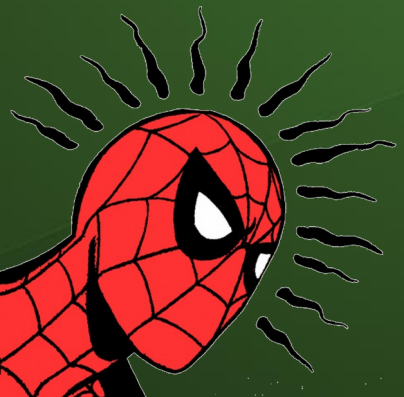
My Cyber Sense Is Tingling!
Detection Engineering With Free Tools



Matthew Gracie
BlueTeamCon
2025

Who Am I And What Am I Talking About?

What Is Cyber Threat Intelligence?

”Threat intelligence refers to the collection, processing, and analysis of data to understand a threat actor’s motives, targets, and attack methods. It transforms raw data into actionable insights, enabling security teams to make informed, data-driven decisions. This shifts organizations from a reactive to a proactive stance in defending against cyber threats.”

Crowdstrike*

source: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/

What Is Cyber Threat Intelligence?

”Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.”

Gartner*

source: https://www.gartner.com/en/documents/2487216

Where Do We Get Threat Intelligence?

Vendor Threat Intelligence

MITRE ATT&CK

Home > Groups > Scattered Spider

Scattered Spider

Scattered Spider is a native English-speaking cybercriminal group that has been active since at least 2022.[1][2] The group initially targeted customer relationship management and business-process outsourcing (BPO) firms as well as telecommunications and technology companies. Beginning in 2023, Scattered Spider expanded its operations to compromise victims in the gaming, hospitality, retail, MSP, manufacturing, and financial sectors.[2] During campaigns, Scattered Spider has leveraged targeted social-engineering techniques, attempted to bypass popular endpoint security tools, and more recently, deployed ransomware for financial gain.[3][4][1][2][5]

ID: G1015
Associated Groups: Roasted 0ktapus, Octo Tempest, Storm-0875
Version: 2.0
Created: 05 July 2023
Last Modified: 04 April 2024

Version Permalink

Associated Group Descriptions

Name	Description
Roasted 0ktapus	[4]
Octo Tempest	[6]
Storm-0875	[6]

Campaigns

ID	Name	First Seen	Last Seen	References	Techniques
C0027	C0027	June 2022 [5]	December 2022 [5]	[5]	Account Discovery: Cloud Account, Account Discovery: Email Account, Account Manipulation: Additional Cloud Roles, Account Manipulation: Device Registration, Account Manipulation: Additional Cloud Credentials, Data from Cloud Storage, Data from Information Repositories: Sharepoint, Exploit Public-Facing Application, External Remote Services, Gather Victim Identity Information: Credentials, Impersonation, Ingress Tool Transfer, Modify Cloud Compute Infrastructure: Create Cloud Instance, Multi-Factor Authentication Request Generation, Network Service Discovery, Obtain Capabilities: Tool, OS Credential Dumping: DCSync, Permission Groups Discovery: Cloud Groups, Phishing: Spearphishing Voice, Phishing for Information: Spearphishing Voice, Phishing for Information: Spearphishing Service, Protocol Tunneling, Proxy, Remote Access Tools, Remote Services: Cloud Services, Valid Accounts: Cloud Accounts, Web Service, Windows Management Instrumentation

