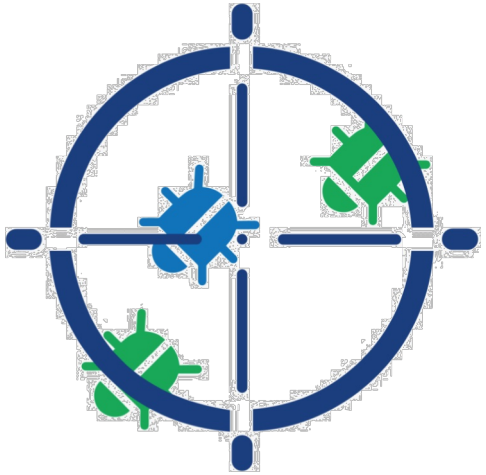
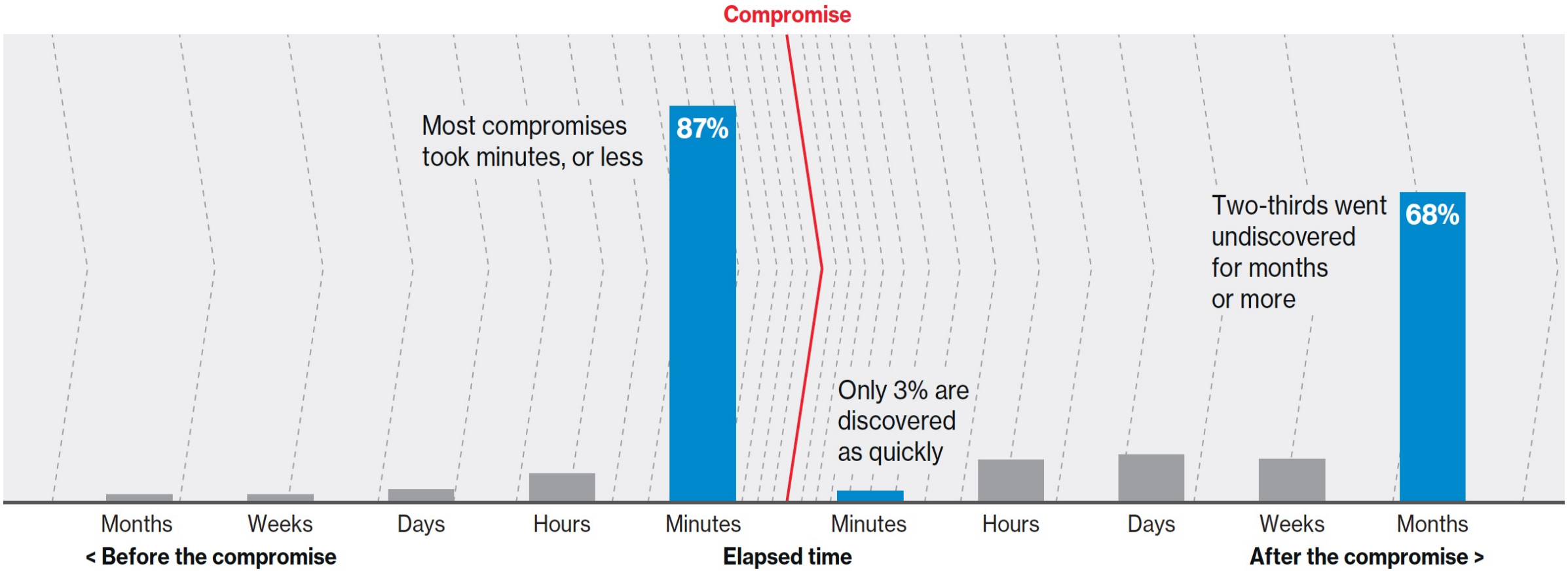


Hunting Threats In your Enterprise

- ✓ Who am I ?
  - ✓ Abdulrahman Al-Nimari
  - ✓ 25 Years IT & Infosec Experience
  - ✓ Lead Enterprise Security Architect
  - ✓ Mantech International Corporation, Riyadh, KSA
  - ✓ CISSP, CISM, CCISO, PMP, GCIH, GCIA, GCUX, GREM, GSEC
  - ✓ @nimari
  - ✓ https://www.linkedin.com/in/alnimari/
  - ✓ alnimari@gmail.com

- ✓ Agenda
  - ✓ What is Threat Hunting ?
  - ✓ Threat Hunting Plan
  - ✓ Hunt Cycle
  - ✓ Hunting in Action
  - ✓ Hunt Maturity Level
  - ✓ Measuring Success (Metrics)
  - ✓ Resources

Verizon Data Breach Investigations Report, 2018



https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

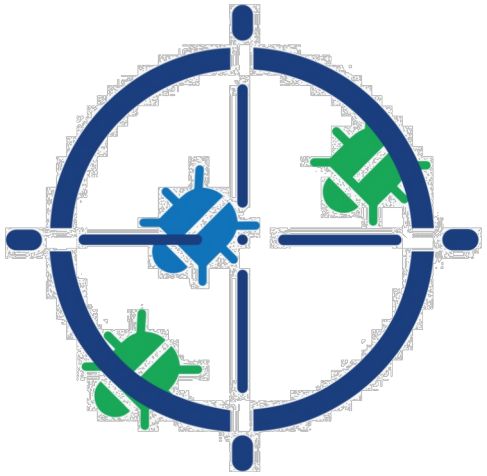
✓ What is threat hunting ?

