purple team



Come together, right now, as purple team



Come together, right now, as purple team

Example workflow:

- Begin recording of “attacker’s activity” using Skype for Business
- “Attacker” performs same actions performed during initial attack
- Purple team members identify alert opportunities from logs
- Tweaking of Sysmon config to include new detections
- Creation of new ES and EDR alerts
- Attack re-run a final time to ensure alerts fire as intended



RESULTS

- 60 SIEM alerts created
- 18 Lookup tables created
- 6 Operational process changes implemented
- 10 EDR rules created
- 8 Sysmon config changes made
- 70 SOPs written
- 3 App Whitelisting bypasses identified
- 2 IR process improvements
- 2 Playbooks written
- 1 SIEM dashboard created
- 1 team notified that they shouldn't uninstall EDR from a host



Two Questions Still Existed:

How can we make the data pop during an investigation?

How can we increase consistency of investigative steps?

An AIOD to find them, an AIOD to guide them

AIOD = All-In-One Dashboard

A dashboard to help our analysts find suspicious activity quickly for any alert they are investigating

- Filter bad up to the top, and leave generic at the lower levels

Shout out to John Stoner!

Crafted with our organization in mind, but the ideas can be used for your organization to implement this too

The screenshot shows the 'AIOD - All In One Dashboard' interface. At the top, it says 'Enter the following items in order to investigate - Username, Hostname, Host IP'. Below this are four input fields: 'Username', 'Hostname', 'Host IP', and 'Time'. The 'Time' field is a dropdown menu currently set to 'Last 4 hours'. To the right of these fields are a green 'Submit' button and a 'Hide Filters' link. Below the input fields is a horizontal tab bar with six tabs: 'Details' (which is selected and underlined), 'Security Vendor Logs', 'AV/IDS/WAF Logs', 'Network Logs', 'Host Logs', and 'Email Logs'.

Standardizes searches performed by analysts during investigations

Emphasizes suspicious events by cross-referencing with lookup tables and summing total number of hits

Tab order flows from items that provide most confidence of malicious activity on the left to generic hunting on the right

Each tab follows the same flow too:

- Highly suspicious/High fidelity indicator at the top, generic logs or flat logs towards the bottom

Network Logs tab though contains some secret sauce that we are ready to share with you here!

Suspicious Indicator Lookup Tables

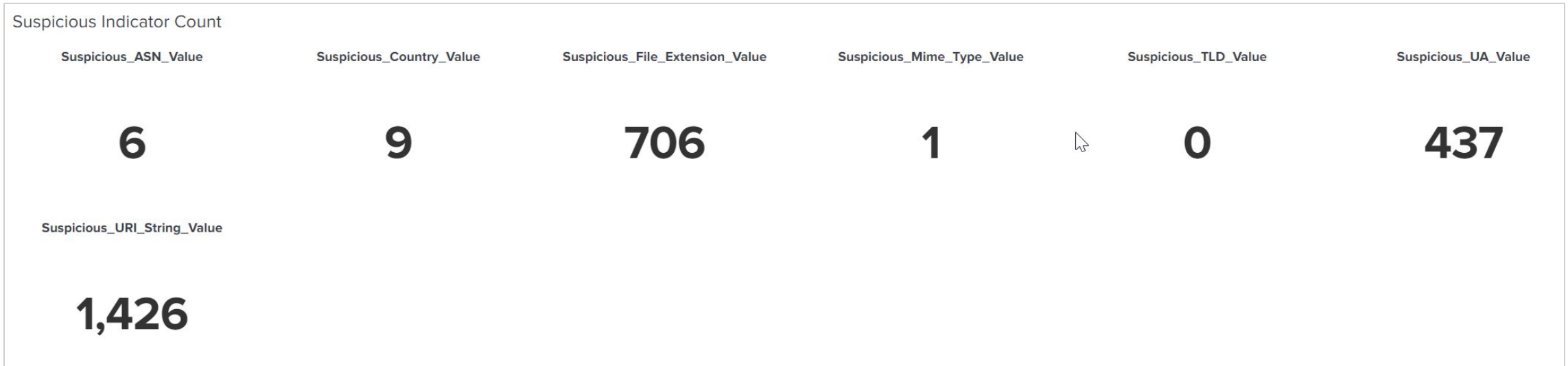
Created lookup tables based around the following:

