Presented by: corelight OPTIV SANS

Demystifying The Hunt:

How to Assess Threat Hunting Readiness and Prepare for the Next Step

Today’s speakers

Fayyaz Rajpari

Global Executive Services Director

OPTIV

Gary Fisk

Sales Engineer

corelight

Matt Bromiley

SANS Digital Forensics & IR Instructor

SANS

J

Agenda

1. Hunting 101 roundtable
2. Assessing your readiness
3. Operationalizing the hunt
4. Sample hunts
5. Q&A

Hunting 101

J

What is threat hunting?

J

As a hunter,
where do you look for evidence?

J

How do you form strong hunting hypotheses?

J

What makes
the most effective threat hunters
successful?

Assessing the maturity of your threat hunting program.

Are the right eyes are on your Kingdom?

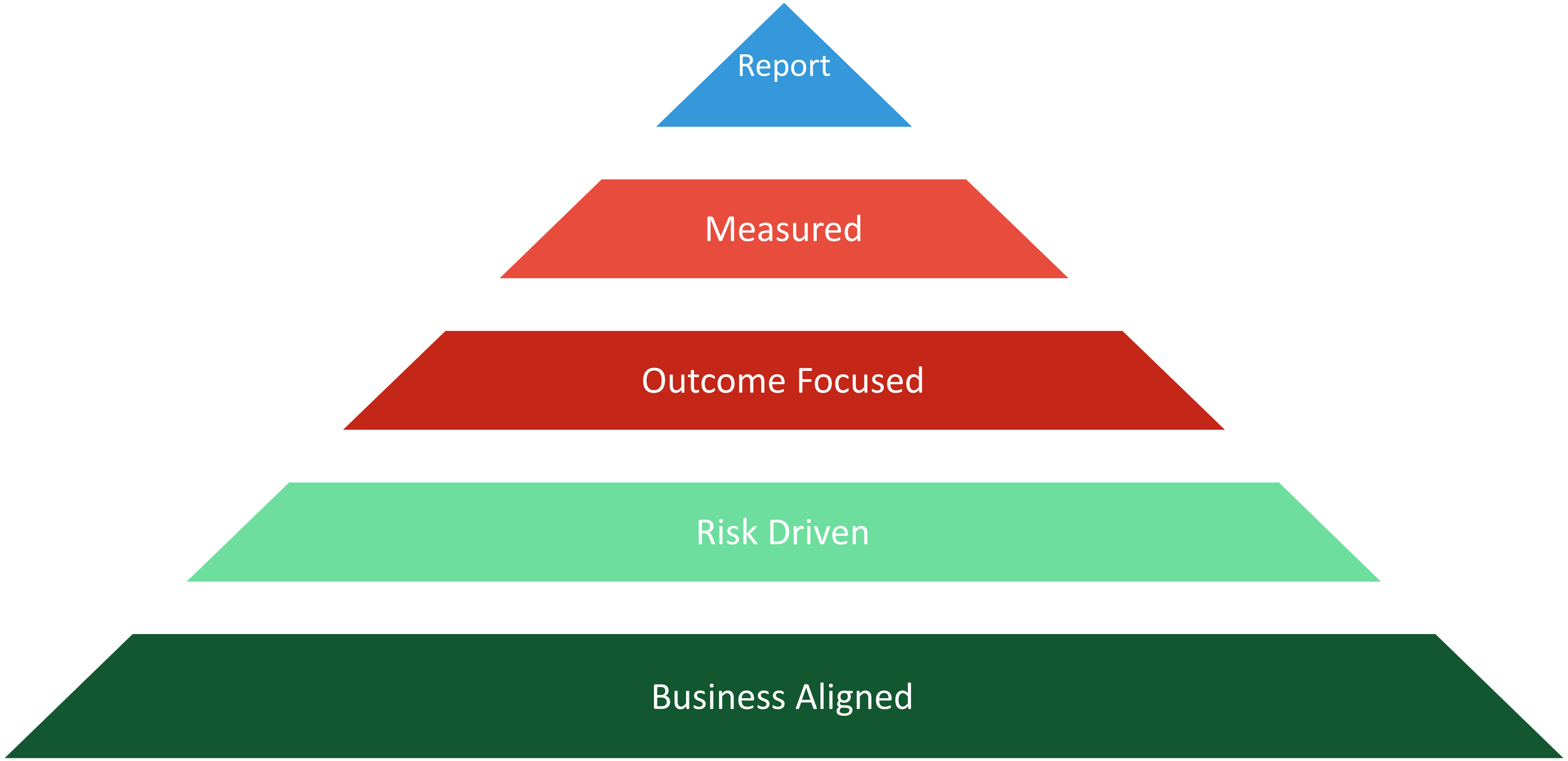
Do you monitor all points of entrance and exits?