- ✓ **Cyber threat hunting** is "the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions"

  (Wikipedia)

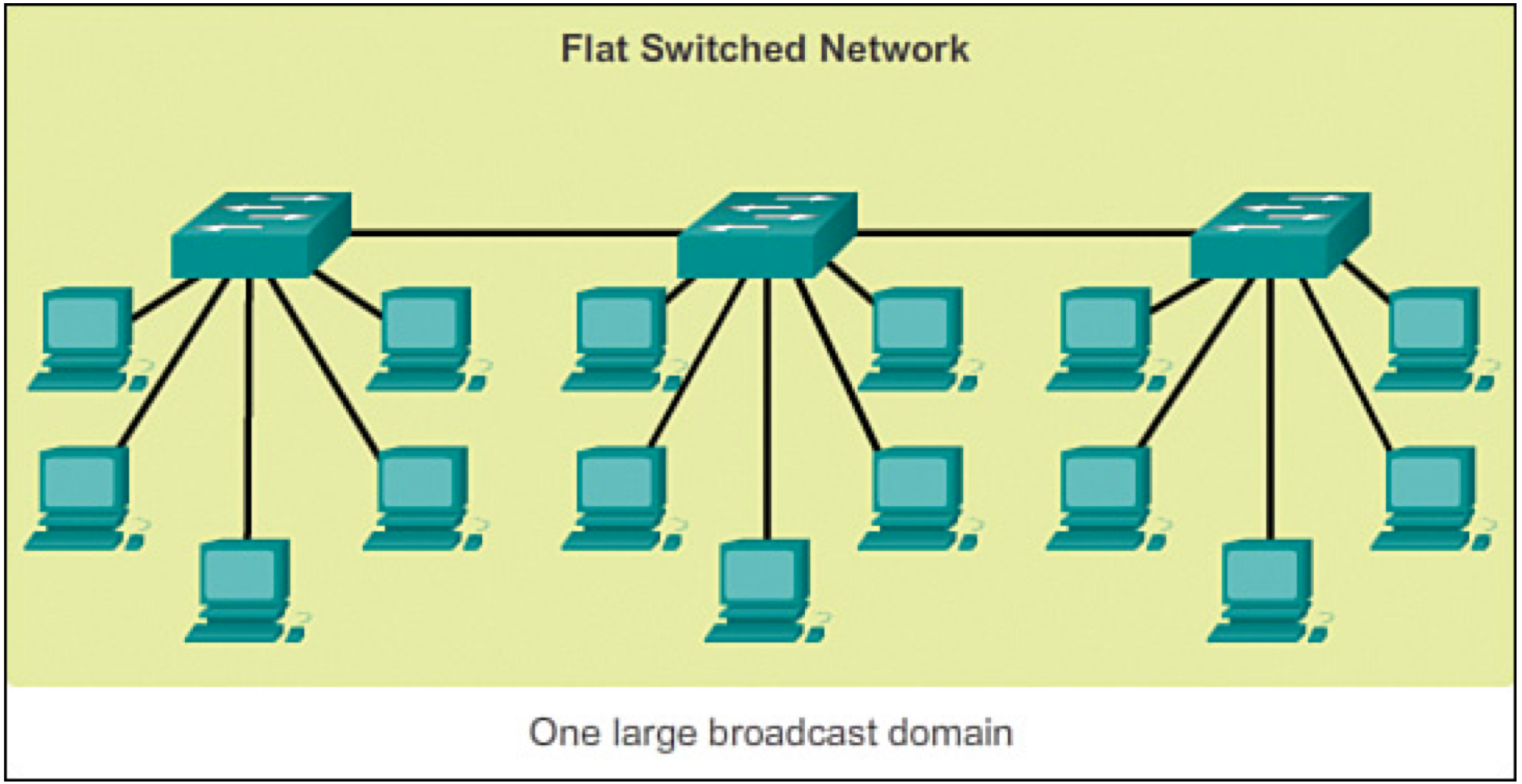
- ✓ **Cyber threat hunting** is “the practice of searching iteratively through data to detect advanced threats that evade traditional security solutions”

  (sqrrl)