Techniques Used

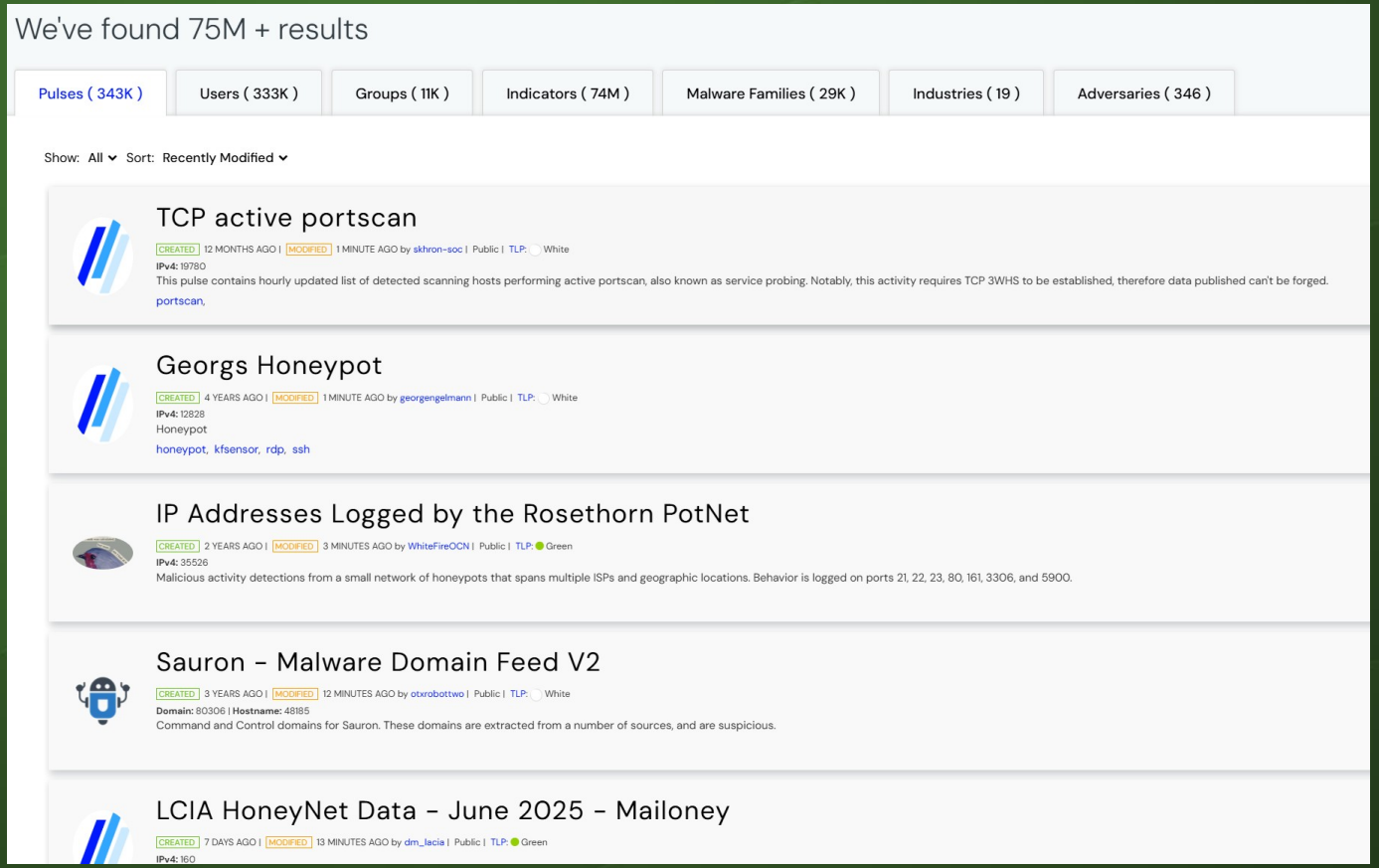
ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1087	.002	Account Discovery: Domain Account	Scattered Spider leverages legitimate domain accounts to gain access to the target environment.[3][2]
		.003	Account Discovery: Email Account	During C0027, Scattered Spider accessed Azure AD to identify email addresses.[5]
		.004	Account Discovery: Cloud Account	During C0027, Scattered Spider accessed Azure AD to download bulk lists of group members and to identify privileged users, along with the email addresses and AD