Has anyone gone rogue?

Why are they in your kingdom?

What are they stealing and how?

Setting the Foundation



Report

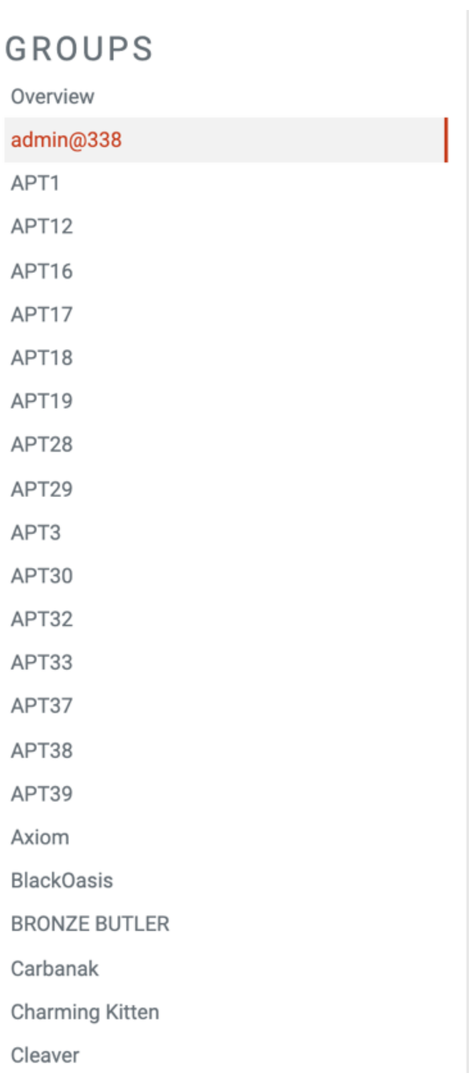
Measured

Outcome Focused

Risk Driven

Business Aligned

Know your adversary!



