Guest Lecture: Intro to Cyber Threat Intelligence & Threat Hunting

By Adrian Korn

About Me

Adrian Korn

- Manager of Threat Intelligence Research
- Co-Organizer of DEFCON Toronto (DC416)
- Former Director of OSINT Operations
- Previous stints in SOC, Threat Detection, Threat Intelligence, & Threat Hunting
- Bachelor’s Degree in InfoSec & Diploma in Computer Networking

Agenda

01 Introduction to Cyber Threat Intelligence

02 CTI case study

03 Introduction to Threat Hunting

04 Careers Paths and Resources for Cyber Threat Intelligence & Threat Hunting

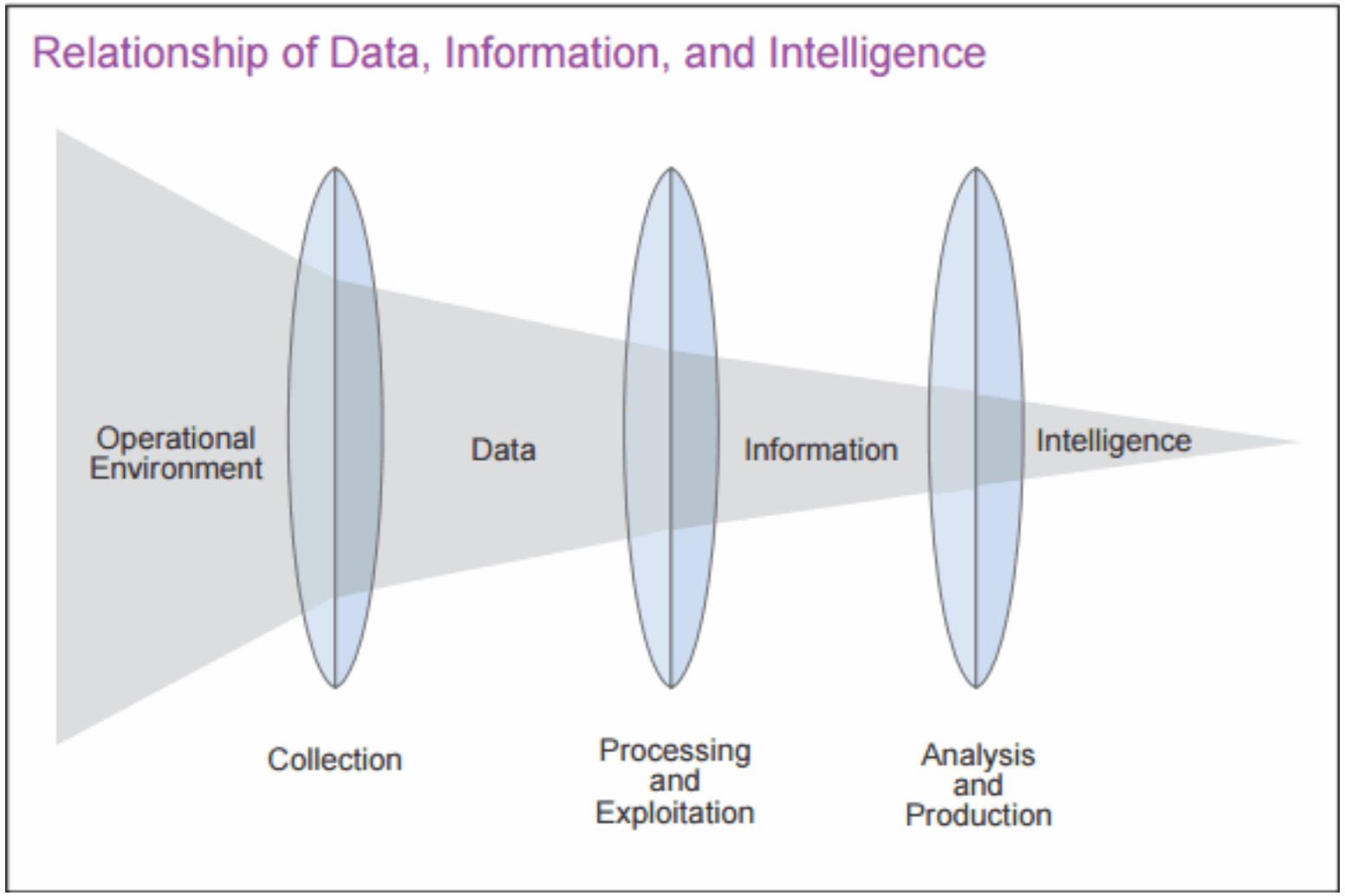
05 Questions?