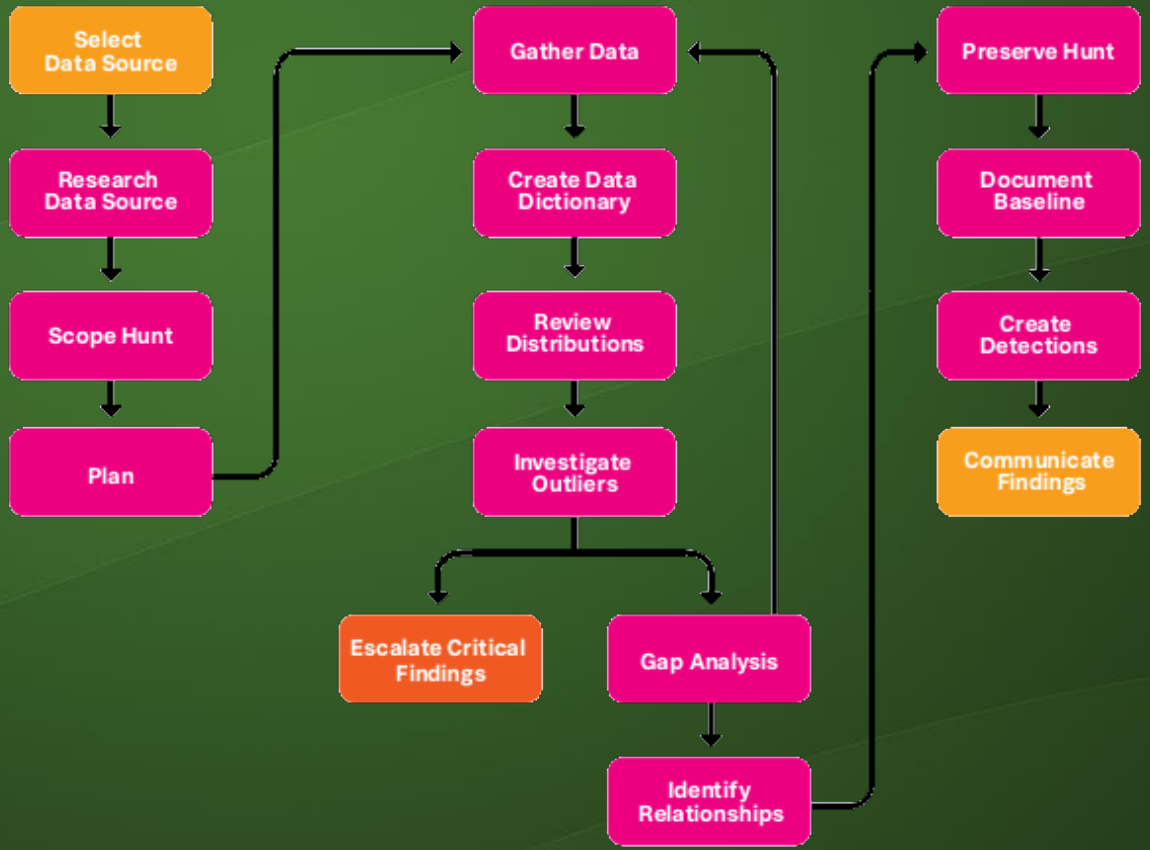
ISACs


national council of
ISACs
HOME
ABOUT NCI
ABOUT ISACS
MEMBER ISACS
REPORTS
NEWS
CONTACT
ISACs are member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators.
Sector-based Information Sharing and Analysis Centers collaborate with each other via the National Council of ISACs. Formed in 2003, the NCI today comprises 28 organizations. It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government. Critical infrastructure sectors and subsectors that do not have ISACs are invited to contact the NCI to learn how they can participate in NCI activities.
Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.
JOIN YOUR SECTOR'S ISAC TODAY