GROUPS

Overview

admin@338

APT1

APT12

APT16

APT17

APT18

APT19

APT28

APT29

APT3

APT30

APT32

APT33

APT37

APT38

APT39

Axiom

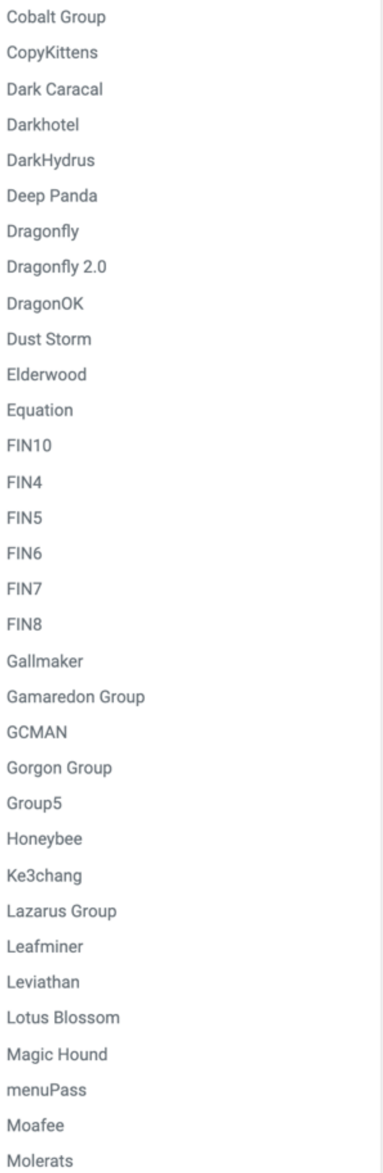
BlackOasis

BRONZE BUTLER

Carbanak

Charming Kitten

Cleaver



Cobalt Group

CopyKittens

Dark Caracal

Darkhotel

DarkHydrus

Deep Panda

Dragonfly

Dragonfly 2.0

DragonOK

Dust Storm

Elderwood

Equation

FIN10

FIN4

FIN5

FIN6

FIN7

FIN8

Gallmaker

Gamaredon Group

GCMAN

Gorgon Group

Group5

Honeybee

Ke3chang

Lazarus Group

Leafminer

Leviathan

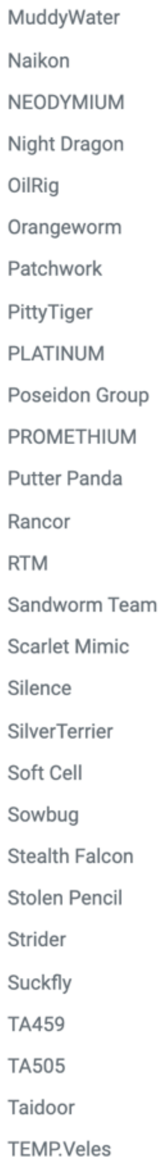
Lotus Blossom

Magic Hound

menuPass

Moafee

Molerats



MuddyWater

Naikon

NEODYMIUM

Night Dragon

OilRig

Orangeworm

Patchwork

PittyTiger

PLATINUM

Poseidon Group

PROMETHIUM

Putter Panda

Rancor

RTM

Sandworm Team

Scarlet Mimic

Silence

SilverTerrier

Soft Cell

Sowbug

Stealth Falcon

Stolen Pencil

Strider

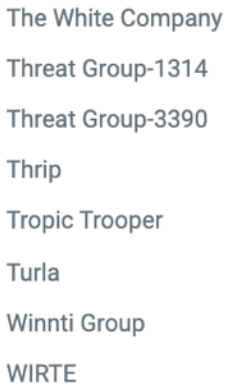
Suckfly

TA459

TA505

Taidoor

TEMP.Veles



The White Company

Threat Group-1314

Threat Group-3390

Thrip

Tropic Trooper