Introduction to Cyber Threat Intelligence

What is Cyber Threat Intelligence?

Cyber Threat intelligence (CTI) is data that is collected, processed, and analyzed to create ”intelligence”. This intelligence helps stakeholders understand a threat actor’s motives, targets, and attack behaviors. CTI enables organizations to make faster, more informed, intel-driven security decisions and change an organization’s behavior from reactive to proactive in the fight against threat actors.

How is Intelligence Created?



What are Indicators of Compromise?

An Indicator of Compromise (IOC) is a digital forensics artifact that **suggests** an endpoint or network may have been compromised

Examples of IOCs include:

- Known Command and Control Server IPs, Domains, and URLs
- Hash of known malware
- Registry keys that appear when a threat actor changes something on a system

Sources of IOCs include:

- An organization who has experienced an incident shares IOCs with you
- Open source or private threat feeds from communities and companies
- Staying one step ahead of threat actors and tracking their infrastructure to know IOCs before they are ever seen

What are Tactics, Techniques, and Procedures?

Tactics, Techniques, and Procedures (TTPs) describe the behaviour of a threat actor.

- **Tactics** – Represent a threat actor's tactical goal: the reason for performing an action (WHY)
  - Example: A threat actor may want to achieve credential access.

- **Techniques** – Represent how a threat actor achieves a tactical goal. (HOW)
  - Example: A threat actor may dump credentials from a system to achieve credential access.

- **Procedures** – Represent specific implementation a threat actor uses for techniques (DETAILED HOW)
  - Example: A threat actor uses PowerShell to inject into lsass.exe process to dump credentials by scraping LSASS memory on a victim host.

What is MITRE ATT&CK?

ATT&CK is a knowledge base of cyber adversary behavior and taxonomy for adversarial actions across their lifecycle. ATT&CK has two parts: ATT&CK for Enterprise, which covers behavior against enterprise IT networks and cloud, and ATT&CK for Mobile, which focuses on behavior against mobile devices.

Source: MITRE Corporation

MITRE ATT&CK Framework Tactics

Enterprise tactics

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

Enterprise Tactics: 14

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

MITRE ATT&CK Framework Techniques

Enterprise Techniques

Techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.