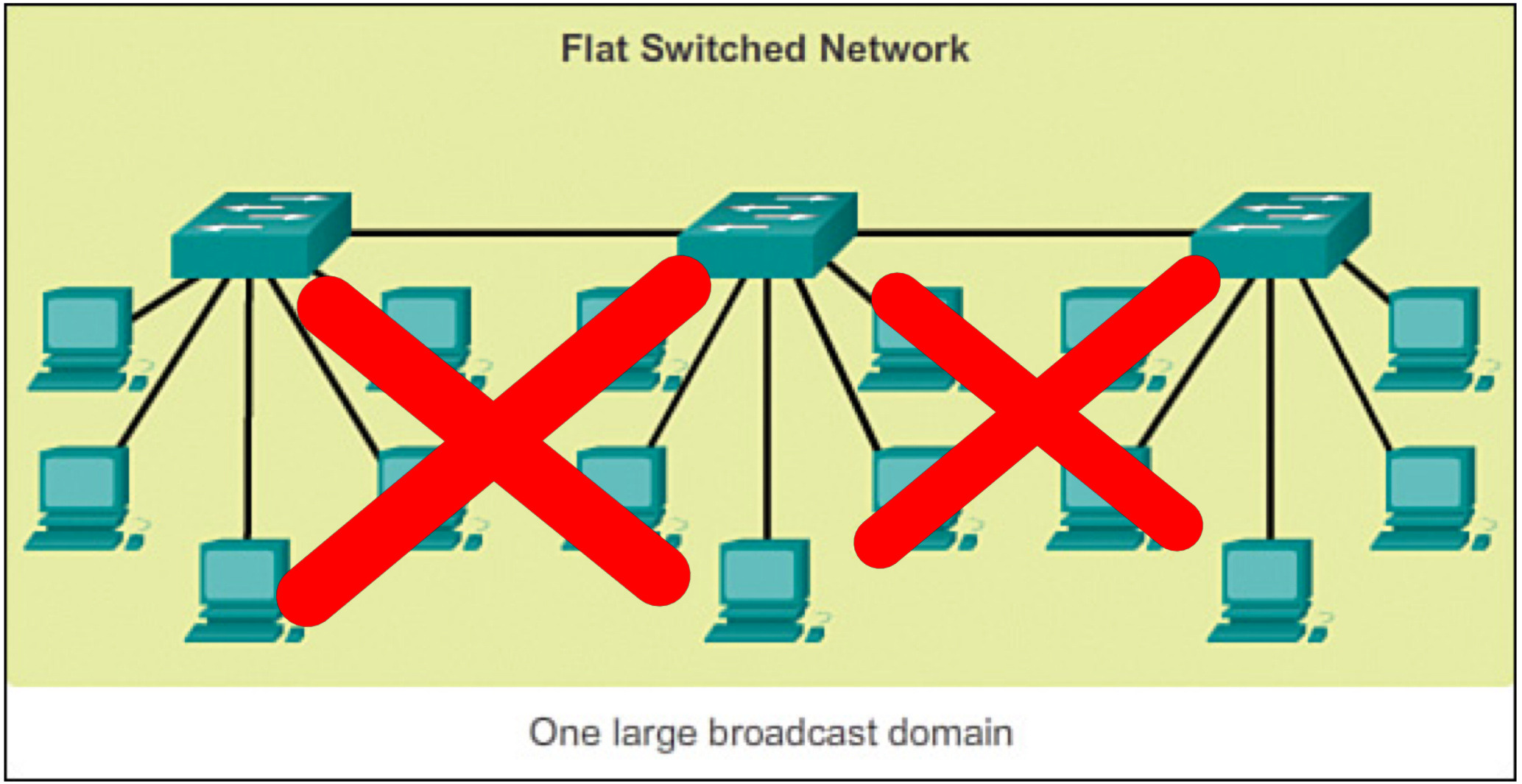


- ✓ Threat Hunting Plan
  - ✓ Design Your Network For Hunting
  - ✓ Get your Team Ready
  - ✓ Know your Enterprise
  - ✓ Know Your Adversary TTP
  - ✓ Collect Hunt Data
  - ✓ Create Hypotheses
  - ✓ Start Hunting