Community Threat Exchanges

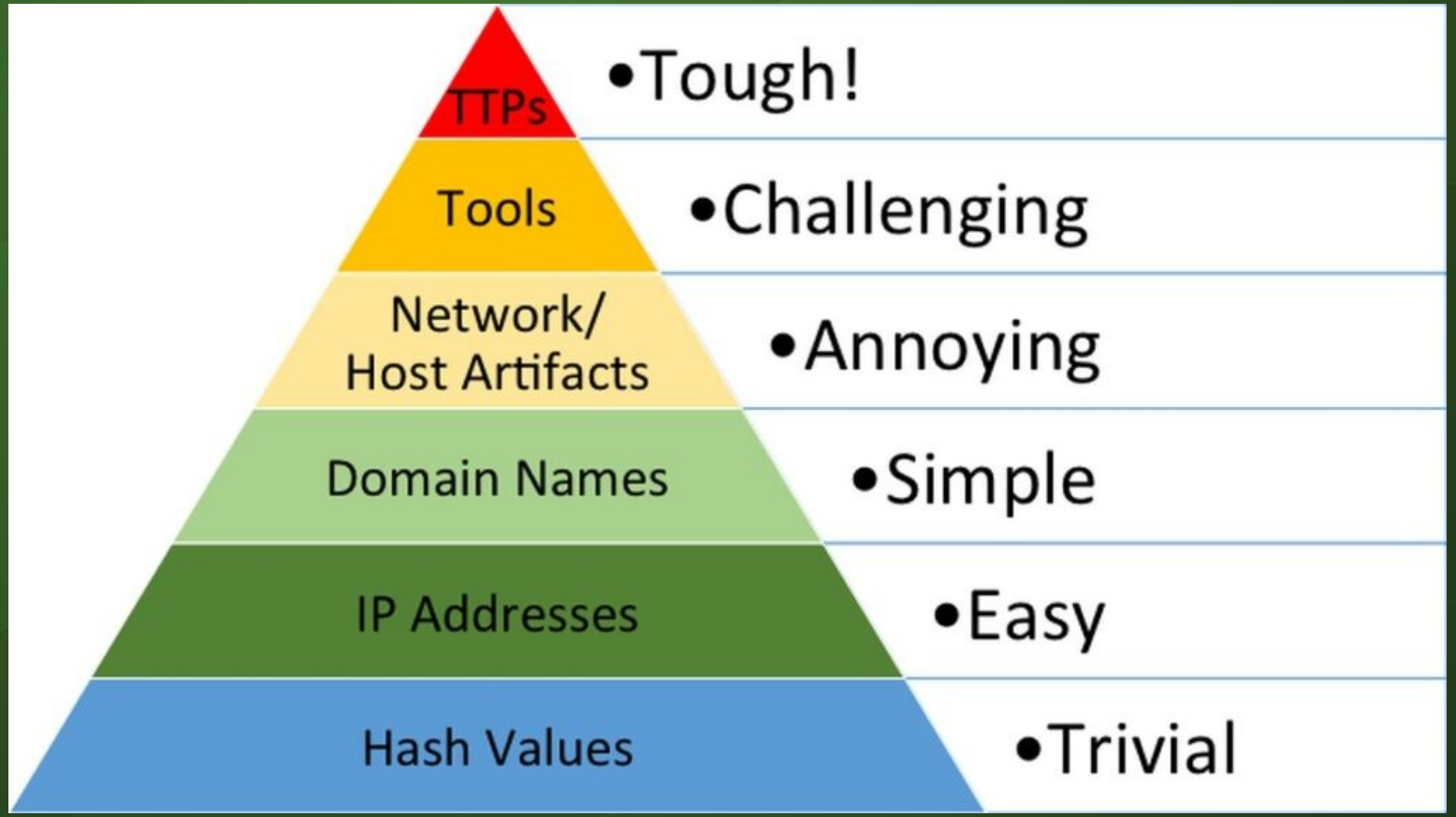


Roll Your Own



source: PEAK Threat Hunting Framework

The Pyramid Of Pain



How Do We Leverage Threat Intelligence?

Security Onion

”Security Onion is a free and open platform built by defenders for defenders. It includes network visibility, host visibility, intrusion detection honeypots, log management, and case management. Security Onion has been downloaded over 2 million times and is being used by security teams around the world to monitor and defend their enterprises.”

source: https://docs.securityonion.net/en/2.4/about.html

Security Onion

”Security Onion is a free and open platform built by defenders for defenders. It includes network visibility, host visibility, intrusion detection honeypots, log management, and case management. Security Onion has been downloaded over 2 million times and is being used by security teams around the world to monitor and defend their enterprises.”

source: https://docs.securityonion.net/en/2.4/about.html

Security Onion

network visibility

- Suricata IDS engine
- Zeek metadata generation and logging
- file carving

host visibility

- endpoint logs and telemetry from Windows, OS X, and Linux

log management

- network and cloud service logs

Detection Languages

- Zeek Intel
- Suricata
- YARA
- Sigma

The Detection Engineering Workflow

Workflow Example

Threat Intelligence Example

A recent threat hunt identified data being exfiltrated from a workstation by a malicious process named wombat.exe. This executable had an original filename of dnsExfiltrator.exe and was apparently sourced from Github. It was written to disk by another executable called AVUpdate.exe, which was downloaded from a counterfeit web site that the user was sent to by a phishing email.

Wombat.exe was exfiltrating files using encoded DNS subdomains in very long TXT queries, all for the domain threescoops.online.

