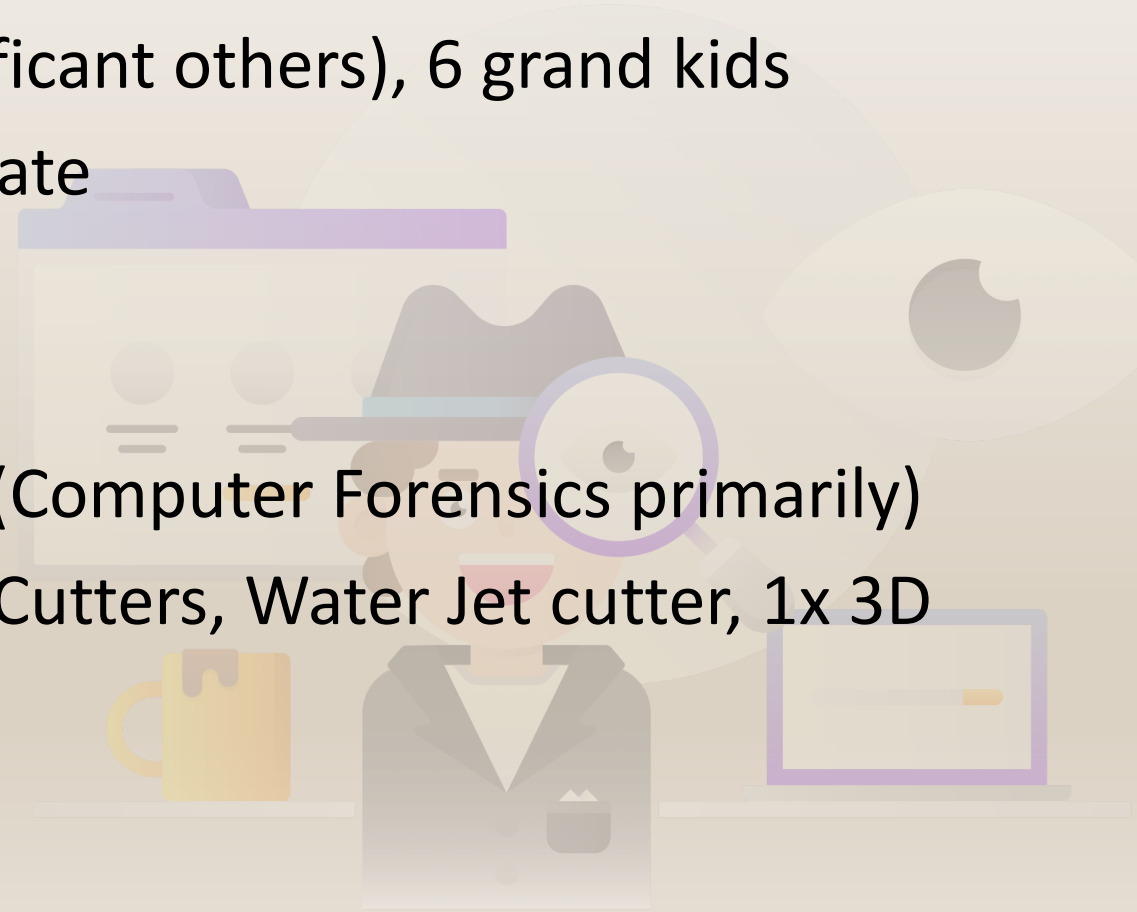
Cyber Threat Hunting in the Real World

Tim Crothers

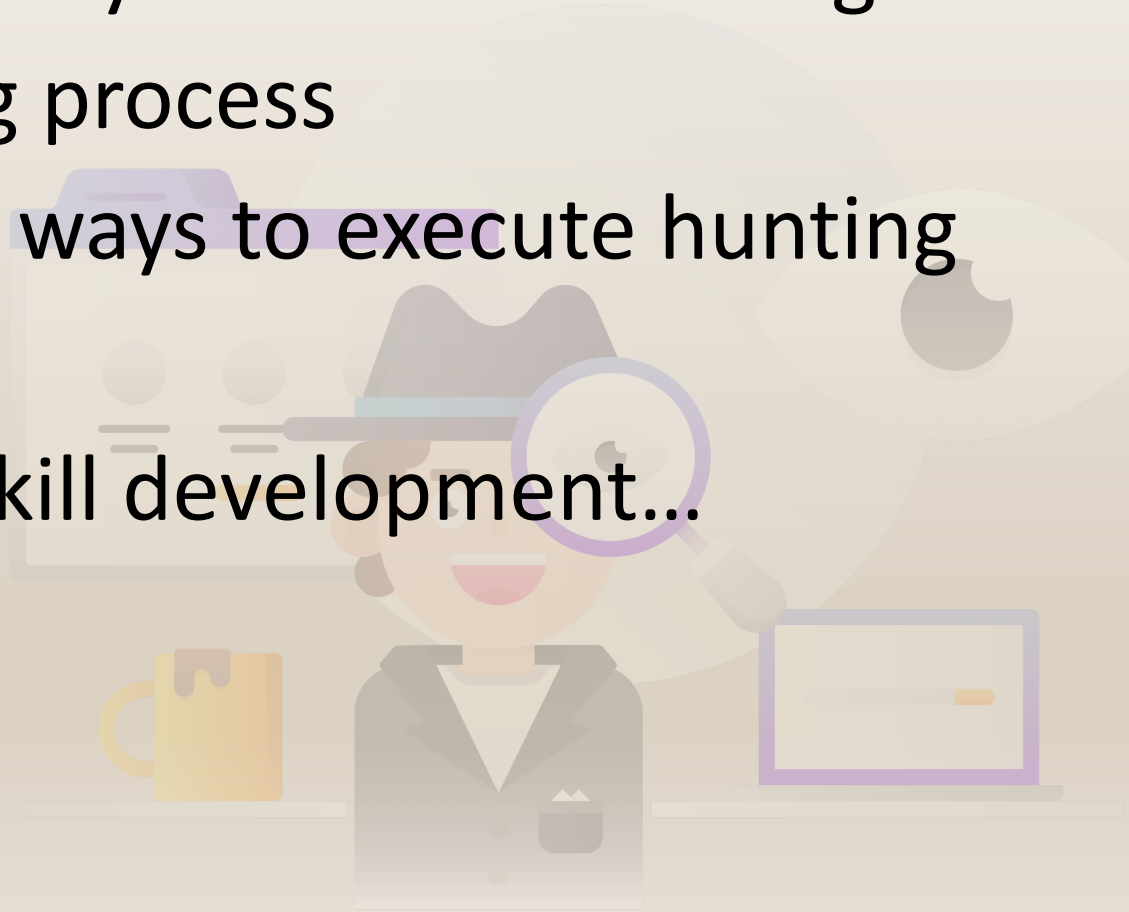
Who am I?

- 25 years in “InfoSec” / 37 years in “IT”
- Wife of 33 years, 3 kids (& their significant others), 6 grand kids
- Authored/co-authored 17 books to date
- Worked in 38 countries to date
- Technical and Rescue Diver
- Spent 5½ years as a Sheriff’s Deputy (Computer Forensics primarily)
- Fabrication lab with 3 CNC’s, 4 Laser Cutters, Water Jet cutter, 1x 3D printers, Lathe, etc., etc.



