Lessons Learned

Introduction

We have to reconcile with the idea that we won't really know for certain if we've fully eradicated an adversary from our environment. For really advanced adversaries, the reality is that it's a game of cat and mouse, and that our only comfort is our confidence that our process from Preparation to Identification and Scoping to Containment and Threat Intel Creation to Eradication and Recovery has been done diligently.

The findings that we have will serve as input to further improve this process, and hopefully, we'd easily detect them in near real-time if ever they come back in our environment and they show the same IOAs and IOCs.

Learning Objectives:
In this room, we will be wrapping up the lessons that we, as incident responders, have learned from all the prior parts of the Incident Response process which were discussed in the previous rooms of this module.

Specific emphasis is given on how these lessons can be consumed by the organization through the creation of technical and executive summaries. The room also touches upon how all of these immediately and directly impact the organization's continuous monitoring capability through the threat intelligence created over the course of the IR process.

Room Prerequisites:

- Preparation | Live IR Module
- Identification and Scoping | Live IR Module
- Containment and Threat Intelligence Creation | Live IR Module
- Eradication, Remediation, Recovery | Live IR Module

Brewing It All Together

This phase of the IR process is essentially a sit-down with the data that you've gathered throughout the IR process and the learnings gained from them. This isn't the most exciting part of the process in terms of getting your hands dirty and fighting in the field, and as such, may easily be neglected or skipped entirely. However, a lot of potential is lost whenever this is the case.

Wisdom is gained whenever you actively strive to learn from the experience, but it will remain just an experience and you will remain unlearned when the active effort of piecing it together is not there. Evaluated experience is key: this principle is transferable in most aspects of life, and it's the same in incident response.

Below is a recap of all the things that we've learned throughout the IR journey that we have so far.

Preparation
In this room, the emphasis is placed on the importance of establishing a response capability to ensure that the organization is able to respond to incidents. The room specifically focused on the importance of preparing the people, important documentation, and ample technological capabilities to maintain a level of readiness when an incident calls for it.

People touched upon the creation of a CSIRT team to ensure that the right people with their specific expertise are ready to go when an incident arises. Documentations touched upon the creation of policies and procedures that would make it easier for the response team to do their work seamlessly, while at the same time creating the opportunity to keep these details for later use, for litigation purposes or for the improvement of the organization's security posture.

Technological capabilities touched upon the pieces of technology that would help make it easier for the team, focusing on having an inventory of assets, baseline security tools, and of course, having enough visibility.

Overall, being prepared means ensuring that people are ready, visibility is ample, and systems, networks, and applications are sufficiently secure.

Identification and Scoping
In this room, the emphasis is placed on the importance of the feedback loop between identification and scoping, wherein it is specifically stated that it is not a linear progression, rather it is a cyclic process that aims to continually refine the incident responder's understanding of the incident and its scope.

The importance of the process being intelligence-driven is also stressed. Information must be taken advantage of, otherwise responders will essentially go about their work blindly. Overall, being in this phase of incident response means being on top of the ever-evolving incident environment, while being steered by threat intelligence.

Containment and Threat Intel Creation
In this room, the emphasis is placed on the importance of threat intelligence in the cyclic process of identification, scoping, and containment. Just like the previous room, it acknowledges that an incident is constantly evolving and with that comes the assumed responsibility of always keeping informed and playing the game one step ahead of the threat actor by leveraging intelligence.

Containment strategies are discussed as well, which allows us to act while limiting the damage that the threat actor may cause to a minimum.

Eradication, Remediation, and Recovery
In this room, the emphasis is placed on the fact that remediation is part of an ongoing IR process, and its success is reliant on the effectivity and synergy of all of the previous phases of the process.

While the containment phase limits the damage of the threat actor, in this phase, we act to plan for and actually remove the threat actor from the environment. Post-removal actions were also touched upon in the remediation and recovery parts of the room.

****

Answer the questions below:

What phase of the IR process focuses on people, documentations, and technological capabilities?
Answer: Preparation

What phase of the IR process is reliant on the effectivity and synergy of all the other phases?
Answer: Eradication, Remediation, and Recovery

The SwiftSpend Incident Recap

Since we ought to sit down with the data that we've gathered throughout the IR process, below is a recap of all of the things about the SwiftSpend compromise that we found out over the course of our IR journey. Listing them out this way would not only make it easier to remember, but also would help us build our Executive and Technical summaries that are to be discussed later on in this room.

Identification and Scoping

We saw how the compromise at SwiftSpend Financial (SSF) started and listed below is a summary of how it developed.