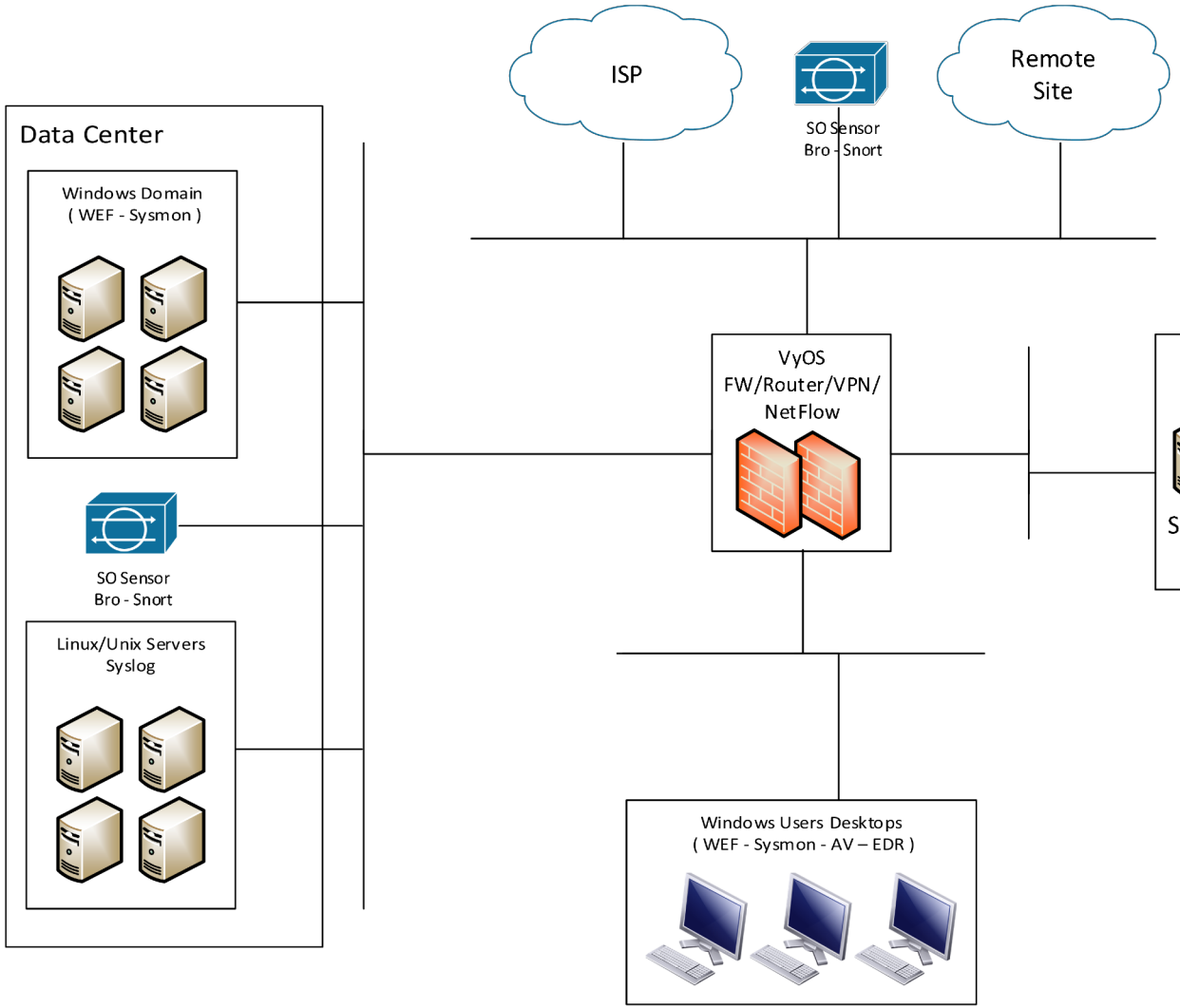
Design Your Enterprise for Hunting



Design Your Enterprise for Hunting



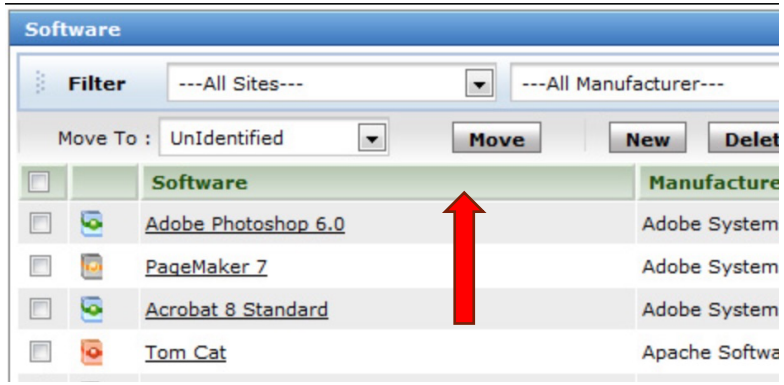
Design Your Enterprise for Hunting

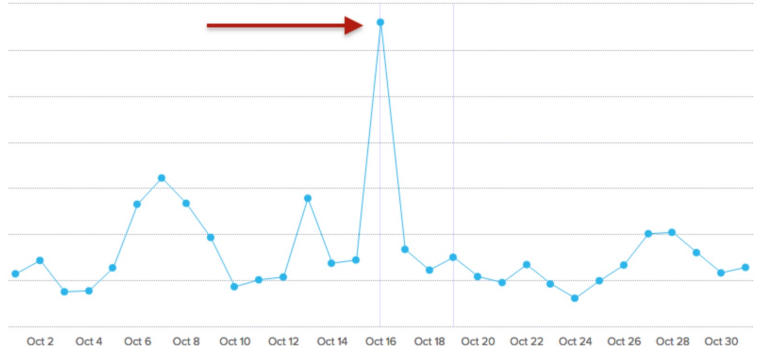


- ✓ Segmentation : Security Zones
- ✓ NTP : Network Time Protocol
- ✓ Protection/Detection : FW/IDS/IPS/DLP/Proxy
- ✓ Tapping : Dump PCAP Data
- ✓ Visibility : Enable Logging as required

✓ Know Your Enterprise

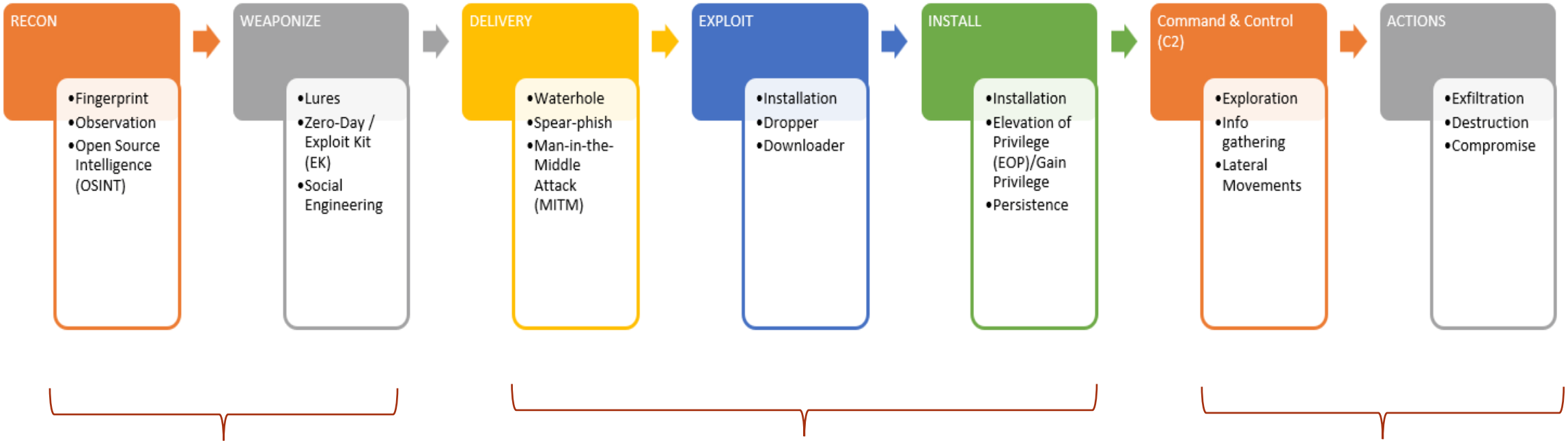
- ✓ Identify Assets
- ✓ Know Threats to Your Assets
- ✓ Prioritize (High Value / Critical Assets First)
- ✓ Baselining – Know what is normal ?