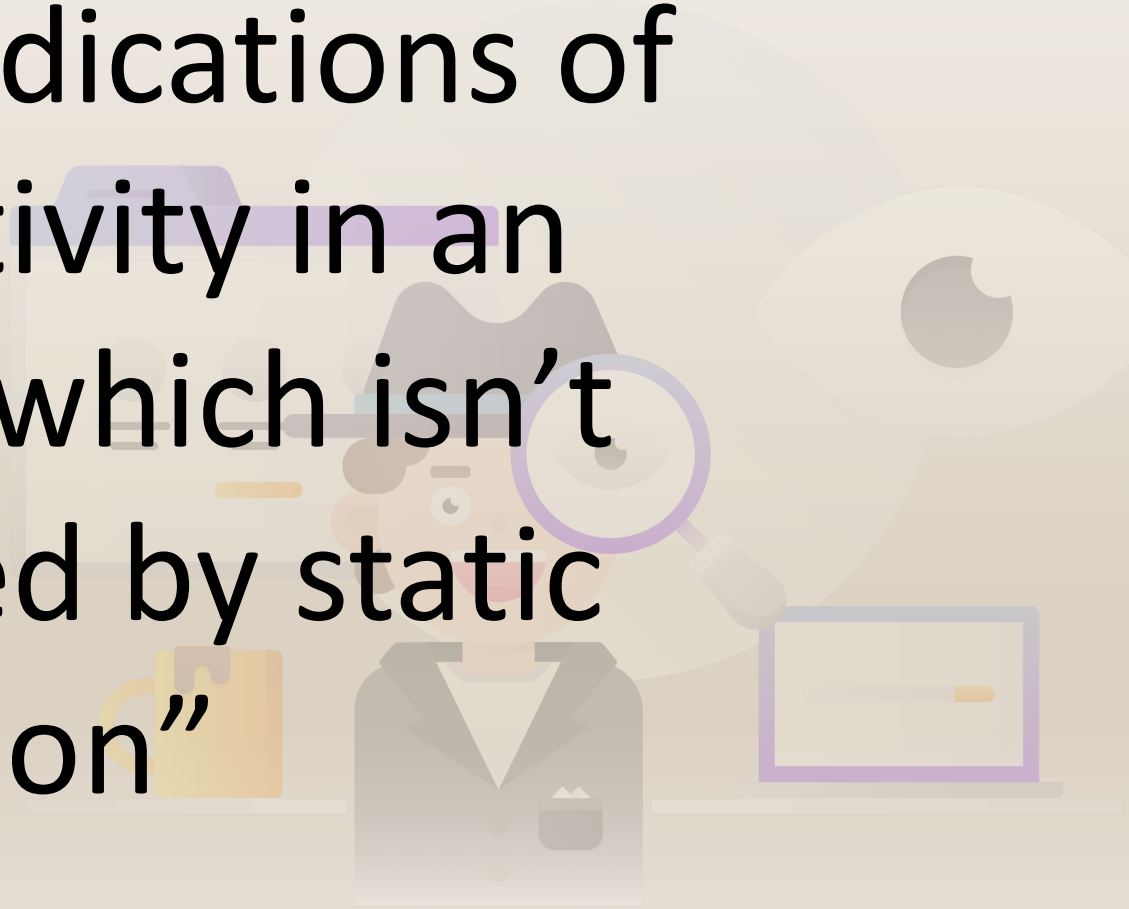
Objectives

- Have a solid understanding of Cyber Threat Hunting
- Understanding of the hunting process
- Demonstrate some tools and ways to execute hunting
- Practice
- Resources to continue your skill development…



Definition

"Looking for indications of malicious activity in an environment which isn't being detected by static detection"