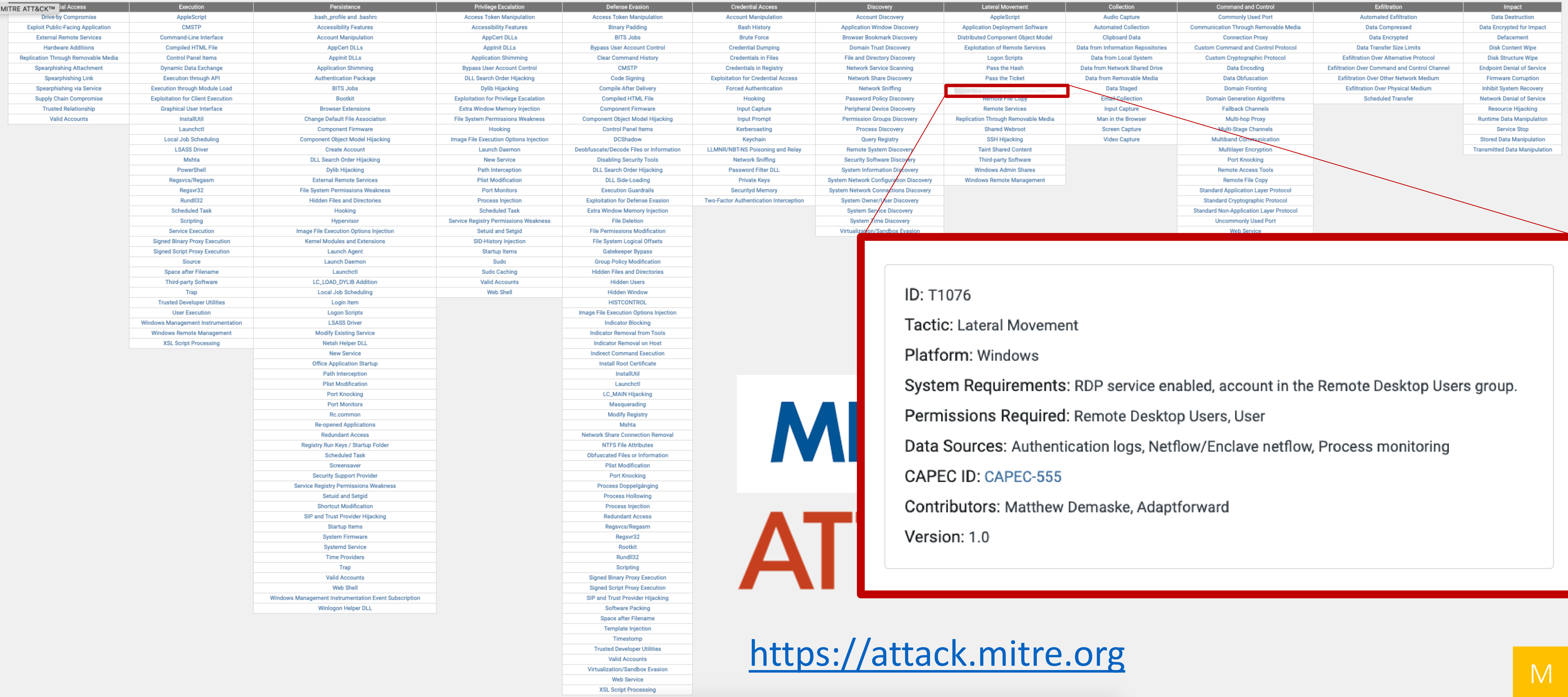
Turla

Winnti Group

WIRTE

https://attack.mitre.org/groups/

Know their techniques and tactics!



MITRE ATT&CK™

ial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	[illegible]	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelgänging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

ID: T1076

Tactic: Lateral Movement

Platform: Windows

System Requirements: RDP service enabled, account in the Remote Desktop Users group.

Permissions Required: Remote Desktop Users, User

Data Sources: Authentication logs, Netflow/Enclave netflow, Process monitoring

CAPEC ID: CAPEC-555

Contributors: Matthew Demaske, Adaptforward

Version: 1.0

https://attack.mitre.org

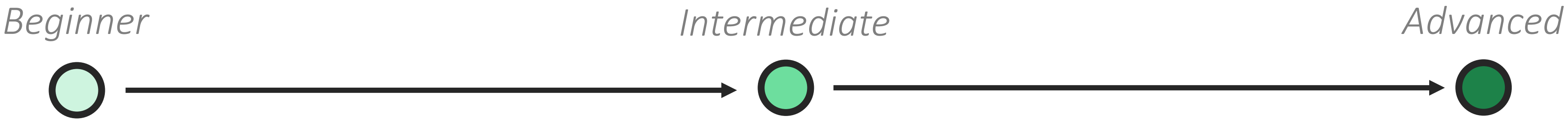
Five areas of threat hunting maturity

- Data
- Tools
- People & process
- Threat intel
- Automation

Icons made by [monkik] from www.flaticon.com

Assessing hunt maturity: people & process

People & process



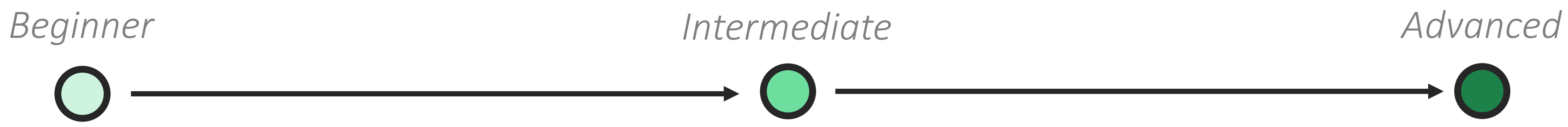
- Hunting = job function
- Hunting for anomalies
- Success = discovery