- Outdated endpoint protection definitions of the device owned by Derrick Marshall, which is none other than the Head of IT - Operations and Support
- Phishing incident involving Michael Ascot; credentials have been compromised but the SOC quickly advised the user to update his credentials
- It's later found out that it was a phishing campaign targeting both Michael Ascot and Alexander Swift, however the latter did not open a ticket nor report the issue
- Multiple phishing domains regarding the above incident were further discovered and added to the SoD
- In light of the incident, it's been found out that it all stems from an unpatched vulnerability in the form of missing email security (i.e., SPF, DMARC, and DKIM) that has already been previously identified for a while now, but for some reason is still yet to be remediated
- An updated SoD has been crafted, and is attached in the VM

Containment and Threat Intel Creation

We developed unique pieces of threat intelligence from a packet capture. Listed below is a summary of our threat intel creation.

- Discovery of a malicious IP that serves as the threat actor's host for additional malicious downloadables
- Another malicious IP (3.250.7.149) has been noted which is linked to the tal0nix threat actor; further details link this threat actor to phishing reports involving an O365 page that presents the need to login via email and password
- 2 different versions of a malicious Dropper was discovered as well

Eradication, Remediation, and Recovery

We discussed the SSF compromise in further detail, particularly the effect of the swiftspend_admin credential leakage that led to the Jenkins server compromise and the discovery of the threat actor script leading to the implementation of their actions on objectives.

- swiftspend_admin credential leakage and threat actor discovery of password reuse that led to the compromise of the Jenkins server
- Jenkins platform compromise: discovery of a scheduled exfiltration script (backup.sh) disguised as a backup implementation for the server
- Compromised Jenkins service account used as a backdoor

- Hijacked swiftspend domain (backup.swiftspend.com) via manual addition of the threat actor's IP (194.26.135.132) that receives the exfiltrated files to the server's hosts file

****

Answer the questions below:

What malicious file type has been found with two different versions?
Answer: Dropper

What's the name of the malicious file found in the Jenkins server?
Answer: backup.sh

The Executive and Technical Summaries

Before everything else, start the virtual machine by clicking the green Start Machine button on the upper-right section of this task. If the VM is not visible, use the blue Show Split View button at the top-right of the page.

Technical Summary
A technical summary is a summary of the relevant findings about the incident from detection to recovery. The goal of this document is to provide a concise description of the technical aspects of the incident, but it can also function as a quick reference guide.

At the end of the day, it's supposed to collate the most important findings of the investigation while at the same time still being able to paint the complete picture, so a challenge that may arise is choosing which details to include and which ones to leave out. Remember that it is meant to be read by a technical audience, so it is advised to keep a balance of technical writing and conciseness in creating this summary.

The details from this summary are meant to be actioned upon, consequently ensuring that this type of compromise, from foothold to exploited vulnerabilities to lack of visibility, will all be covered so as to prevent it from happening again in the future.

Executive Summary
At the end of the day, the Incident Response team will answer to the client, and in SwiftSpend's case, the 'client' is essentially itself. The specific stakeholders involved would want to make sure that all of the findings are accounted for with the intention of

being actioned upon, so having an executive summary is a way for them to keep a formal documentation of what happened.

Depending on the severity of the compromise, sometimes the C-Suite may want to know more about how it affected the business in the macro sense as well. However, since it's a summary, it's recommended to stick to the relevant items that they would want to know about.

A concise summary would contain, but may not be limited to the following:

- A summary of the impact of the compromise
    - Did we lose money?
    - Did they steal it?
    - Did we lose it due to downtime of sensitive servers / endpoints?

- Did we lose data?
    - PIIs?
    - Proprietary pieces of information that are top secret?

    - Was it a high-profile case, and if so, what kind of reputational damage are we looking at here?

- A summary of the events and / or circumstances that led to / caused the compromise
    - How did this happen?

- A summary of the actions already done, and actions planned in the near, mid, and long term to remediate and recover from it, and to prevent it from happening again in the future

****

Answer the questions below:

In the draft, it seems that the analyst included a number of technical details that are not necessarily needed in the Executive Summary. The first paragraph alone has two details that can be removed to look something like this:

On the 13th of July, 2023, Michael Ascot received an email with a URL that leads to a seemingly innocuous O365 page that requires the user to "re-authenticate". Upon supplying his credentials, the page didn't show anything; the user

immediately became suspicious and upon asking for clarifications via email, he received an Outlook error prompting the user to report the incident to SOC.

What are the two technical details removed in the revised paragraph? (Separate them with a comma and a space; format: technical detail 1, technical detail 2)

Executive Summary

On the 13th of July, 2023, Michael Ascot received an email from alex.swift@swiftspend[.]finance with a URL that leads to a seemingly innocuous O365 page that requires the user to "re-authenticate". Upon supplying his credentials, the page didn't show anything and so Michael immediately became suspicious and sent a reply to the email asking for clarifications for which he received the outlook error that lead to the user raising Ticket#2023012398704232 to SOC.