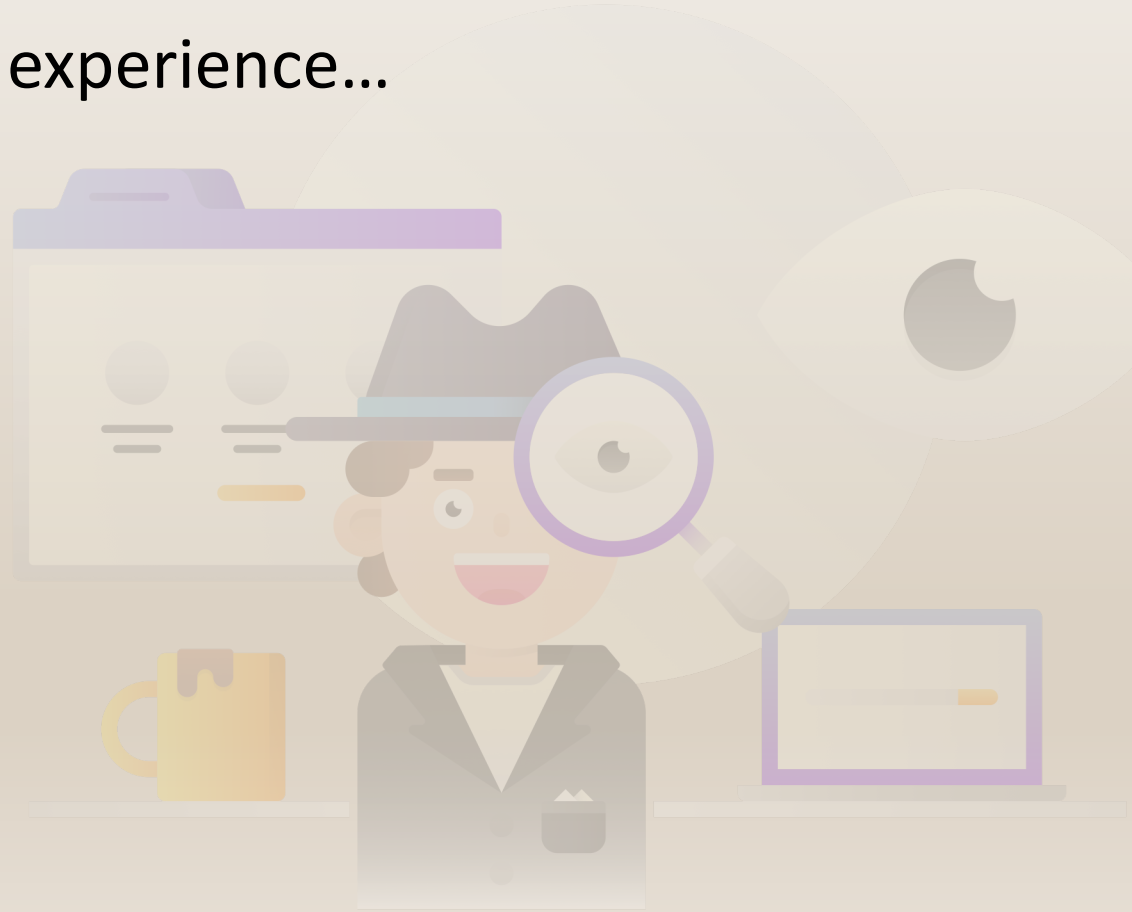


Benefits

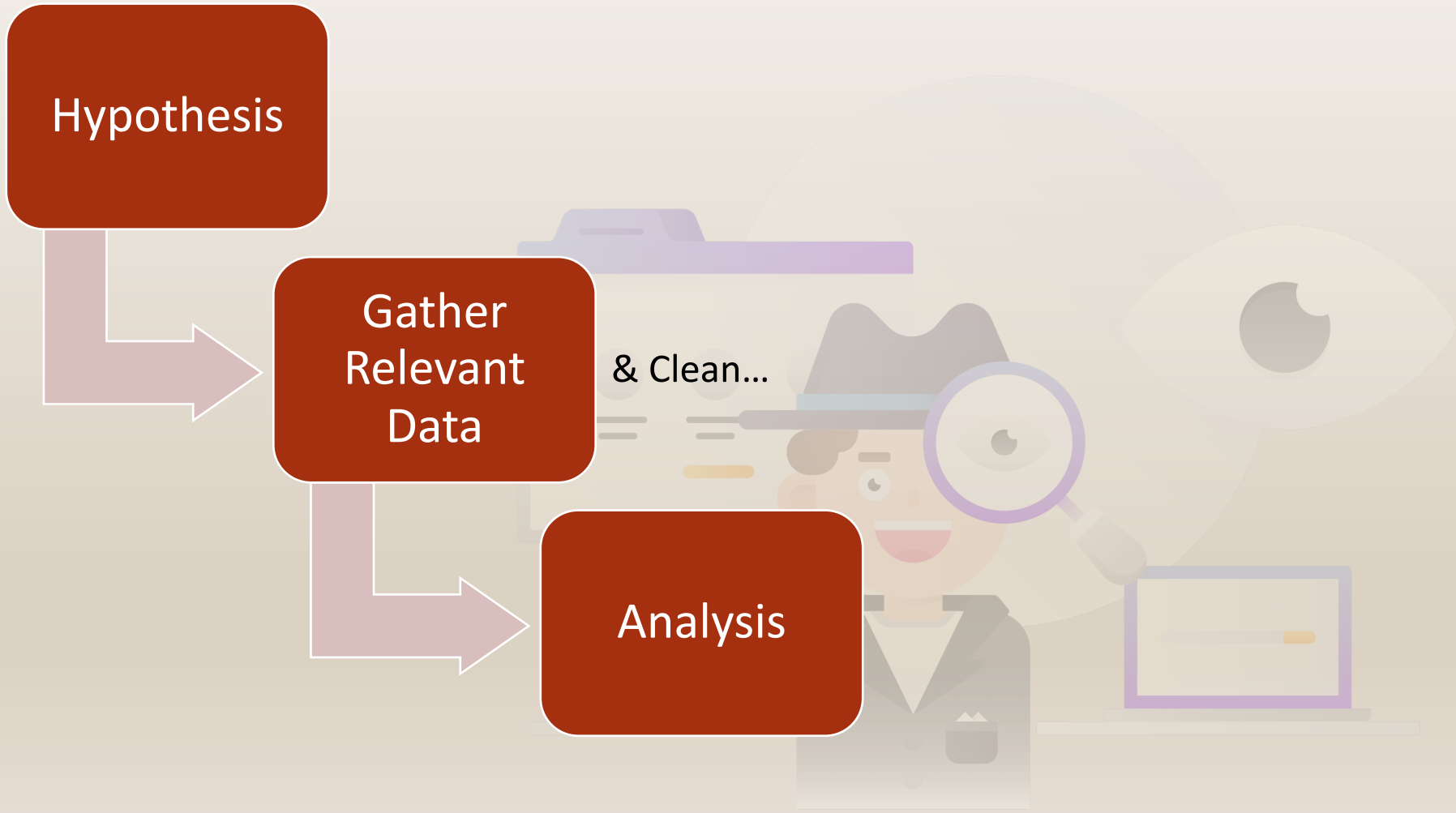
- Finding unknown malicious activity…
- Increased understanding of the environment…
- Develop skills for finding interesting anomalies in the environment…
- Improve your static detection…

Caveats

- A **LOT** of work…
- Slow going until you have a fair bit of experience…
- Manual effort…



Process of Hunting



Adversarial Understanding

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory					Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent		Hidden Window						
	Source			HISTCONTROL						
	Space after Filename			Image File Execution Options Injection						

WARNING!!!!!