- Suspicious User Agent
- Suspicious Strings in URI
- Suspicious Countries
- Suspicious Proxy Categories
- Dynamic DNS Domains
- Suspicious ASNs
- Suspicious Mime Types
- Suspicious TLDs
- Suspicious File Extensions
- Suspicious Child Processes

Data is based off OSINT and Industry related threat intelligence

Try to keep data high-fidelity; not always possible

Visualize Suspicious Indicator Lookup



Above data created using very generic data to inflate counts.

Top of network data tab contains count of all suspicious indicators found for current search criteria

Goal: Show analyst suspicious indicators they should expect to find, and emphasize when something stands out

Alerts, policies, and challenges oh my!

60 SIEM alerts created

- Alert testing lifecycle

70 SOPs written

- Alert SOPs containing Summary, Description, Tips and Tricks, Investigative searches, the original search, previous iterations of search and change tracking...in OneNote currently

Working on monitoring at alerting in upper tiers of pyramid of pain

What policy changes were made

- Firewall Provisioning
- Server Deployment
- WAF integration

Challenges we still face

Don't Get Lost in the Data Lake

Key discovery was that the attackers were in our whitelisting solution's logs

These logs were being ingested by Splunk, but not actively being alerted on or looked at!

- This is a bad practice, and should not have happened!

Developed an onboarding procedure for new log sources in which we identify use cases for the data and develop ES alerts for them

The key thing here is to make sure all data has a use and is being looked at

- Leave no stone unturned!

Training day montage

AIOD training

Capturing data for Internal BOTS (Boss of the SOC)

Attempt to teach the analytical mindset:

- Asking questions and challenging the norm is good!
- If you see something say something!
- If the gut says its weird, it probably is

Splunk Admins don't hate us but, start broad in your search and then narrow in on interesting sourcetypes that don't have many events!

- Sometimes when you hunt you need to cast a broad net, but make sure not to impact the usability of Splunk for others

What if I don't have the resources to red team?