Know Your Adversary - Cyber Kill Chain

A cyber kill chain is a ‘Lockheed Martin’ model that reveals the stages of a cyber attack from early reconnaissance to the goal of data exfiltration :



https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Know Your Adversary – Mitre ATT&CK

ATT&CK = Adversarial Tactics, Techniques, and Common Knowledge

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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	BITS Jobs	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	Binary Padding	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 Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	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 Network Shared Drive	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 from Removable Media	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-Stage Channels

Collect Hunt Data

Data Domains :

Network	Host	Application
- Flow Data - NetFlow - PCAP - DNS - Proxy Logs - FW/SW/Routers	- AV/EDR/FW - Windows/Sysmon Events - File System - Autoruns	- Authentication - Transaction Logs - DB Logs - Security Alerts

- ✓ Log Data
- ✓ PCAP Data
- ✓ Netflow
- ✓ Threat Intelligence Data

- ✓ Threat Intelligence Feeds （Open Source）
  - ✓ https://otx.alienvault.com/
  - ✓ https://www.iocbucket.com/
  - ✓ https://abuse.ch/
  - ✓ https://www.blocklist.de/
  - ✓ https://www.virustotal.com/
  - ✓ https://malwr.com/
  - ✓ ……

Creating Hypothesis

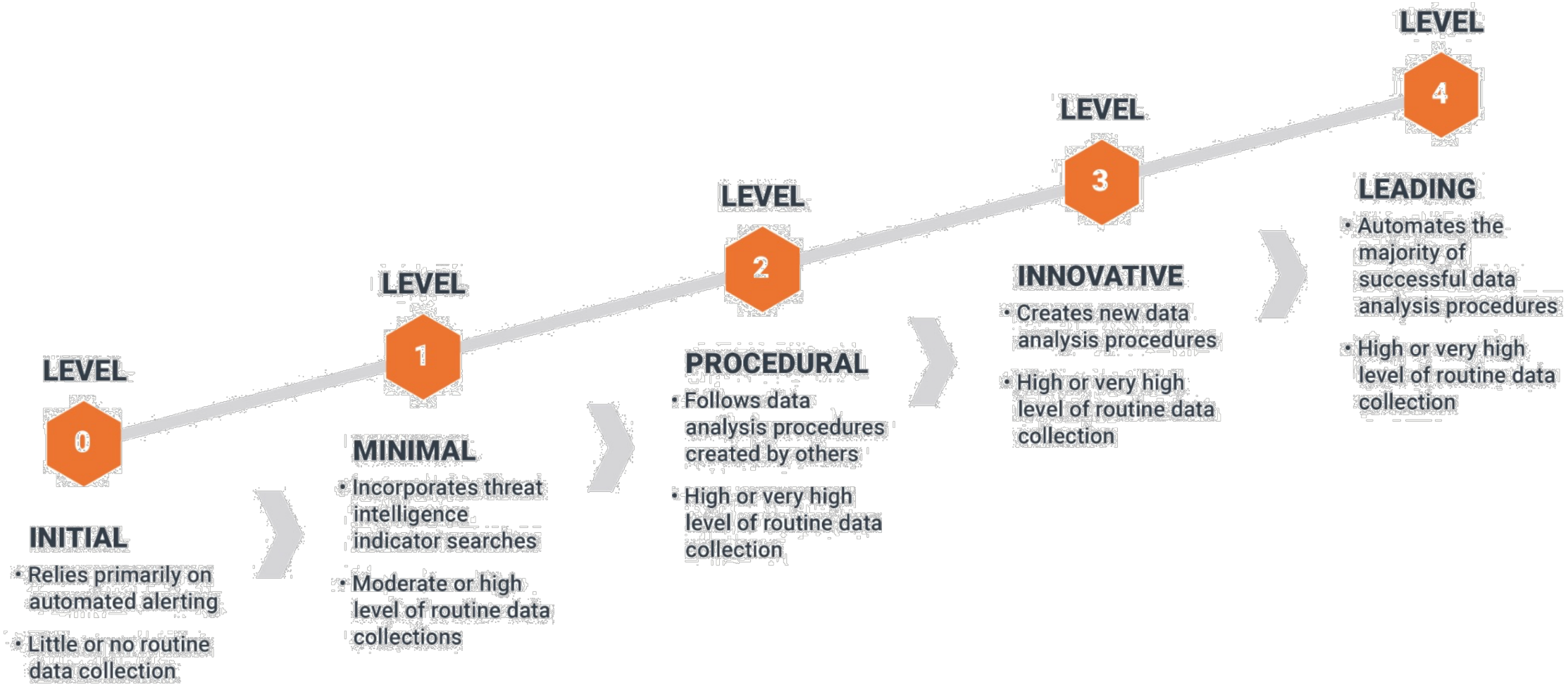
Hypotheses	Data (Where to Hunt)	What to look for ?
Data Staging/Exfiltration ?	PCAPS, NetFlow	Compressed Files
Lateral Movement ?	PCAPS, Logs	PSEXEC, Powershell
Fileless Malware ?	PCAPS, NetFlow	Powershell, WMI
Command & Control (C2) ?	HTTP, Bro Logs	MaliciousURLs/Domains/User agent/DNS
.....		