Brad Duncan
@Malware_Traffic
Palo Alto Unit42 Threat Research Team
https://unit42.paloaltonetworks.com/

Convert pcaps

zeek –r file.pcap local

@load frameworks/files/extract-all-files

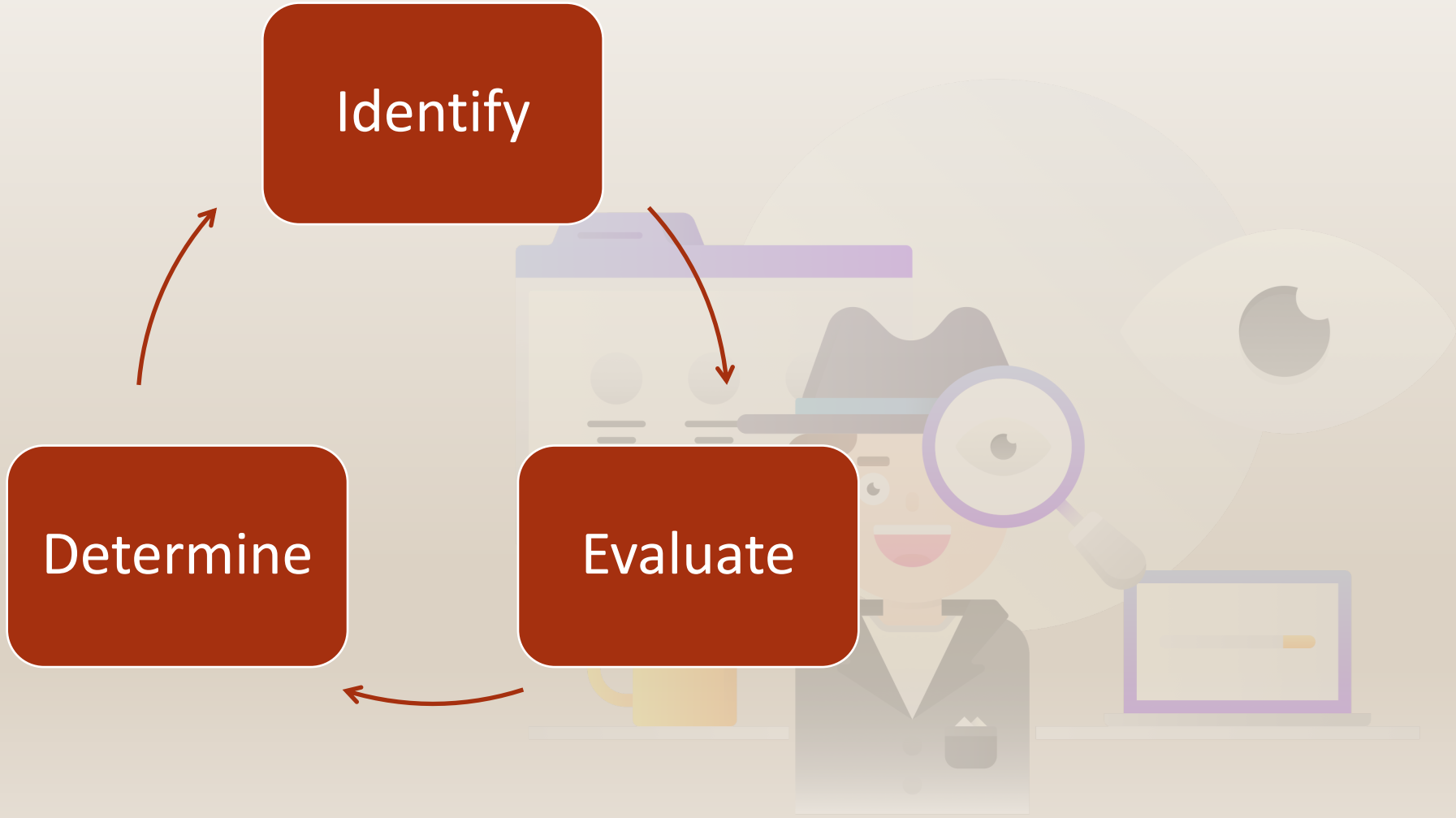
@load policy/tuning/json-logs.zeek

Patterns and Nuances

- Domains
- IPs
- Hashes

- Content anomalies
- Timing irregularities
- Size irregularities

Analysis



Gather and Clean

https://github.com/Soinull/assimilate/blob/master/pcap_to_bro.sh

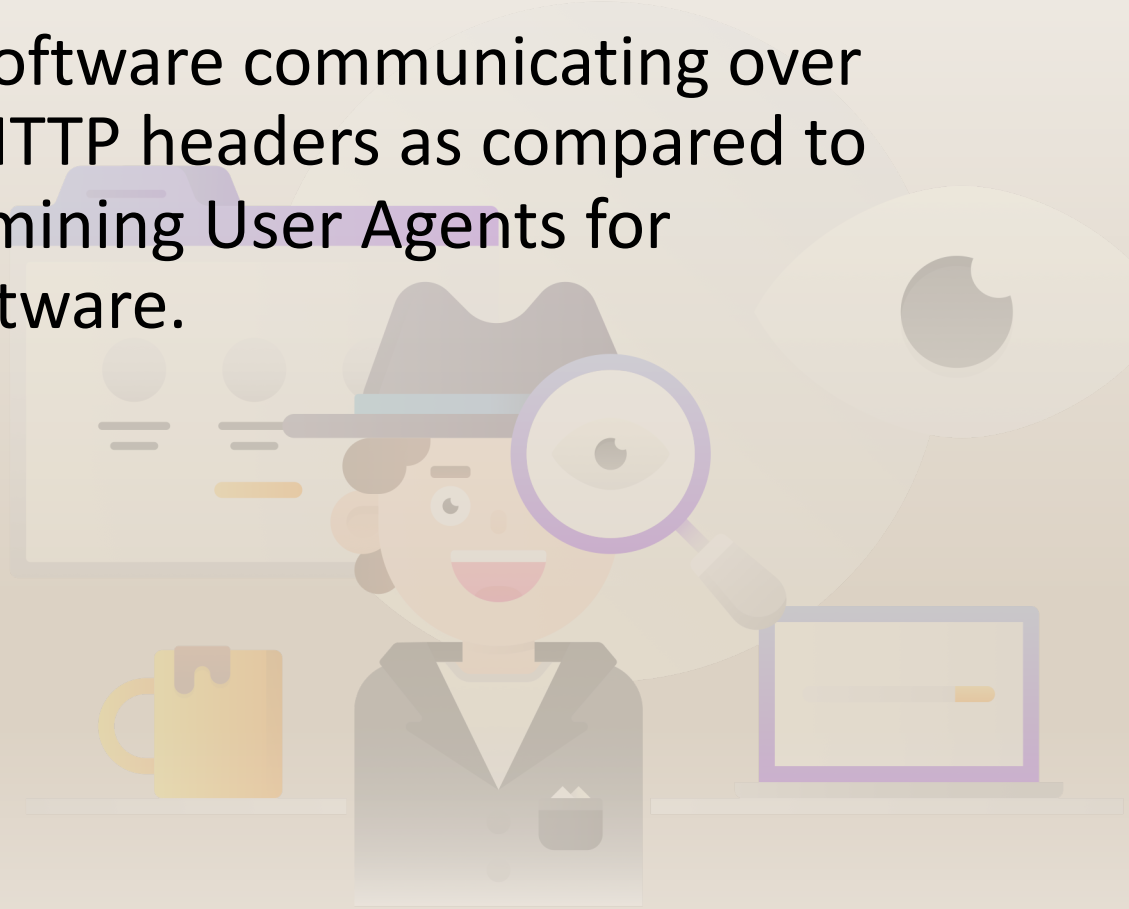