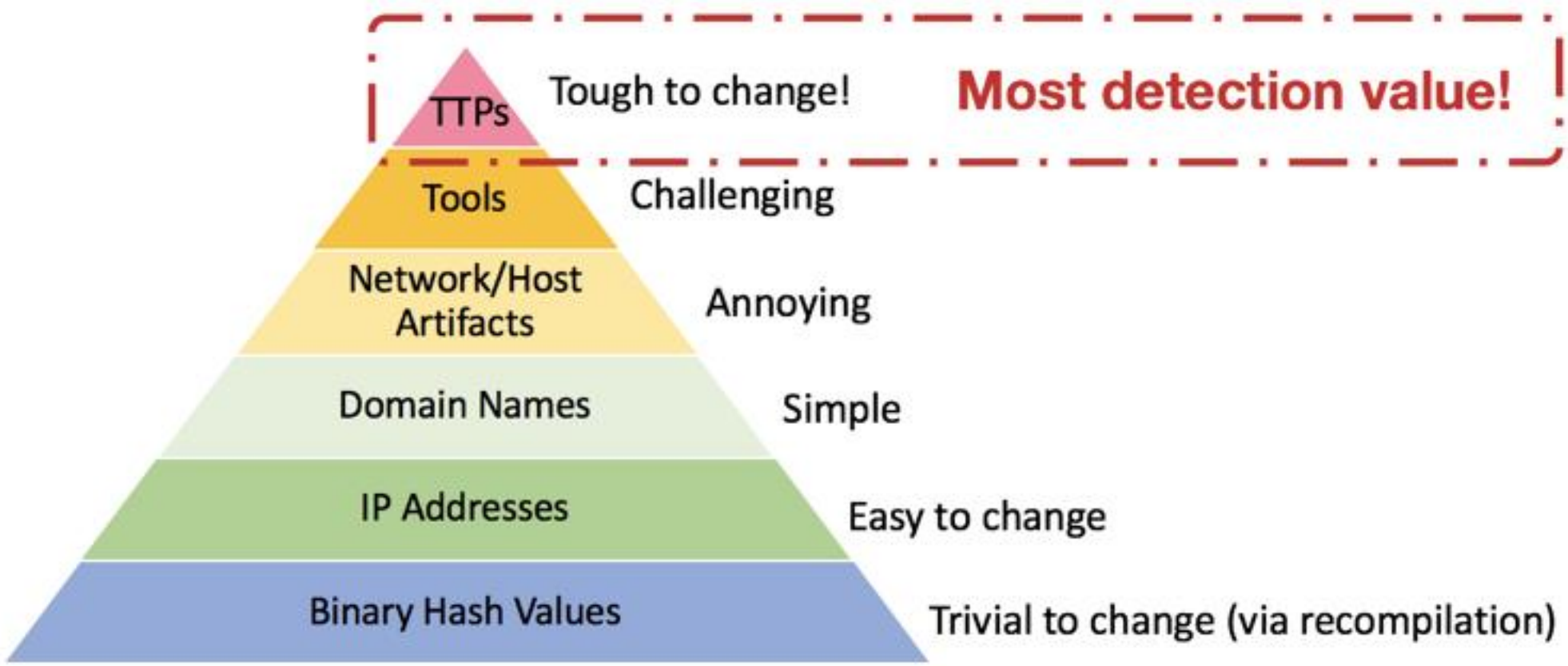
Techniques: 193
Sub-techniques: 401

ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.
.001	Setuid and Setgid	An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS, when the setuid or setgid bits are set for an application binary, the application will run with the privileges of the owning user or group respectively. Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them may not have the specific required privileges.
.002	Bypass User Account Control	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.
.003	Sudo and Sudo Caching	Adversaries may perform sudo caching and/or use the sudoers file to elevate privileges. Adversaries may do this to execute commands as other users or spawn processes with higher privileges.
.004	Elevated Execution with Prompt	Adversaries may leverage the `AuthorizationExecuteWithPrivileges` API to escalate privileges by prompting the user for credentials. The purpose of this API is to give application developers an easy way to

What has the most Detection value?

IOCs or TTPs?