Hunting Cycle

Iterate aggressively through this cycle

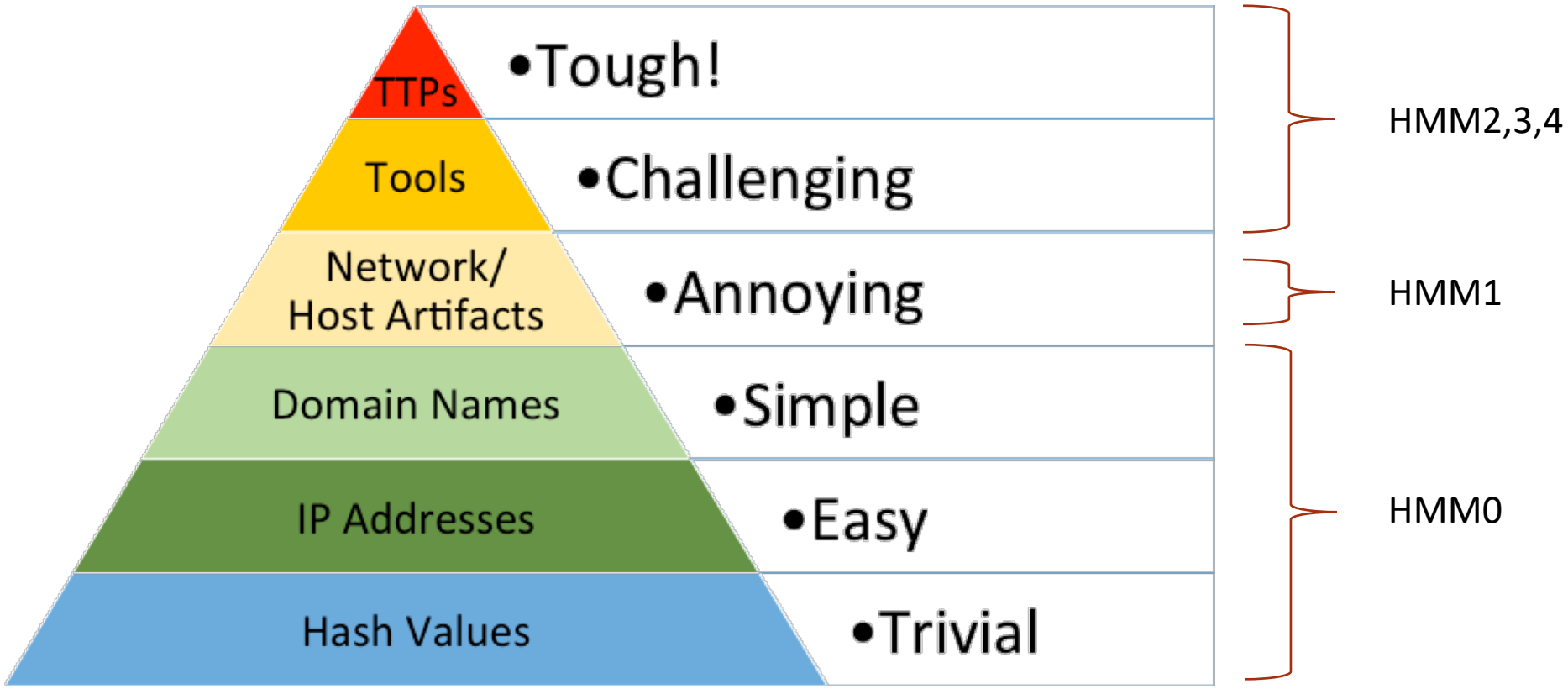
https://sqrrl.com/the-threat-hunting-reference-model-part-2-the-hunting-loop/