Answer: alex.swift@swiftspend[.]finance, Ticket#2023012398704232

Depending on the audience, you can put as much or as little detail as you want in the Executive Summary but remember that it is imperative to stick to the essentials. For example, the second and third paragraphs can be condensed more while still retaining its essence.

What technical detail in the fifth paragraph of the draft can be removed? (The answer is the entire string that you will be removing to make the paragraph more concise.)

It is also confirmed that email controls weren't able to detect the initial phishing campaign because of a previously identified unpatched vulnerability in the form of missing email security (i.e., SPF, DKIM, DMARC) that is yet to be remediated.

Answer: (i.e., SPF, DKIM, DMARC)

A Technical Summary must be concise while remaining effective in tracking the important artefacts, among other things.

In the draft, the third paragraph talks about the discovery of numerous artefacts via the review of a packet capture. What are those artefacts? (Separate them with a comma and a space; format: technical detail 1, technical detail 2)

IP Address	3[.]250[.]38[.]141	Malware hosting	Packet Capture
IP Address	3[.]250[.]7[.]149	Phishing IP	Pivoting from Ticket
File (Executable)	Dropper.exe	Malware	Packet Capture

Looking at the Spreadsheet of Doom(SoD) and looking for artifacts that were found in the packet capture we see the IP address that hosted the malware and the name of the malware.
Answer: 3[.]250[.]38[.]141, Dropper.exe

The fourth paragraph talked about a swiftspend domain being hijacked to host the threat actor's exfiltration IP. How did the investigators find out about this? (The answer is the entire string as described in the SoD)

File (Script)	backup.sh	Exfiltration script	Pivoting from Jenkin

Answer: Pivoting from backup.sh

Unique Threat Intelligence

The SoD that we've created is a prime resource for threat intelligence unique to SSF. Remember that these are traces of a specific adversary that your environment has already faced and so, the inclusion of these indicators as part of your organization's continuous monitoring and detection mechanism will immediately spot re-intrusion of that specific adversary.

This step is proof of how the phases of the IR process are cyclic. In integrating these indicators to the SOC's detection mechanism, we go full circle. You can even go one step further and try to 'generalize' these indicators so similar threat actors may be detected too. The possibilities are great, and the world is your oyster.

To maximize our efficiency, we will transform these IOCs into detection rules in a vendor-agnostic format using Sigma, however, you can opt to use whichever format you're familiar with.

Sigma is an open-source generic signature language developed to describe log events in a structured format. This allows for quick sharing of detection methods by security analysts. It also allows for a more flexible way of 'storing' a detection method as it can be easily transformed into different formats depending on the SIEM that you're using. This can be achieved through tools such as Uncoder.io, among others.

Let's find the malware-hosting IPs in our SoD, and create a detection mechanism for them. A basic example of how it can be written into a functional Sigma rule is as follows.

tal0nixIPdownloads.yml

```
title: Executable Download from tal0nix IPs
status: test
description: Detects download of .exe files from tal0nix IP hosts found in the SoD
reference: https://github.com/SigmaHQ/sigma/blob/master/rules/windows/create_stream_hash/create_stream_hash_susp_ip_domains.yml
author: Mokmokmok
date: 2023/07/13
modified: 2023/07/13
logsource:
  product: windows
  category: create_stream_hash
detection:
  selection:
    Contents:
      - 'http://188.40.75.132'
      - 'http://3.250.38.141'
    TargetFilename|contains:
      - '.exe:Zone'
  condition: selection
falsepositives:
  - Unkown
level: High
```

The Sigma rule that we came up with from some of the details in the SoD is very simple and straightforward, yet the additional layer of detection that it gives the organization is invaluable. This is one of the reasons why this phase of the IR process should never be slept on.

****

Answer the questions below:

What did we use to transform IOCs as detection rules in a vendor-agnostic format?

Answer: Sigma

In the Sigma Rule that we've created, what is the logsource category used by the author?

```
logsource:
  product: windows
  category: create_stream_hash
```

Answer: create_stream_hash

Conclusion

This room aimed to tie up the most important lessons from all of the prior phases of the Incident Response framework. A recap of the SwiftSpend Incident was done to make way for the discussion of how and why Executive and Technical Summaries are written, which is immediately followed by a review of these summaries.

Finally, a sample Sigma Rule has been created to emphasize one of the final processes of this phase of Incident Response. which is to improve the organization's detection mechanism, effectively going full circle.