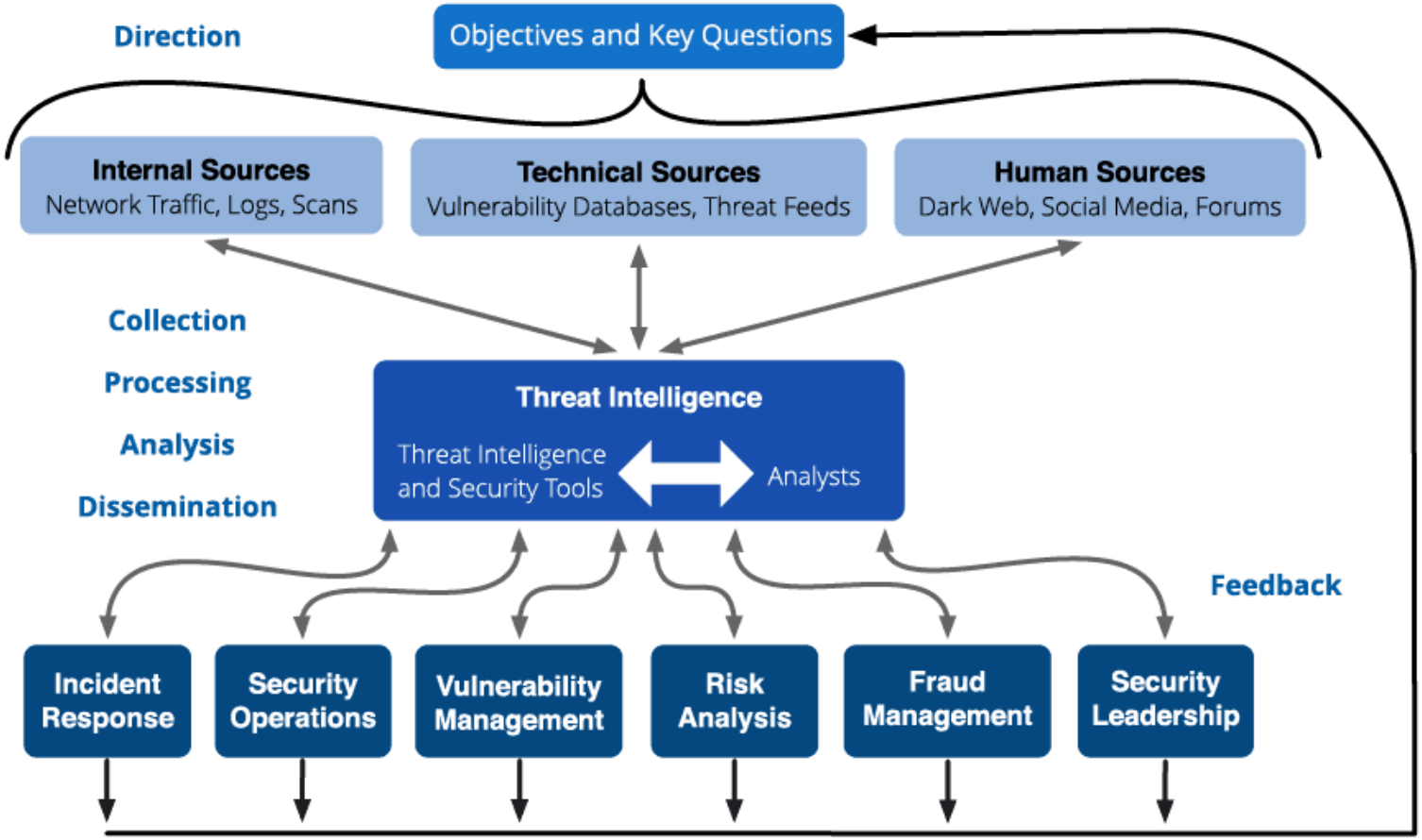
Pyramid of Pain



Valuable Threat Actor TTPs to Track

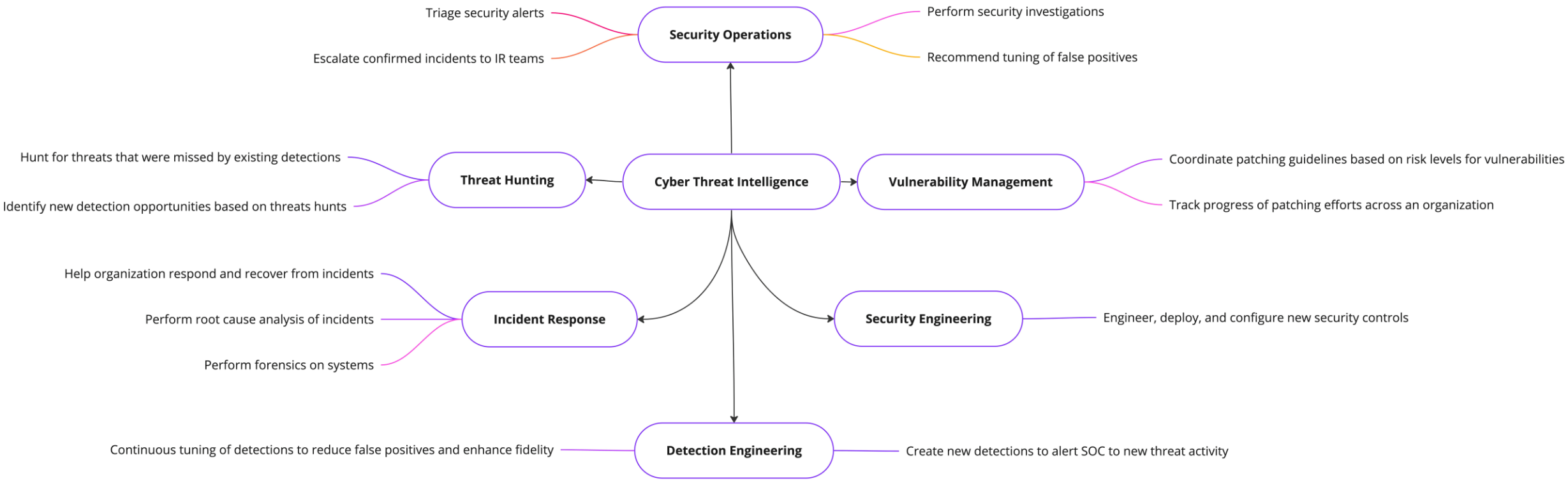
- Types of malware they use
  - Eg. Emotet, Qakbot, Gootloader, etc.
- Type of Infrastructure they are using
  - Eg. Shady hosting providers
- Vulnerabilities they exploit
  - Eg. Log4Shell, ProxyLogon, etc.
- Tools they use
  - Eg. Cobalt Strike, Mimikatz, PowerShell, etc.

Cyber Threat Intelligence Lifecycle



Source: Recorded Future

How does CTI fit in with other security teams?