Example 1

Hypothesis:

Malware masquerading as legitimate software communicating over HTTP will have small anomalies in it's HTTP headers as compared to normal legitimate HTTP traffic. By examining User Agents for anomalies we might spot malicious software.

Data:

HTTP headers with User Agents



Example 2

Hypothesis:

Malware likes to hide in operating systems by mimicking legitimate names slightly misspelled

Data:

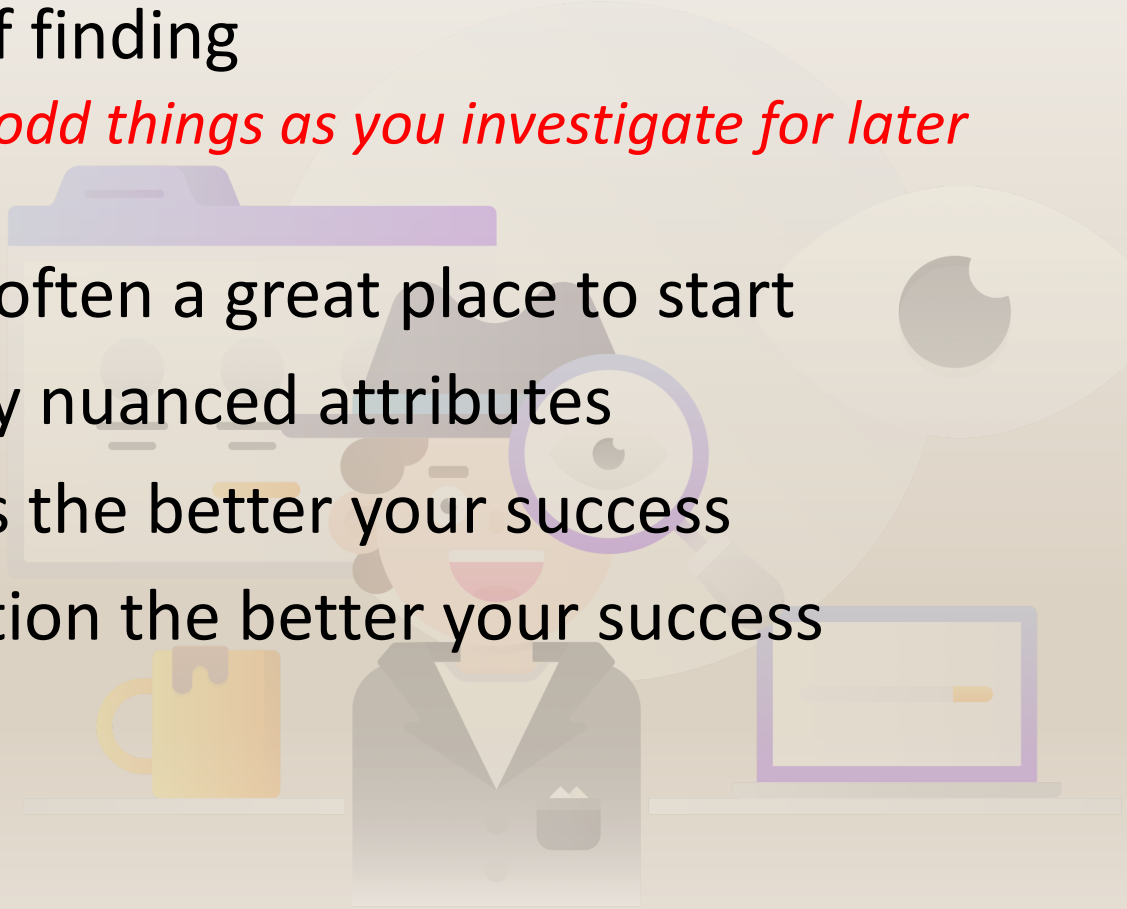
Host process names with execution and running paths

