



DUBLIN

IRELAND

34<sup>th</sup> ANNUAL FIRST CONFERENCE  
JUNE 26 - JULY 1

2022

#FIRSTCON22

# Formulating an Intelligence-Driven Threat Hunting Methodology

---

Joe Slowik (@jfslowik), Gigamon (US)

# Introductions!

- Joe Slowik:
  - Gigamon, Threat Intelligence & Detections Engineering Lead
  - Paralus LLC, CTI Training
  - Previously:
    - DomainTools, CTI Research
    - Dragos, ICS-Focused CTI Research
    - Los Alamos National Laboratory, IR Team Lead
    - US Navy, *Various*



# Agenda

- Threat Hunting Defined
- Hunting Pre-Requisites
- Conceptualizing A Hunting Process
- Hunting Examples
- Hunting To Detections



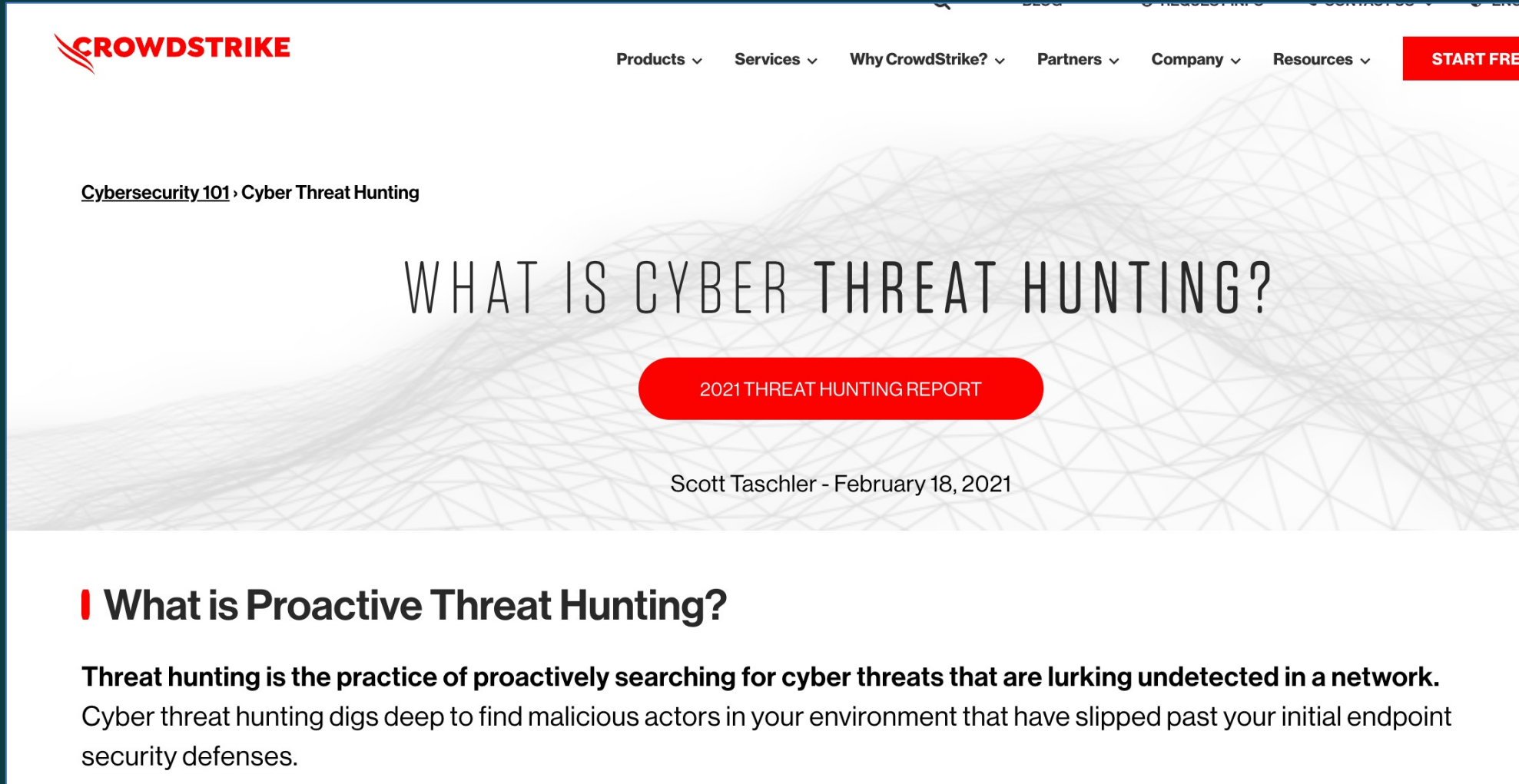
[https://static.tvtropes.org/pmwiki/pub/images/elmer\\_fudd.jpg](https://static.tvtropes.org/pmwiki/pub/images/elmer_fudd.jpg)

# “Hunting”



<https://www.kxan.com/wp-content/uploads/sites/40/2022/02/1040x585-2022-0111-best-hunting-hats-4514ac.jpg?w=1280>

# Formal Definitions?



The screenshot shows the CrowdStrike website header with the logo and navigation menu. The main content area features a large title 'WHAT IS CYBER THREAT HUNTING?' and a prominent red button labeled '2021 THREAT HUNTING REPORT'. Below the button, the author 'Scott Taschler' and the date 'February 18, 2021' are listed. The article begins with a section header 'What is Proactive Threat Hunting?' followed by a definition of threat hunting.