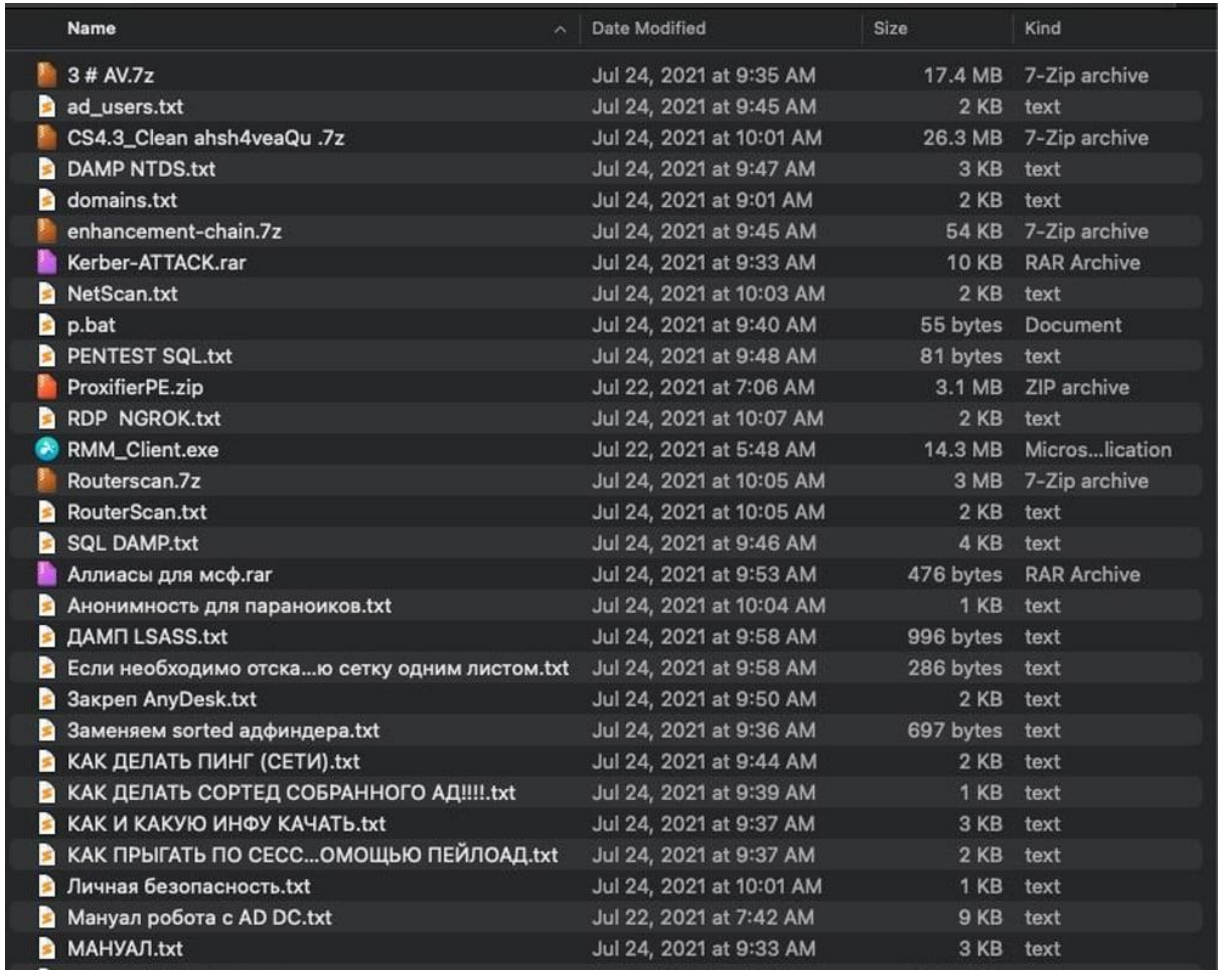


Case Study:
Conti Ransomware
Leaked Playbook

Conti Playbook Leak: What happened?

- In September 2021, a disgruntled affiliate of the Conti Ransomware group leaked Conti's playbook on a hacker forum
- This was a significant OPSEC risk for Conti as it exposed how their affiliates are instructed to carry out attacks
- Within Ransomware groups, affiliates are often given playbooks by the leaders of the group that train them on how to effectively compromise targets, exfiltrate data, and encrypt their systems

What files were leaked?