Hunting Maturity Model



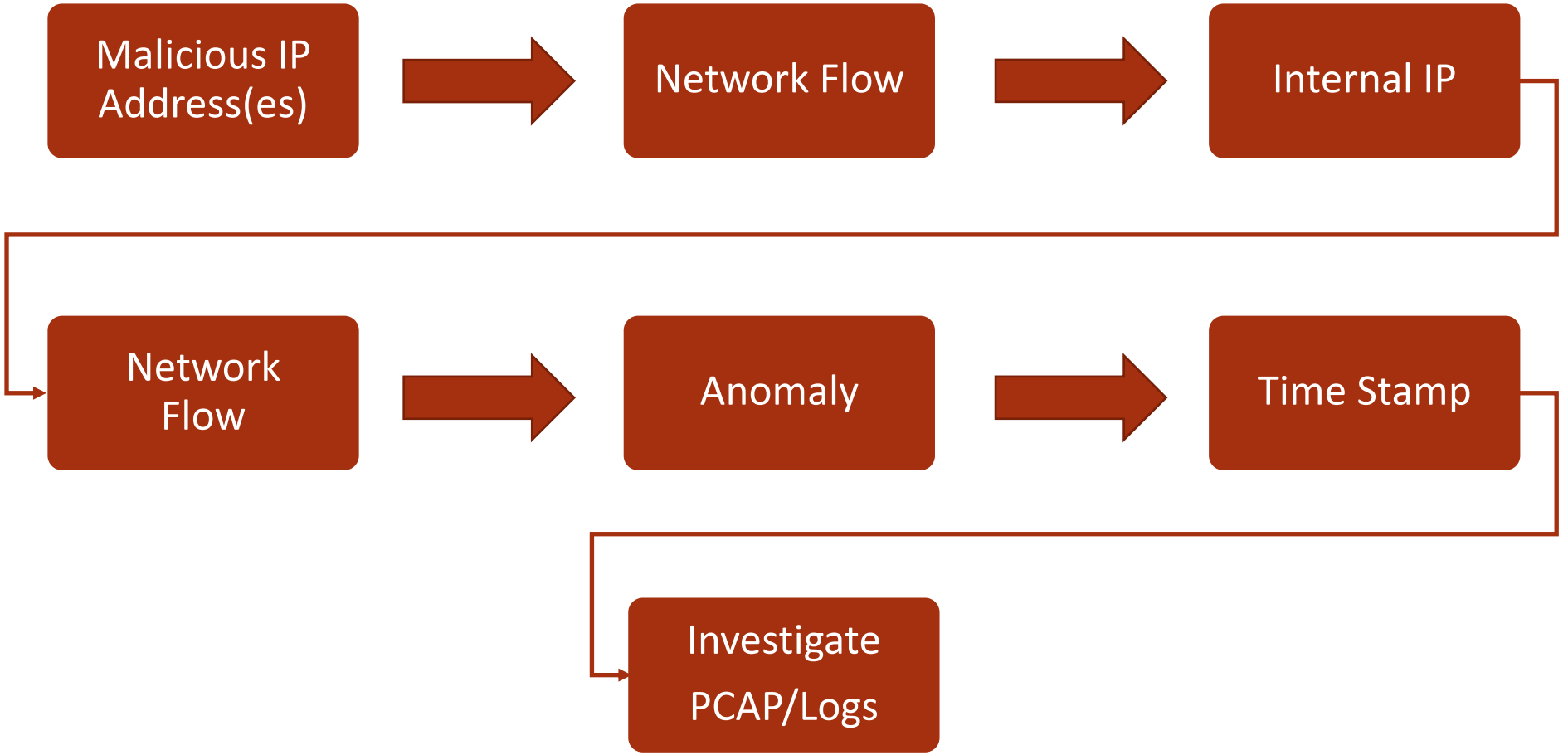
https://sqrrl.com/the-threat-hunting-reference-model-part-1-measuring-hunting-maturity/