- Hunting = role
- Hunting for techniques
- Success is evaluated

- Hunting = a team
- Hunting for adversaries
- Success is measured

Assessing hunt maturity: data

Data



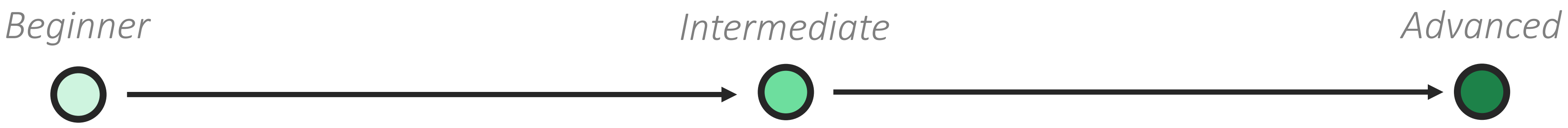
- Ad hoc visibility
- Spotty/dirty/unstructured
- Many data puddles

- Instrumented visibility
- Comprehensive & cleanish
- Data is centralized, mostly

- Architected visibility
- Complete/clean/structured
- A single data lake

Assessing hunt maturity: tools

Tools



Beginner

Intermediate

Advanced

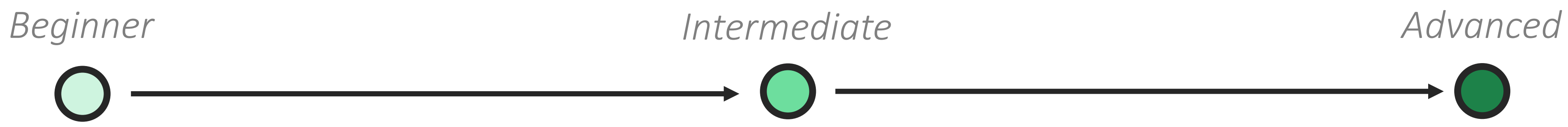
- FOSS Tools
- Single-file Viewers
- Command-Line

- Commercial, OTS
- SIEM/Aggregator
- Command-Line

- Custom-Built, Org-Specific
- Automated Parsing/Ingestion
- Advanced Custom Correlation & Detection

Assessing hunt maturity: threat intel

Threat intel



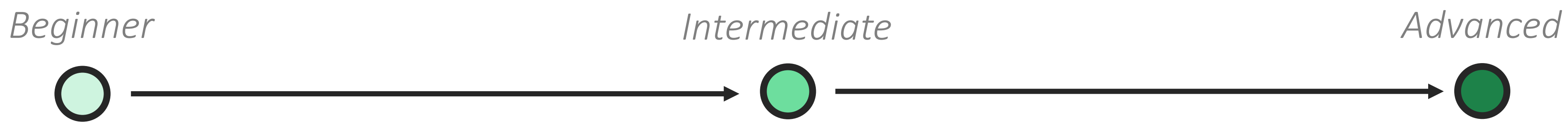
- Packaged vendor content
- Ad hoc procedures/team
- Intermittent

- Curated content (i.e. ISAC)
- Identified intel collectors
- Regularized

- Created content
- Dedicated intel analysts
- Continuous, w/ governance

Assessing hunt maturity: automation

Automation



- Assessing repeatable hunt tasks
- Tool Integrations mapped
- Success = use cases developed

- Scoped playbooks
- Automated actions
- Success is evaluated

- Metrics reported
- Automated hunts
- Success = continuous improvement from metrics