Name	Date Modified	Size	Kind
3 # AV.7z	Jul 24, 2021 at 9:35 AM	17.4 MB	7-Zip archive
ad_users.txt	Jul 24, 2021 at 9:45 AM	2 KB	text
CS4.3_Clean ahsh4veaQu .7z	Jul 24, 2021 at 10:01 AM	26.3 MB	7-Zip archive
DAMP NTDS.txt	Jul 24, 2021 at 9:47 AM	3 KB	text
domains.txt	Jul 24, 2021 at 9:01 AM	2 KB	text
enhancement-chain.7z	Jul 24, 2021 at 9:45 AM	54 KB	7-Zip archive
Kerber-ATTACK.rar	Jul 24, 2021 at 9:33 AM	10 KB	RAR Archive
NetScan.txt	Jul 24, 2021 at 10:03 AM	2 KB	text
p.bat	Jul 24, 2021 at 9:40 AM	55 bytes	Document
PENTEST SQL.txt	Jul 24, 2021 at 9:48 AM	81 bytes	text
ProxifierPE.zip	Jul 22, 2021 at 7:06 AM	3.1 MB	ZIP archive
RDP NGROK.txt	Jul 24, 2021 at 10:07 AM	2 KB	text
RMM_Client.exe	Jul 22, 2021 at 5:48 AM	14.3 MB	Micros...lication
Routerscan.7z	Jul 24, 2021 at 10:05 AM	3 MB	7-Zip archive
RouterScan.txt	Jul 24, 2021 at 10:05 AM	2 KB	text
SQL DAMP.txt	Jul 24, 2021 at 9:46 AM	4 KB	text
Аллиасы для мсф.rar	Jul 24, 2021 at 9:53 AM	476 bytes	RAR Archive
Анонимность для параноиков.txt	Jul 24, 2021 at 10:04 AM	1 KB	text
ДАМП LSASS.txt	Jul 24, 2021 at 9:58 AM	996 bytes	text
Если необходимо отска...ю сетку одним листом.txt	Jul 24, 2021 at 9:58 AM	286 bytes	text
Закреп AnyDesk.txt	Jul 24, 2021 at 9:50 AM	2 KB	text
Заменяем sorted адфиндера.txt	Jul 24, 2021 at 9:36 AM	697 bytes	text
КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt	Jul 24, 2021 at 9:44 AM	2 KB	text
КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt	Jul 24, 2021 at 9:39 AM	1 KB	text
КАК И КАКУЮ ИНФУ КАЧАТЬ.txt	Jul 24, 2021 at 9:37 AM	3 KB	text
КАК ПРЫГАТЬ ПО СЕСС...ОМОЩЬЮ ПЕЙЛОАД.txt	Jul 24, 2021 at 9:37 AM	2 KB	text
Личная безопасность.txt	Jul 24, 2021 at 10:01 AM	1 KB	text
Мануал робота с AD DC.txt	Jul 22, 2021 at 7:42 AM	9 KB	text
МАНУАЛ.txt	Jul 24, 2021 at 9:33 AM	3 KB	text

How did the CTI Community Benefit from this?

Conti Leaked Playbook TTPs

1 Tactic Specific
- 1.1 Execution
- 1.2 Persistence
- 1.3 Defense Evasion
- 1.4 Credential Access
- 1.5 Discovery
- 1.6 Collection
- 1.7 Command and Control
- 1.8 Exfiltration

2 Software Specific
- 2.1 Cobalt Strike (S0154)
- 2.2 AdFind (S0552)
- 2.3 PowerSploit (S0194)
- 2.4 Ngrok (S0508)
- 2.5 PsExec (S0029)
- 2.6 Atera Agent

Tactic Specific

Execution

ID	Tactic	Context
T1059.003	Command and Scripting Interpreter: Windows Command Shell	• Executing `trendmicro pass AV remove.bat` to remove AV • Executing multiple commands from Windows Command Shell using Cobalt Strike
T1059.001	Command and Scripting Interpreter: PowerShell	• Executing `rclonemanager.ps1` to automate their exfiltration. • Executing multiple commands from PowerShell using Cobalt Strike

T1053.005	Scheduled Task/Job: Scheduled Task	• Cobalt Strike commands for scheduling tasks
		  • `shell SCHTASKS /s ip\hostname /RU "SYSTEM" /create /tn "WindowsSensor15" /tr "cmd.exe /c C:\ProgramData\P32.exe" /sc ONCE /sd 01 /01/1970 /st 00:00`
		  • `shell SCHTASKS /s ip\hostname /run /TN "WindowsSensor15"`
		  • `shell schtasks /S ip\hostname /TN "WindowsSensor15" /DELETE /F`

Source: https://github.com/DISREL/Conti-Leaked-Playbook-TTPs

How did the CTI Community Benefit from this?