We have the email address that sent the phishing email, the hash values for AVUpdate.exe and wombat.exe, as well as the IP addresses for the counterfeit web site, the probable C2 for AVUpdate, and the destination of the DNS requests.

How do we detect this in the future?

The Detection Engineering Workflow

Choose Your Indicator

Identify The Data Source

Write And Test The Detection

Deploy To Production

Monitor And Tune

Threat Intelligence Example

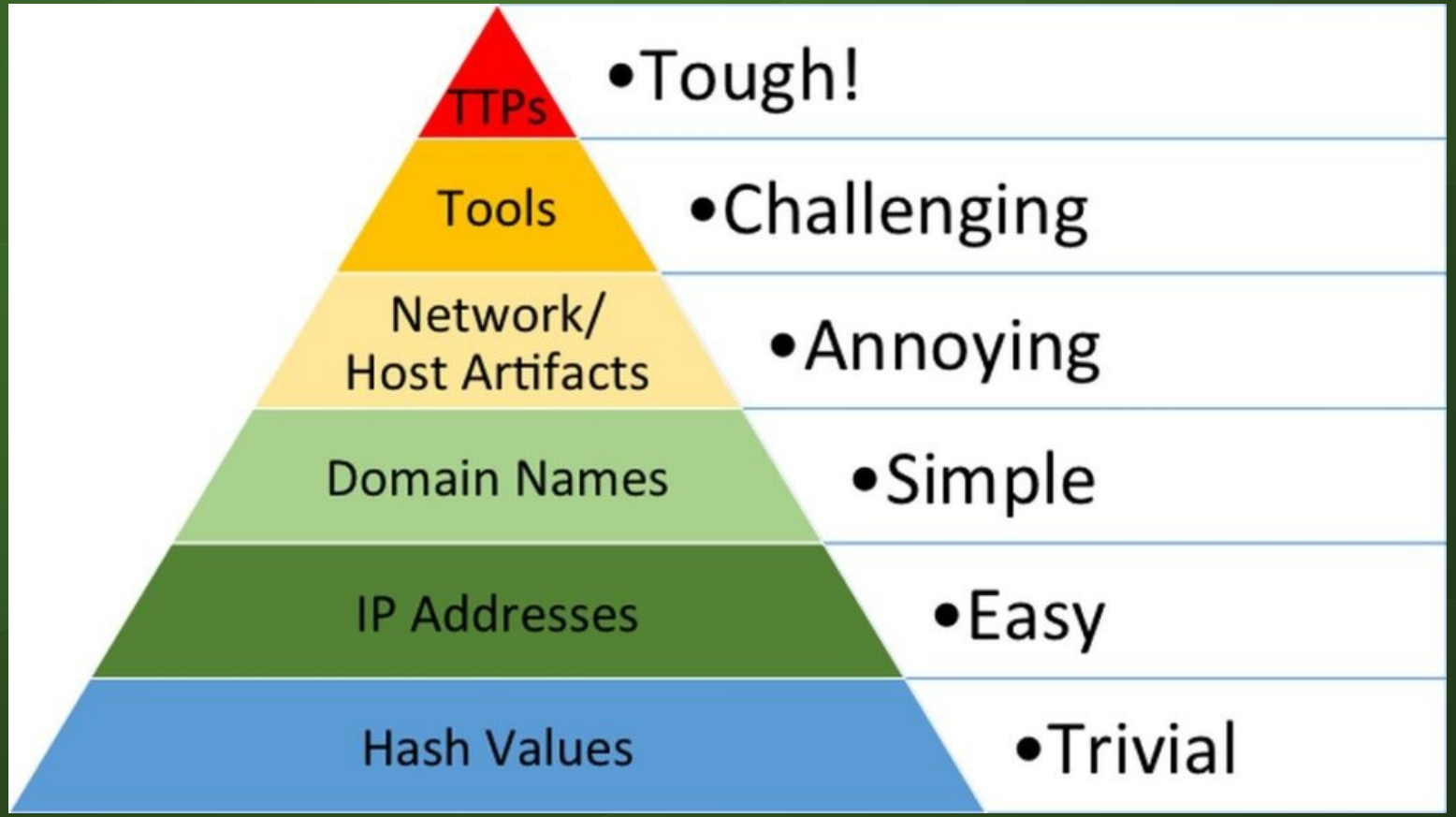
A recent threat hunt identified data being exfiltrated from a workstation by a malicious process named wombat.exe. This executable had an original filename of dnsExfiltrator.exe and was apparently sourced from Github. It was written to disk by another executable called AVUpdate.exe, which was downloaded from a counterfeit web site that the user was sent to by a phishing email.