Still find a way to test alerts

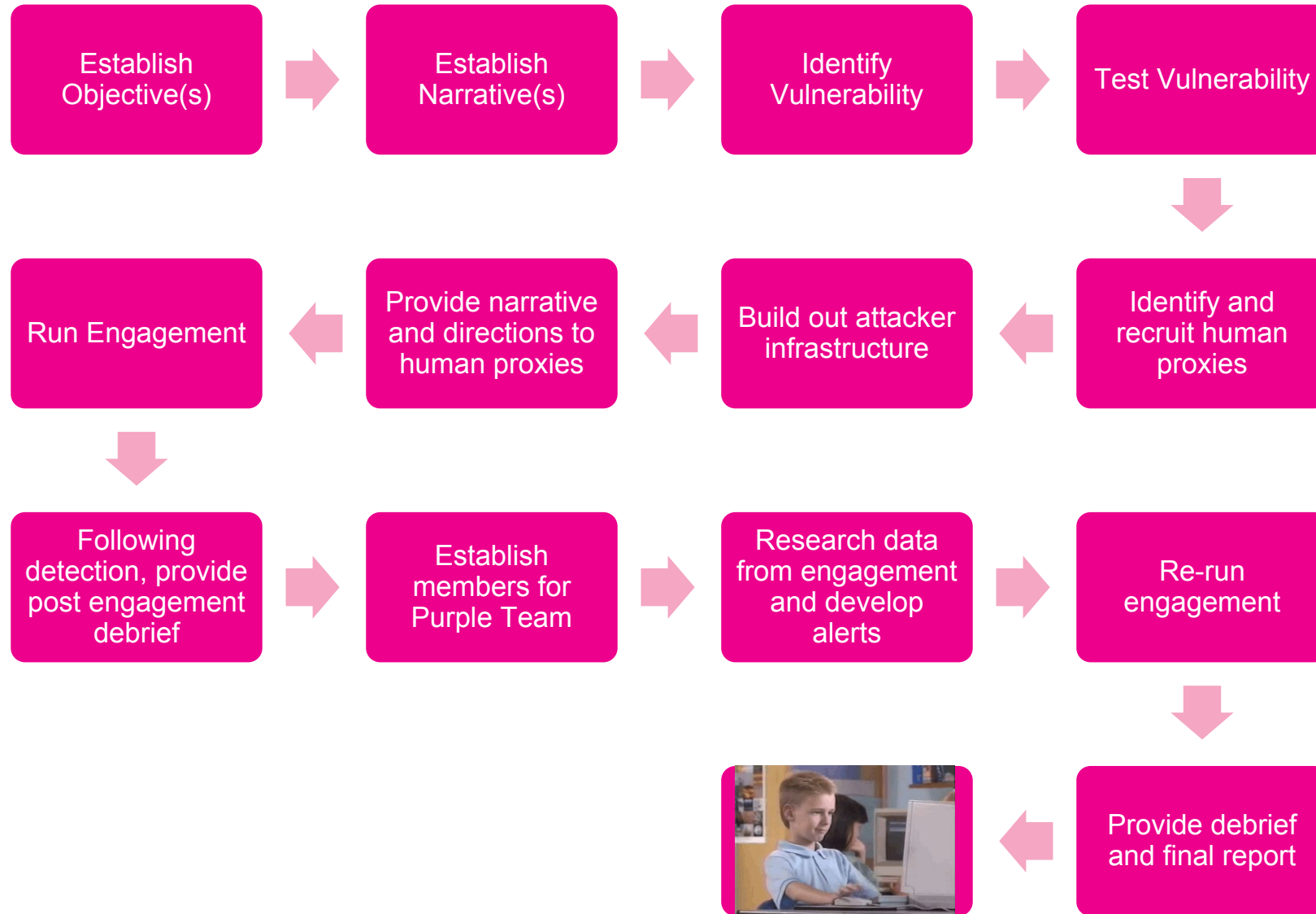
Take time each quarter to audit policies and SOPs

Run table top exercises!

- Great way to run through your policies, SOPs, and incident response plan
- Work's your defender's brains and allows you to see what steps they would take!
 - Bonus points if you have a geographically dispersed team, don't allow them to join the table top until an analysts says they would alert those who are remote or vise versa!

Red Team Engagement Workflow

© 2019 SPLUNK INC.



OpSec!

Do not use company infrastructure to access attacker infrastructure

- TOR
- Proxy
- Home internet

Practice deleting logs from your SIEM if possible

Ensure that none of your emails, in particular message subjects, contain IoCs that could be found by others not in the know happening upon it

Pad the beginning and end of malicious files where possible

Change filenames of malicious files to something that goes along with the narrative where possible i.e. web shell changed from cmd.jsp to HrsBuild.jsp

Modify hashes of publicly obtained malicious files

Use a local firewall to isolate access to it to a malicious service if this cannot be done in advance by your infrastructure firewall

Change hostname of attacker machine if it is something obvious i.e. "kali"

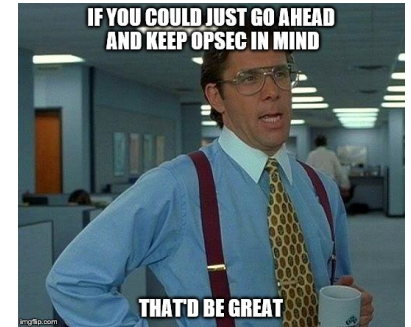
Only allow what needs access to attacker infrastructure where possible in order to prevent services like Shodan or web proxies that visit new URLs from unintentionally revealing information.