T1562.001	Impair Defenses: Disable or Modify Tools	• Using `Bitdefender_2019_Uninstall_Tool.exe` to uninstall any Bitdefender products.
		• Using `gmer.exe`, `PCHunter32/64.exe`, `PowerTool/64.exe` to disable Windows Defender and delete `MsMpEng.dll`
		• Using `trendmicro pass AV remove.bat` to uninstall Trend Micro AV products.
		• Disable Microsoft Defender using `powershell Set-MpPreference -DisableRealtimeMonitoring $true`
		• Disable Microsoft Defender using GUI on RDP
		  • Open `gpedit.msc`
		  • `Computer Configuration - Administrative Templates - Windows Components - Windows Defender`
		  • Disable “Protection in Real Time”

T1112	Modify Registry	• Modify registry to allow Trend Micro AV uninstallation `reg add "HKLM\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc." /v "Allow Uninstall" /t REG_DWORD /d 1 /f` • Modify registry to allow RDP connections `reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f && reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fAllowToGetHelp /t REG_DWORD /d 1 /f` • Add registry using PowerShell to enable/change RDP port • `Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name PortNumber -Value 1350`

T1562.004	Impair Defenses: Disable or Modify System Firewall	• Modify firewall to allow RDP connections
		  • `NetSh Advfirewall set allprofiles state off`
		  • `netsh advfirewall firewall set rule group="remote desktop" new enable=Yes`
		  • `netsh firewall set service type = remotedesktop mode = enable`
		• Add firewall rules using PowerShell to enable/change RDP port
		  • `New-NetFirewallRule -DisplayName "New RDP Port 1350" -Direction Inbound -LocalPort 1350 -Protocol TCP -Action allow`
		  • `New-NetFirewallRule -DisplayName "New RDP Port 1350" -Direction Inbound -LocalPort`

Source: https://github.com/DISREL/Conti-Leaked-Playbook-TTPs

Introduction to Threat Hunting

What is Threat Hunting?

Using knowledge of threat actor TTPs to hunt for threats in your network what have gone previously undetected. Threat Hunts leverage an ”assumed breach” methodology.

Why would an Organization Threat Hunt?

- Sophisticated threat actors will deploy a variety of evasive measures to avoid detections
- Threat Actors will leverage previously unknown techniques in their attacks (eg. Zero-day exploits)
- Organizations with mature security programs want to threat hunt so they identify a missed threat before it becomes a breach

What do you need to Threat Hunt?

- Deep understanding of threat actor TTPs (CTI can help here)
- Telemetry and Data (logs from endpoint, network, and applications)
- Understanding of the network you are hunting in

Threat Hunting Framework

Source: Gigamon

What is fun about threat hunting?

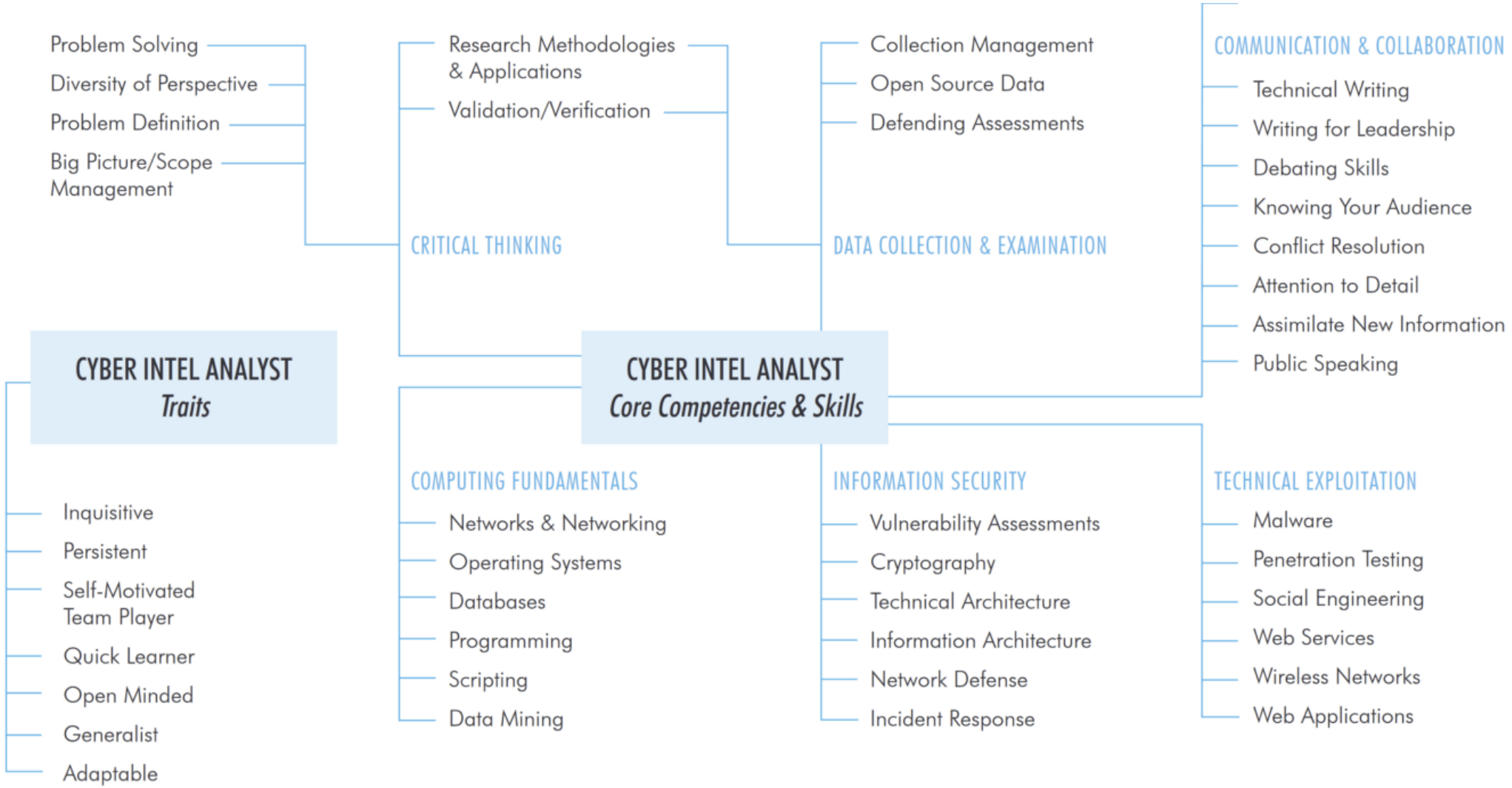
- The thrill of finding a threat that every security control failed to prevent and every detection missed
- The thrill of catching a threat actor red handed
- Finding a threat before it escalates into a breach situation
- Everyday is a challenge. New TTPs emerge and there are new hunts to do
- You are not bound to the same type of hunts every day vs. a SOC analyst may look at similar alerts everyday