Wombat.exe was exfiltrating files using encoded DNS subdomains in very long TXT queries, all for the domain threescoops.online.

We have the email address that sent the phishing email, the hash values for AVUpdate.exe and wombat.exe, as well as the IP addresses for the counterfeit web site, the probable C2 for AVUpdate, and the destination of the DNS requests.

How do we detect this in the future?

The Pyramid Of Pain



Threat Intelligence Example

A recent threat hunt identified data being exfiltrated from a workstation by a malicious process named wombat.exe. This executable had an original filename of dnsExfiltrator.exe and was apparently sourced from Github. It was written to disk by another executable called AVUpdate.exe, which was downloaded from a counterfeit web site that the user was sent to by a phishing email.

Wombat.exe was exfiltrating files using encoded DNS subdomains in very long TXT queries, all for the domain threescoops.online.

We have the email address that sent the phishing email, the hash values for AVUpdate.exe and wombat.exe, as well as the IP addresses for the counterfeit web site, the probable C2 for AVUpdate, and the destination of the DNS requests.

How do we detect this in the future?

The Detection Engineering Workflow

Choose Your Indicator

Identify The Data Source

Write And Test The Detection

Deploy To Production

Monitor And Tune

Potential Data Sources

- DNS metadata from Zeek
- DNS queries in endpoint telemetry
- Logs from internal DNS server
- Custom Suricata IDS signature

Potential Data Sources

- DNS metadata from Zeek
- DNS queries in endpoint telemetry
- Logs from internal DNS server
- Custom Suricata IDS signature

The Detection Engineering Workflow

Sigma Detection Rule

Detecting Lengthy DNS TXT Requests

OVERVIEW | OPERATIONAL NOTES | DETECTION SOURCE | TUNING (0) | HISTORY

Summary

This will raise an alert for any DNS request spotted by Zeek that is longer that 200 characters and of type TXT.

