Building an Actionable Intel Program - Presentation Notes typed by a human and not AI

Jeffrey - LinkedIn

- What the @#$& is Threat Intelligence?
    - "detailed, actionable information about cybersecurity threats. Threat intelligence helps security teams take a more proactive approach to detecting, mitigating, and preventing cyberattacks." -IBM.
    - Money doesn't hurt a program, but you do NOT need a six-figure budget to create a Threat Intelligence Program at your Company!

- If not applied correctly, threat intelligence can exist only in theory without producing tangible results through actionable steps!
    - Ensure your program drives change and informs business risk based on your intelligence.

- Why create a Threat Intel Program? (from Intel471)
    - *Early threat detection mitigates pending attacks* - Example is Dark Web monitoring for infostealer creds of your company that are available for purchase to thwart pending attacks.
    - *Understand threat actors for a proactive defense* - Know Thy Adversary. Understand threat actors that target healthcare, who they are, what they are interested in, and their sponsorship (e-crime vs. state-sponsored)
    - *Prioritize vulnerability management* - In a world of endless vulnerabilities to remediate, threat intelligence can help you understand what vulnerabilities are "popular" right now among threat actors. Historic ways of prioritizing vulnerabilities, like prolificacy or CVSS score, can overlook different ways threat actors chain vulnerabilities or even introduce an application vulnerable to exploitation.
    - *Inform strategic decisions for business* - With a limited budget comes little room for error when choosing what projects to fund. Threat Intelligence can help InfoSec leaders understand the current threat landscape and plan future projects to fill/strengthen gaps.

- Dangers of Cobwebbed Intelligence (when intelligence sits on a shelf and isn't used actionably)
    - Discouraged employees
    - The program is seen as a waste of resources and may get axed
    - The organization doesn't see benefits

- Intelligence Lifecycle by Flashpoint

1. **Planning & Direction**
    a. What is the point of the Intelligence (Intelligence Requirement) we are collecting, and what is the goal?
        i. This guidance usually comes from Senior InfoSec leadership
    b. Our Intelligence Requirement that we will walk through is: *Understand threat actors for a proactive defense*

2. **Collection**
    a. Where can I find information on adversaries that target Healthcare?
    b. Free blogs/articles

c. If your program has a Threat Intel tool or receives finished intelligence, use it! However, make sure you're not siloing your adversarial intelligence to one source.
d. MITRE ATT&CK - Our "Rosetta Stone" for us to speak a common language regarding adversarial techniques across any security vendor's report through T-codes (ex, T1234.001)
e. Google Dork to find webpages/PDFs of T-codes for a specific adversary: **`"qilin" intext:"att&ck"`**

3. **Analysis**
   a. Through the open-source reports you read, look for T-codes and then look for any overlaps among threat actors:

A	B	C
Adversary	**Technique**	
INC	T1087.002	
INC	T1071	
INC	T1560.001	
INC	T1059.003	
INC	T1486	
INC	T1074	
INC	T1190	
INC	T1657	
INC	T1562.001	
INC	T1070.004	
INC	T1105	
INC	T1570	
INC	T1036.005	
INC	T1046	
INC	T1135	
INC	T1588.002	
INC	T1069.002	
INC	T1566	
INC	T1219	

Rhysida	T1078.003
Rhysida	T1203
Rhysida	T1059.001
Rhysida	T1053.005
Rhysida	T1204.002
Rhysida	T1053.005
Rhysida	T1068
Rhysida	T1041
Rhysida	T1486
Scattered Spider	T1087.002
Scattered Spider	T1087.003
Scattered Spider	T1087.004
Scattered Spider	T1098.001
Scattered Spider	T1098.003
Scattered Spider	T1098.005
Scattered Spider	T1217
Scattered Spider	T1580
Scattered Spider	T1538
Scattered Spider	T1136
Scattered Spider	T1486

Qilin	T1657
Qilin	T1021.001
Qilin	T1021.002
Qilin	T1021.004
Qilin	T1091
Qilin	T1570
Qilin	T1005
Qilin	T1001
Qilin	T1011.001
Qilin	T1486
Qilin	T1489
Qilin	T1490
Qilin	T1529
Qilin	T1561.001
Qilin	T1562.001
Qilin	T1562.002
Qilin	T1562.009
Qilin	T1574.010
Qilin	T1003
Qilin	T1552.001

4. **Production**
   a. Utilize ATT&CK to develop mitigations and detections
      i. Mitigation - prevent a technique or sub-technique from being successfully executed
         1. Cross-reference the mitigations currently in place at your organization with MITRE's recommendations. Where are the gaps?

Technique	Current Mitigation	Areas for improvement
Windows Management Instrumentation (T1047)	We utilize a PAM tool that ensures Help Desk Local Admin and Administrator accounts have unique passwords that are rotated after each use	Restrict non-admin users from utilizing WMI by "disallowing users access to a specific WMI namespace" https://learn.microsoft.com/en-us/windows/win32/wmisdk/securing-a-remote-wmi-connection

        ii. Detection - identifies when malicious or suspicious activity occurs
    b. Threat actors practice sheep think mirroring tactics, techniques, and procedures (TTPs) from one another. As a result, developing mitigations and detections for specific T-codes can disrupt not only the actor you initially observed but also others who adopt the same malicious techniques.

5. **Dissemination and Feedback**
    a. Don't just share or present the report; depending on who you are sharing your intelligence with, you may need to tweak the format and technical jargon.
    b. In my experience, the best way to enact change based on your actionable intelligence is to incorporate mitigations and detections into projects that may be more adept at implementing a big environmental change (ex, ingesting firewall and switch logs into your SIEM and creating detections).