Operationalizing the hunt

For today let’s focus on people, data, and tools

Data

Tools

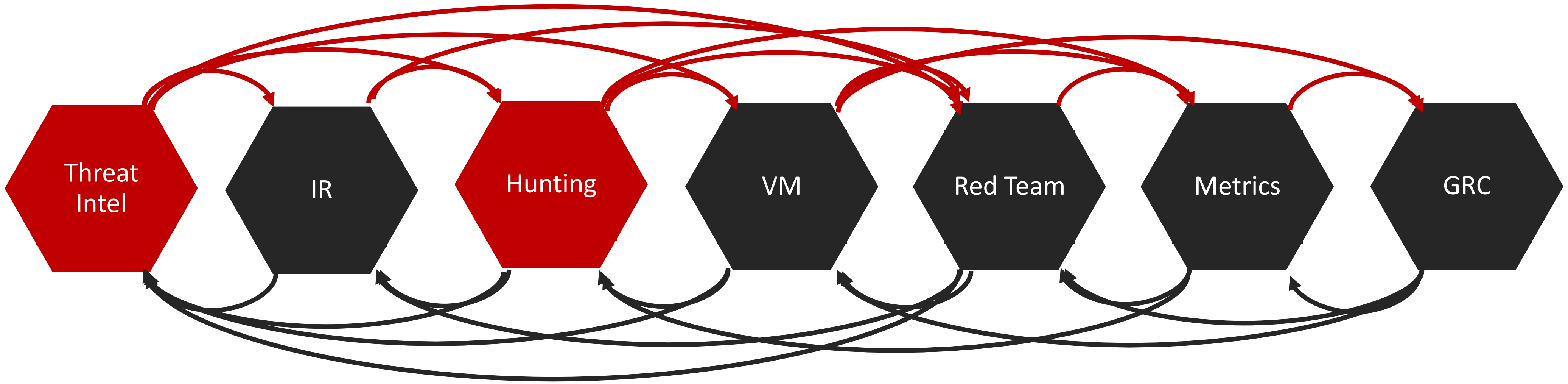
People & process

Threat intel

Automation

Things to think about

People & process



Next steps to take

1. Add hunting skill set as a role
2. Augment with data science backgrounds
3. Have a goal of doing specific and scheduled hunts
4. Collaborate across other cybersecurity teams

People & process

Things to think about

- Hunting: helps you identify data blind spots!
- Integrated data > Isolated data
- Integration does not require consolidation
- Post-collection data integration is time-consuming, thankless, ongoing, but critical!
  - *Character sets, formats, and time coordination will bring you heartache*
- Storage is cheap. High-quality storage at scale is not!

Data

Next steps to take

1. 'Good enough’ asset inventory
2. ”Normal” is relative – learn *your* org’s weirdness
3. Network security monitoring is the fastest way to achieve wide-aperture visibility
4. Assets (and compromises) are on endpoints
5. “Encourage” your vendors to cooperate (ETL is bad)
6. Automated hunting = detection. This is the goal.

Data

Things to think about

- If a tool doesn’t work – move on.
- Work with the data that helps answer your questions.
- Your environment is one entity. Collect & Analyze accordingly.
- Think like an attacker. What would they use?
- **It’s *your* environment. Know the most about it.**

Tools

Next steps to take

1. Start. 1% > 0%
2. If you’re fixing, focus on visibility.
3. If you’re enhancing, ensure visibility and focus on correlation.
4. Echoed sentiment: asset & software inventories.
5. Assess how the whole team benefits from a tool. Adjust accordingly.