“Tricks” to Success

- The deeper your understanding of adversaries and their tools the better your hypothesis & likelihood of finding

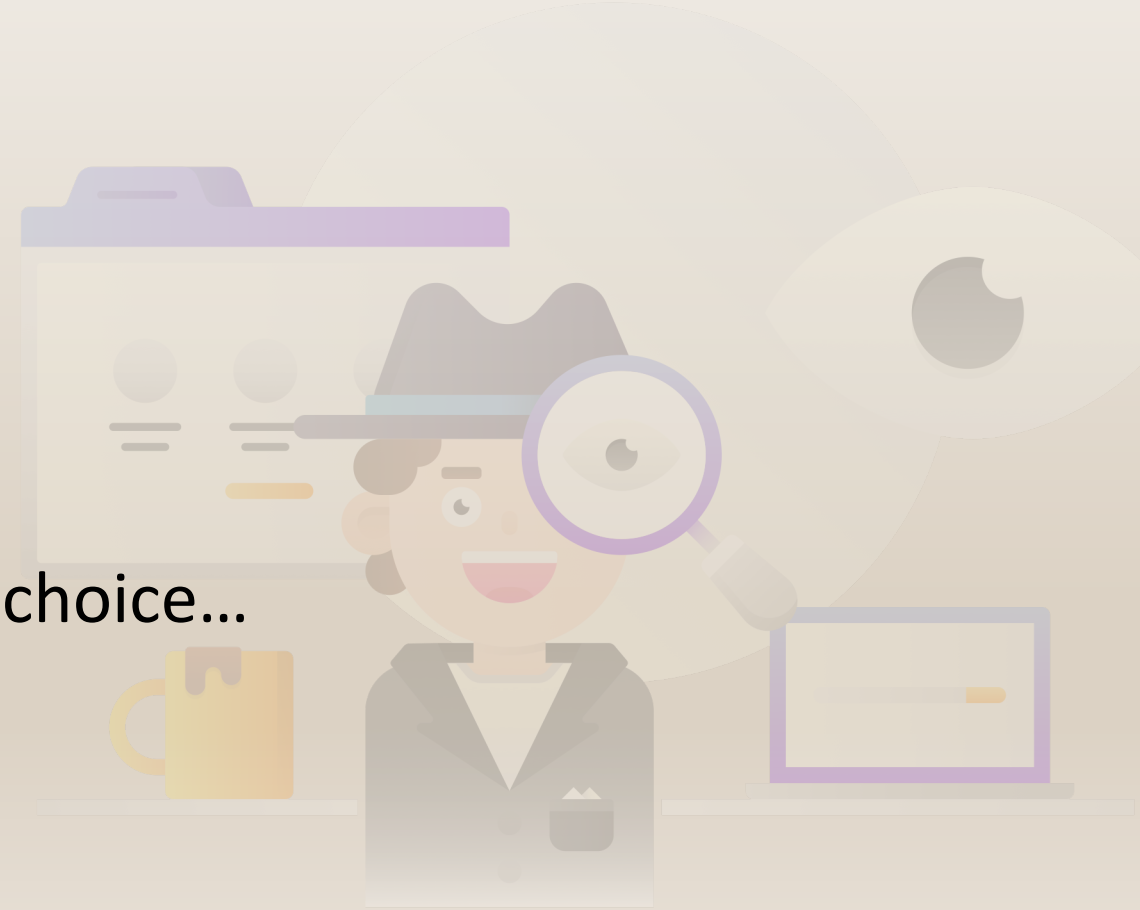
  Pro Tip – Keep a “hunting log” to capture odd things as you investigate for later hunting on…