Make sure to fill out any forms necessary to perform pentesting in a CSP to reduce chances of them messing with infrastructure

"Live off the land" as much as possible

Drop as few files as possible; stay in memory as much as possible

Consider uploading malicious files to VT/PT/Any.Run to determine if it would be detected by A/V. The hash can be changed so the version used in an attack is not easily found on VT. It could be found via YARA rule(s) after all.



Example Objectives

Test tools

- A/V
- EDR
- Application Whitelisting
- Firewall
- IPS
- IDS
- WAF
- SIEM
- Alerts

Test processes

- Operations

Server requests

Software installed

Permissions granted

Firewall rules applied vs what was requested

Example Narratives

Vulnerability scanning

Attempted exploitation i.e. SQLmap or WPscan

Phish

- Credential harvester
- Malicious attachment

Link to malicious file

Internet-facing service with vulnerability

Lateral movement

Password spraying i.e. ADFS or Skype

Bruteforcing passwords i.e. ADFS or Skype

Process auditing: Identify weaknesses or gaps in the processes that could cause security issues i.e. default firewall ports being opened despite not being requested

Mailbox compromise

Messenger compromise i.e. Skype or Slack

Data exfiltration

Social engineering i.e. via Skype or Phone

- Password reset request to helpdesk
- Payroll change request to HR rep
- Sending a colleague a malicious file via compromised Skype account

Let's Wrap This Up

Should you red team?

- Absolutely yes! Value > time to put together

It's ok to fail a red team assessment

- Use it to learn
 - OODA!

Find a way to capture what you want your analysts to quickly identify as malicious/suspicious

- Lookup tables can help here!

Validate security policies

Train your defenders



Q&A



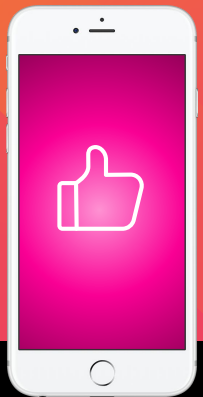
Thank

You



Go to the .conf19 mobile app to

RATE THIS SESSION





Bonus Slides!

Resources to help you on your red teaming journey

Name	Summary
MITRE CALDERA	an automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks.
Uber Metta	Developed by uber; uses Redis/Celery, python, and vagrant with virtualbox to do adversarial simulation.
APT Simulator	a Windows Batch script that uses a set of tools and output files to make a system look as if it was compromised.
Red Team Automation(RTA)	provides a framework of scripts designed to allow blue teams to test their detection capabilities against malicious tradecraft, modeled after MITRE ATT&CK .
Atomic Red Team	a library of simple tests that every security team can execute to test their controls.
LOLBAS	documents every binary, script, and library that can be used for Living Off The Land techniques.
MITRE ATT&CK Matrix	a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
Infection Monkey	an open source security tool for testing a data center's resiliency to perimeter breaches and internal server infection.
Invoke-Adversary	a PowerShell script that helps you to evaluate security products and monitoring solutions based on how well they detect advanced persistent threats.

Tools used during at

Name	Description	Detected by
Inveigh	PowerShell ADIDNS/LLMNR/mDNS/NBNS spoofer and man-in-the-middle tool	A/V Detected as PS/Inveigh
JSP Web shell by Security Risk Advisors	A web shell written in JSP for Tomcat. Requires JS to be run on attacking machine to interact with web shell	Nothing
Meterpreter SSL Reverse Shell in C#	Reverse shell that uses SSL. Also used fake L3 Harris cert.	Nothing
Mimikatz via C#	Dumps credentials in memory	Nothing
MSBuildShell via C#	PowerShell re-written in C#	Nothing
PSAttack	PowerShell Red Team tools including mimikatz, mimikittenz, and Inveigh using NOPS method with encryption	A/V Detected as GenericRXEC-BL!5755FC8F21E1