Tools

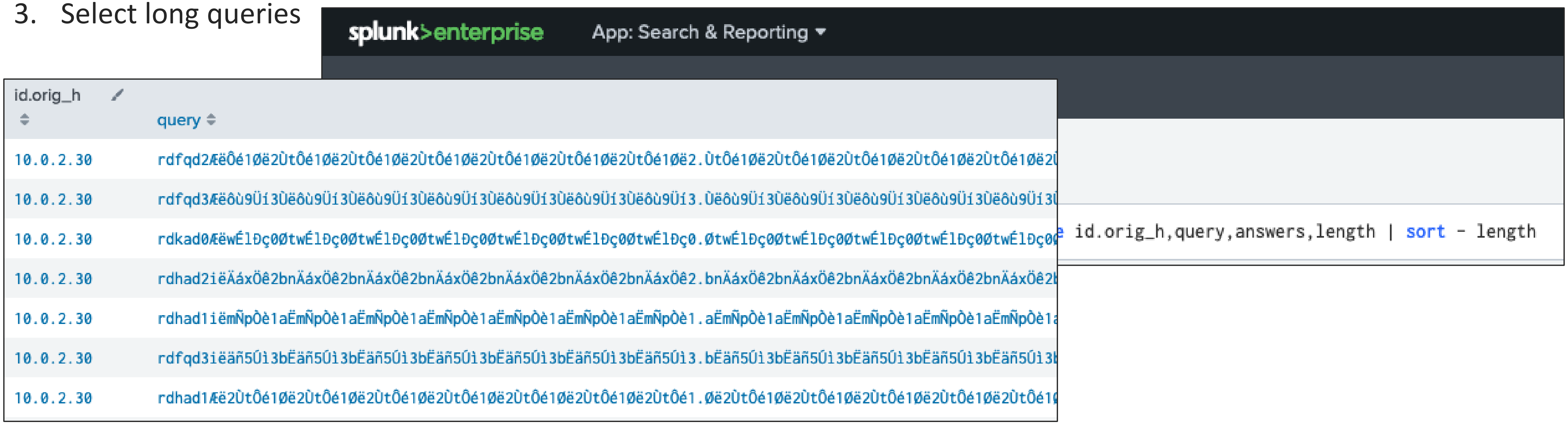
Sample hunts to get you started

J

Data Hiding Hunt (T1320)

Hypothesis – DNS Tunneling may be in use – Use DNS metadata to identify anomalous DNS traffic

1. Instrument the network to track all DNS activity
2. Establish baseline DNS activity and user behaviors (identify false positives from ad networks, etc.)
3. Select long queries



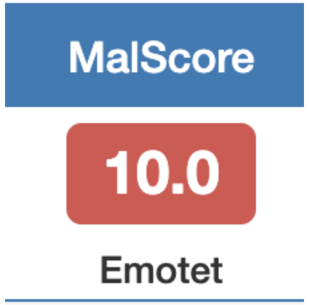
```
e id.orig_h,query,answers,length | sort - length
```

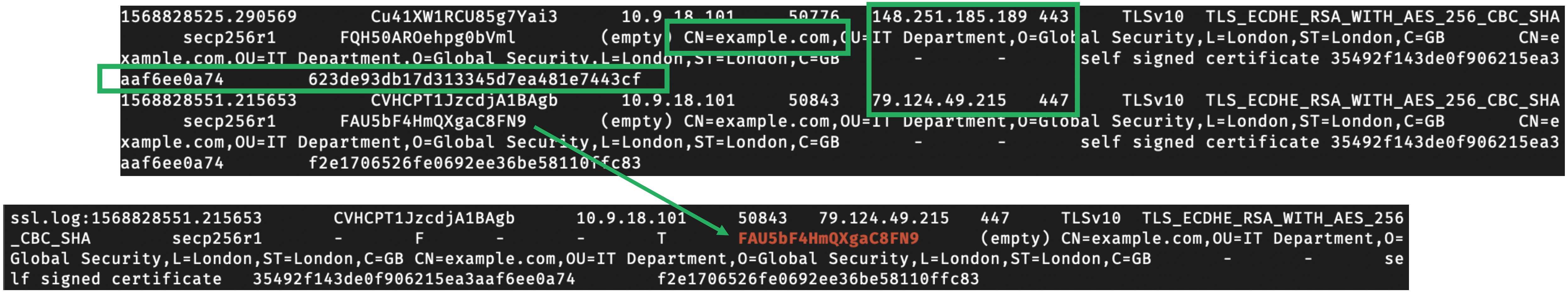
id.orig_h	query
10.0.2.30	rdfqd2ÆëÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2.ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2Ù
10.0.2.30	rdfqd3Æëôù9Üí3Ùëôù9Üí3Ùëôù9Üí3Ùëôù9Üí3Ùëôù9Üí3Ùëôù9Üí3Ùëôù9Üí3Ùëôù9Üí3.Ùëôù9Üí3Ùëôù9Üí3Ùëôù9Üí3Ùëôù9Üí3Ùëôù9Üí3Ù
10.0.2.30	rdkad0ÆëwÉlÐç0ØtwÉlÐç0ØtwÉlÐç0ØtwÉlÐç0ØtwÉlÐç0ØtwÉlÐç0ØtwÉlÐç0ØtwÉlÐç0.ØtwÉlÐç0ØtwÉlÐç0ØtwÉlÐç0ØtwÉlÐç0ØtwÉlÐç0Ø
10.0.2.30	rdhad2iëÄáxÖê2bnÄáxÖê2bnÄáxÖê2bnÄáxÖê2bnÄáxÖê2bnÄáxÖê2bnÄáxÖê2bnÄáxÖê2.bnÄáxÖê2bnÄáxÖê2bnÄáxÖê2bnÄáxÖê2bnÄáxÖê2b
10.0.2.30	rdhad1iëmÑpÒè1aËmÑpÒè1aËmÑpÒè1aËmÑpÒè1aËmÑpÒè1aËmÑpÒè1aËmÑpÒè1aËmÑpÒè1.aËmÑpÒè1aËmÑpÒè1aËmÑpÒè1aËmÑpÒè1aËmÑpÒè1a
10.0.2.30	rdfqd3iëäñ5Úì3bËäñ5Úì3bËäñ5Úì3bËäñ5Úì3bËäñ5Úì3bËäñ5Úì3bËäñ5Úì3bËäñ5Úì3.bËäñ5Úì3bËäñ5Úì3bËäñ5Úì3bËäñ5Úì3bËäñ5Úì3b
10.0.2.30	rdhad1Æë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1.Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Øë2ÙtÔé1Ø