What is challenging about threat hunting?

- Very easy to go down a rabbit hole…..
  - Eg. Ad trackers behave like malware but are typically benign.
- Coming up with new hunts (lots of creativity and research needed)
- Keeping up to date with all the new threat actor TTPs and how to hunt for them
- Finding that needle in the haystack…

Careers Paths and Resources for Cyber Threat Intelligence & Threat Hunting

What Skills do you need to become a CTI Analyst?



Source: Intelligence and National Security Alliance (INSA)

Threat Hunter Competencies

- Many similar traits looked for in CTI Analysts are also sought after for Threat Hunters

- Key soft skills:
  - Curiosity
  - Attention to detail
  - Creativity

- Key technical skills:
  - Foundational understanding of forensic artifacts
  - Strong with SIEMs and querying them
  - Deep understanding of different log types and what they mean
  - Knowledge of MITRE ATT&CK and threat actor tradecraft

Roles in Cyber Security that do Cyber Threat Intelligence

- Threat Intelligence Analyst
- Security Intelligence Analyst
- Cyber Threat Intelligence Analyst
- Cyber Intelligence Analyst
- Threat Intelligence Specialist
- Threat Intelligence Advisor
- Threat Researcher
- Threat Intelligence Researcher
- Malware Researcher
- Malware Analyst
- Security Researcher
- Threat Analyst
- Security Analyst

Roles in Cyber Security that do Threat Hunting

- Threat Hunter
- Cyber Threat Hunter
- Threat Analyst
- Cyber Threat Analyst
- Security Analyst

Resources for Learning more about CTI & Threat Hunting

1. Katie Nickels' self-study CTI resources:
    1. https://medium.com/katies-five-cents/faqs-on-getting-started-in-cyber-threat-intelligence-f567f267348e
    2. https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-2-d04b7a529d36
    3. https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-1-968b5a8daf9a

2. Psychology of Intelligence Analysis By Richard J. Heuer

3. Security & Threat Intel Blogs:
    1. https://blog.talosintelligence.com/
    2. https://arcticwolf.com/resources/security-bulletins
    3. https://blog.google/threat-analysis-group/
    4. https://unit42.paloaltonetworks.com/
    5. https://krebsonsecurity.com/
    6. https://www.bleepingcomputer.com/
4. Awesome Threat Hunting - https://threat-hunting.github.io/awesome_Threat-Hunting/

Contact Info

Adrian Korn

- Email: Adrian@defcontoronto.com
- Twitter: @AK47Intel
- LinkedIn: /in/adrian-korn

Questions?