Pyramid of Pain

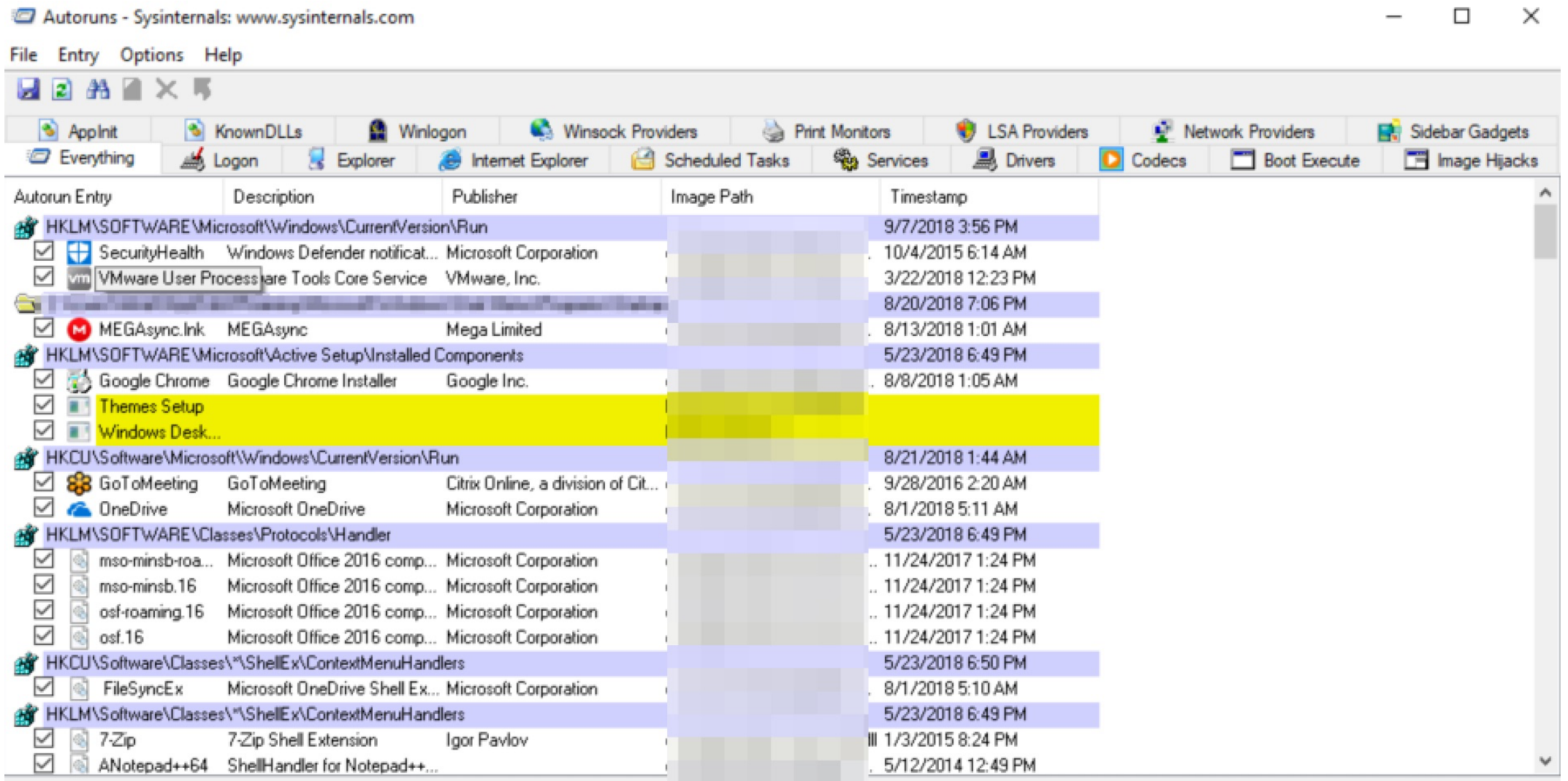


http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

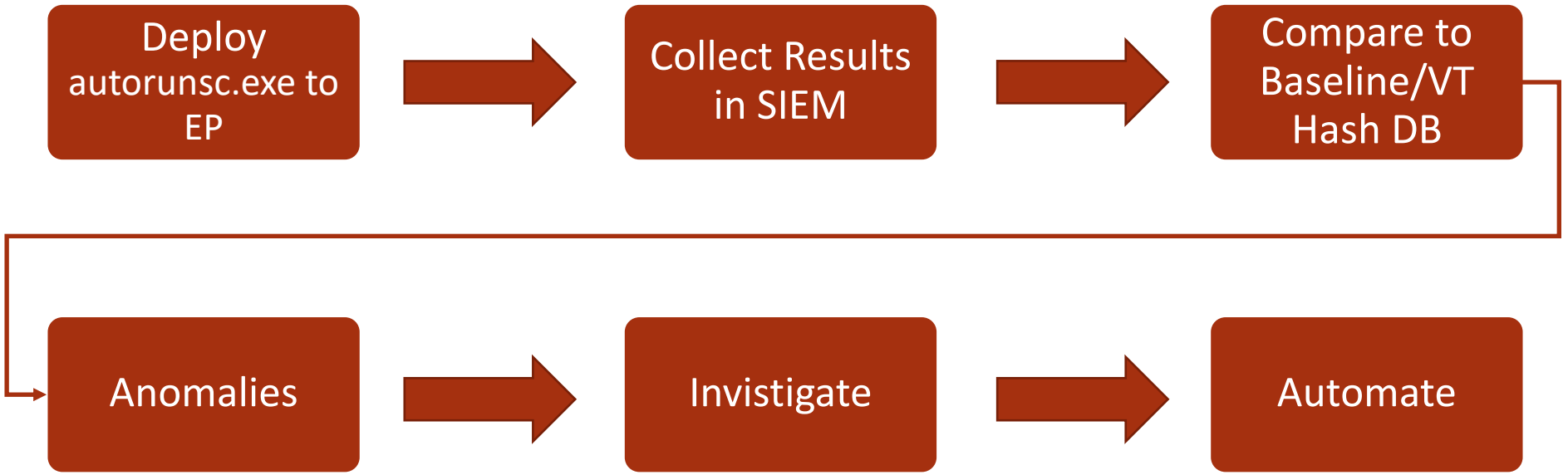
Hunting in Action #1



Hunting in Action #2



Hunting in Action #2



✓ Measuring Success (Metrics)

- ✓ Number of Incidents by severity
- ✓ Number of Compromised Hosts
- ✓ Dwell Time of Incidents Discovered.
- ✓ Logging Gaps Identified and Corrected
- ✓ Vulnerabilities Identified
- ✓ Insecure Practices Identified and Corrected
- ✓ Hunts Transitioned to Analytics
- ✓ New Visibilities Gained

https://sqrrl.com/media/Your-Practical-Guide-to-Threat-Hunting.pdf

- ✓ Resources
  - ✓ https://www.threathunting.net/
  - ✓ https://threathunting.org/
  - ✓ https://intel.criticalstack.com/
  - ✓ https://www.mitre.org/
  - ✓ https://www.elastic.co/
  - ✓ https://github.com/Cyb3rWard0g/ThreatHunter-Playbook
  - ✓ https://nxlog.co/
  - ✓ https://docs.microsoft.com/en-us/sysinternals/

Q & A

Thank You