Hunt #2

Hypothesis – Encrypted traffic is in use for C2– Use SSL/TLS fingerprinting to identify suspicious or known-bad activity

1. Capture client/server handshakes for fingerprinting.
2. Identify what's normal in the network (browsers vs. unknowns, common vs. infrequent, timed vs. sporadic)
3. Query, pivot, and correlate with additional traffic metadata.





```
1568828525.290569       Cu41XW1RCU85g7Yai3      10.9.18.101     50776   148.251.185.189 443     TLSv10  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
      secp256r1       FQH50AROehpg0bVml        (empty) CN=example.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB       CN=e
xample.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB        -       -       self signed certificate 35492f143de0f906215ea3
aaf6ee0a74        623de93db17d313345d7ea481e7443cf
1568828551.215653       CVHCPT1JzcdjA1BAgb      10.9.18.101     50843   79.124.49.215   447     TLSv10  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
      secp256r1       FAU5bF4HmQXgaC8FN9       (empty) CN=example.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB       CN=e
xample.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB        -       -       self signed certificate 35492f143de0f906215ea3
aaf6ee0a74        f2e1706526fe0692ee36be58110ffc83
```

```
ssl.log:1568828551.215653       CVHCPT1JzcdjA1BAgb      10.9.18.101     50843   79.124.49.215   447     TLSv10  TLS_ECDHE_RSA_WITH_AES_256
_CBC_SHA        secp256r1       -       F       -       -       T       FAU5bF4HmQXgaC8FN9      (empty) CN=example.com,OU=IT Department,O=
Global Security,L=London,ST=London,C=GB CN=example.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB       -       -       se
lf signed certificate   35492f143de0f906215ea3aaf6ee0a74        f2e1706526fe0692ee36be58110ffc83
```

Summary and pro tips

- Figure out what “normal” means for your environment
- Hunt for who has eyes on YOU, not who others have eyes on
- Consider *pre*-ATT&CK to understand adversary goals and methods
- MITRE ATT&CK = 314 documented adversary techniques
- Launch specific hunts and map to specific TTPs in ATT&CK
- Start with a top 5, then 10, then more
- Network security monitoring = fast path to wide-aperature visibility

Q+A

Q+A

Fayyaz Rajpari

Global Executive Services Director

OPTIV

Gary Fisk

Sales Engineer

corelight

Matt Bromiley

SANS Digital Forensics & IR Instructor

SANS