- Analyzing what you are looking for is often a great place to start
- The best results often come from very nuanced attributes
- The better your skills at data analytics the better your success
- The better your skills at data preparation the better your success
- There are no ”unsuccessful” hunts



Useful tools

- Excel
- Great text editor
- Grep
- Python
- Jupyter notebook
- Bro/Zeek
- Elastic/Splunk/Big data repository of choice…



Hunt!

Resources

Hunt idea sources:

- Threat Hunting Project - https://www.threathunting.net/ ← START HERE!
- MITRE ATT&CK Framework - https://attack.mitre.org/
- David Bianco @DavidJBianco

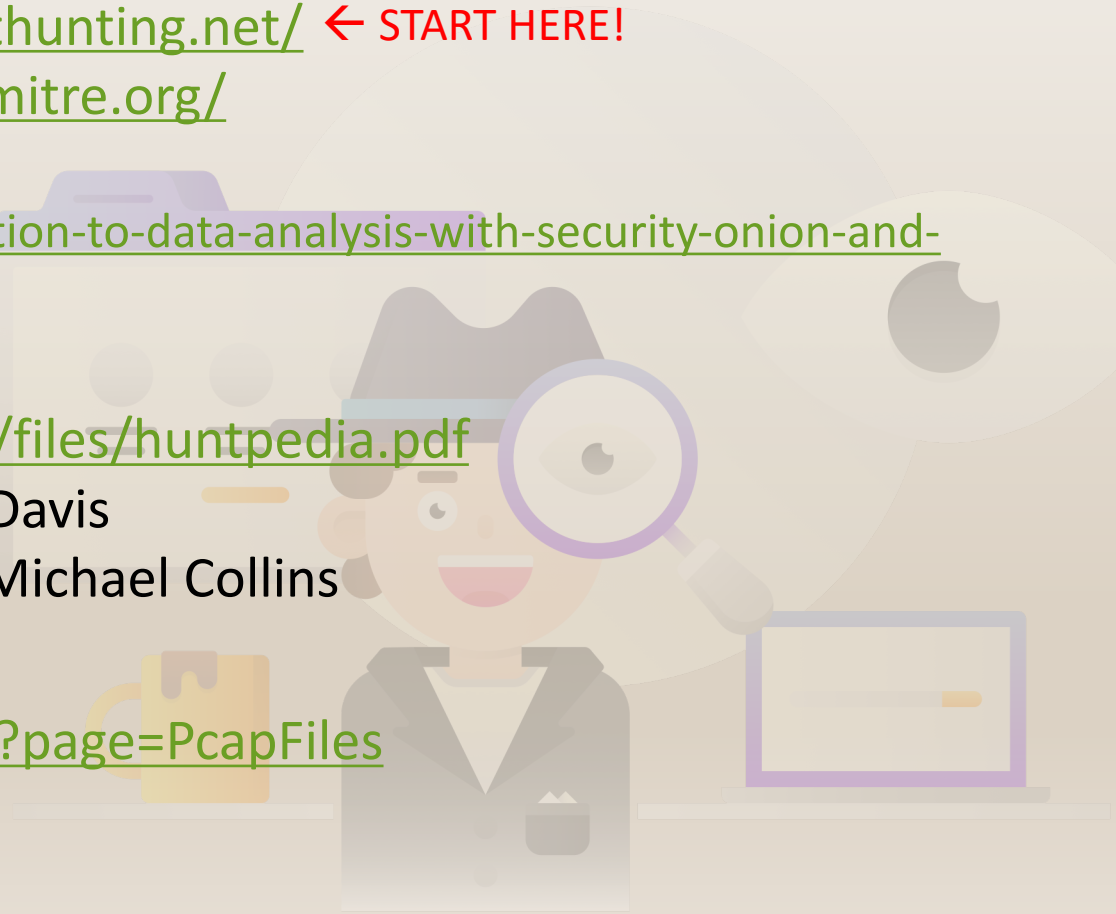
  https://speakerdeck.com/davidjbianco/introduction-to-data-analysis-with-security-onion-and-other-open-source-tools

Books:

- Huntpedia - https://www.threathunting.net/files/huntpedia.pdf
- Data Driven Security by Jay Jacobs and Rob Davis
- Network Security through Data Analysis by Michael Collins

Practice Data:

- Netresec.com - https://www.netresec.com/?page=PcapFiles



Thank You!

https://github.com/soinull/UM_Hunting_Class

linkedin.com/in/timcrothers