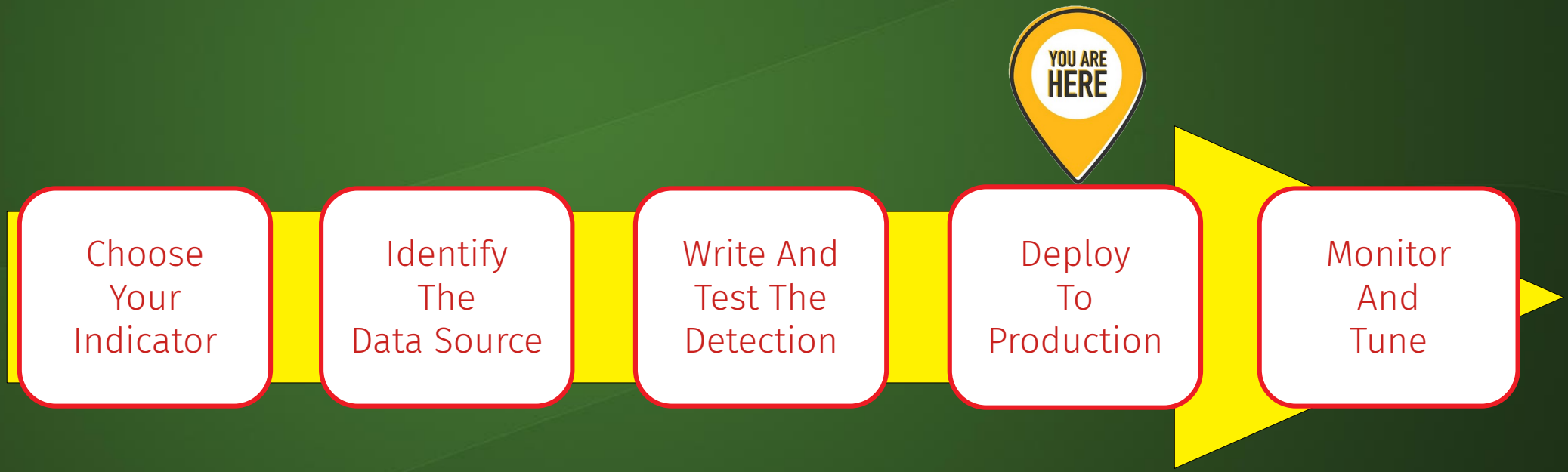
References

https://so-manager/#/case/2pkuSJEBfcdMPWCpkW9X

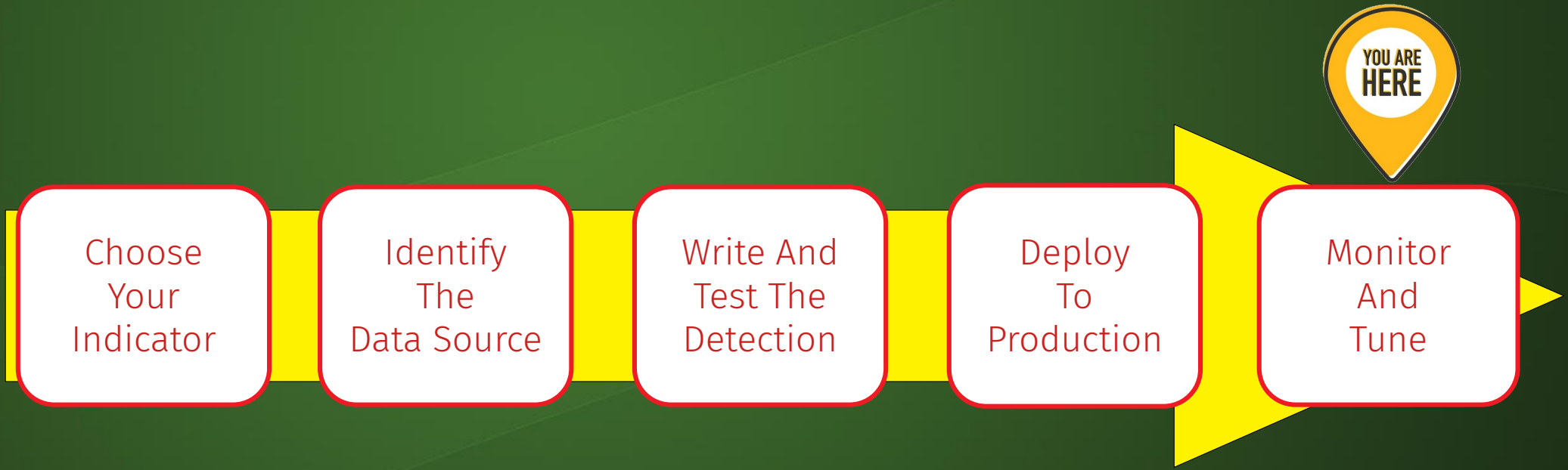
Detection Logic

```
logsource:
  category: dns
  product: zeek
detection:
  selection_dns_type:
    dns.query.type_name: TXT
  selection_dns_query_length:
    dns.query.length|gte: '200'
  condition: all of selection_*
```

The Detection Engineering Workflow



The Detection Engineering Workflow



Threat Intelligence Example 2

(Adapted from https://cloud.google.com/blog/topics/threat-intelligence/triton-actor-ttp-profile-custom-attack-tools-detections/)

A recent threat bulletin outlines the behavior of a group using Scheduled Task XML Triggers as a persistence mechanism. A compromised Windows server would have a new daily task installed via schtasks.exe, pointing to an unsigned executable named napupdatedb.exe. This executable would open a PLINK backdoor for remote SSH connections.

How do we detect this in the future?

Threat Intelligence Example 2

(Adapted from https://cloud.google.com/blog/topics/threat-intelligence/triton-actor-ttp-profile-custom-attack-tools-detections/)

A recent threat bulletin outlines the behavior of a group using Scheduled Task XML Triggers as a persistence mechanism. A compromised Windows server would have a new daily task installed via schtasks.exe, pointing to an unsigned executable named napupdatedb.exe. This executable would open a PLINK backdoor for remote SSH connections.

How do we detect this in the future?

The Detection Engineering Workflow

Conclusion

Questions?

@infosecgoon

infosecgoon@roadflares.org

https://www.github.com/infosecgoon