**CROWDSTRIKE** Products ▾ Services ▾ Why CrowdStrike? ▾ Partners ▾ Company ▾ Resources ▾ [START FREE](#)

Cybersecurity 101 · Cyber Threat Hunting

## WHAT IS CYBER THREAT HUNTING?

[2021 THREAT HUNTING REPORT](#)

Scott Taschler - February 18, 2021

### What is Proactive Threat Hunting?

**Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network.** Cyber threat hunting digs deep to find malicious actors in your environment that have slipped past your initial endpoint security defenses.

# Threat Hunting In Brief

Identify Missed Intrusions!

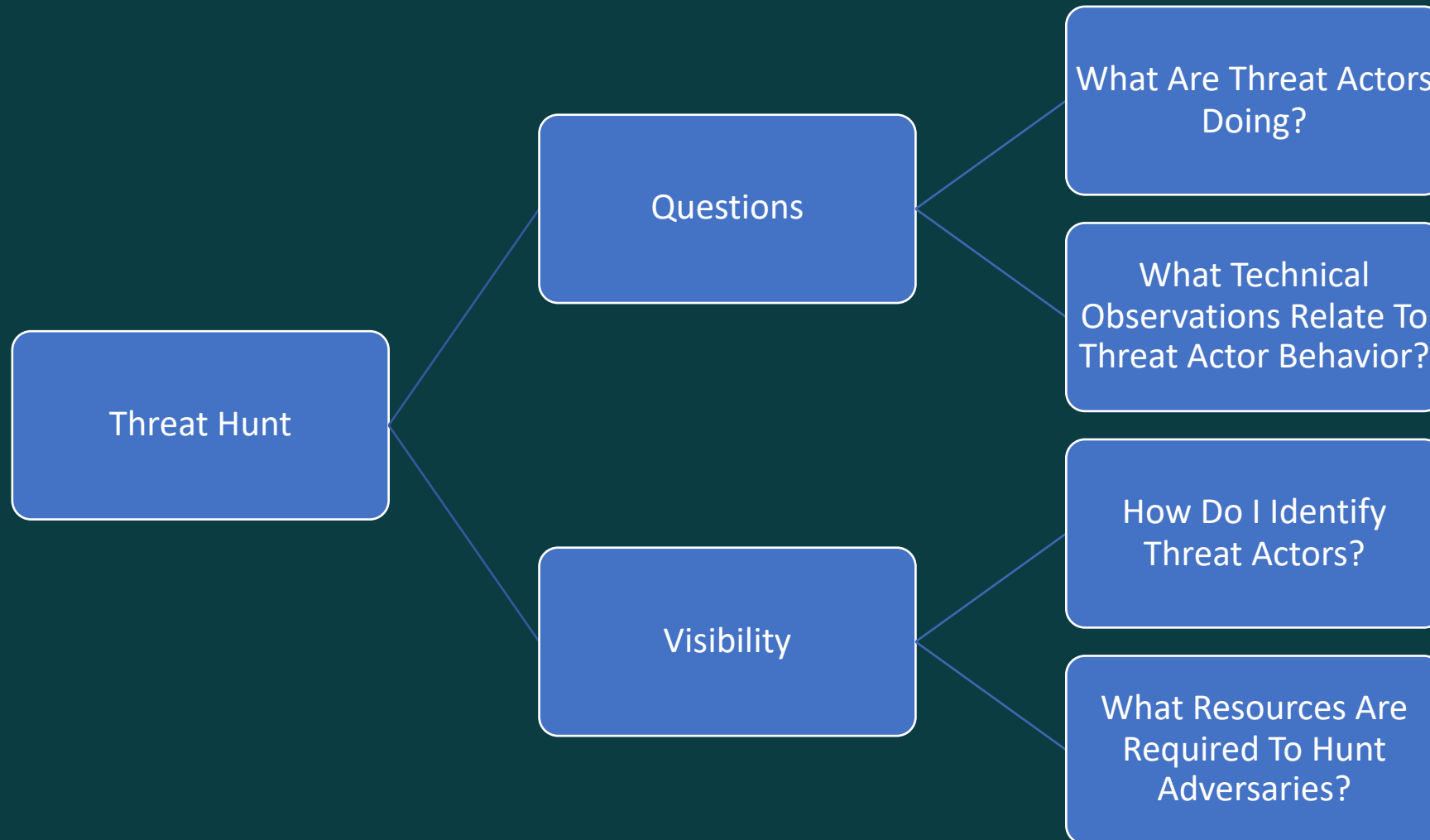


Support SOC By Identifying Adversaries!



Supplement Automated Detections Through  
Interactive Search!

# Threat Hunting Components



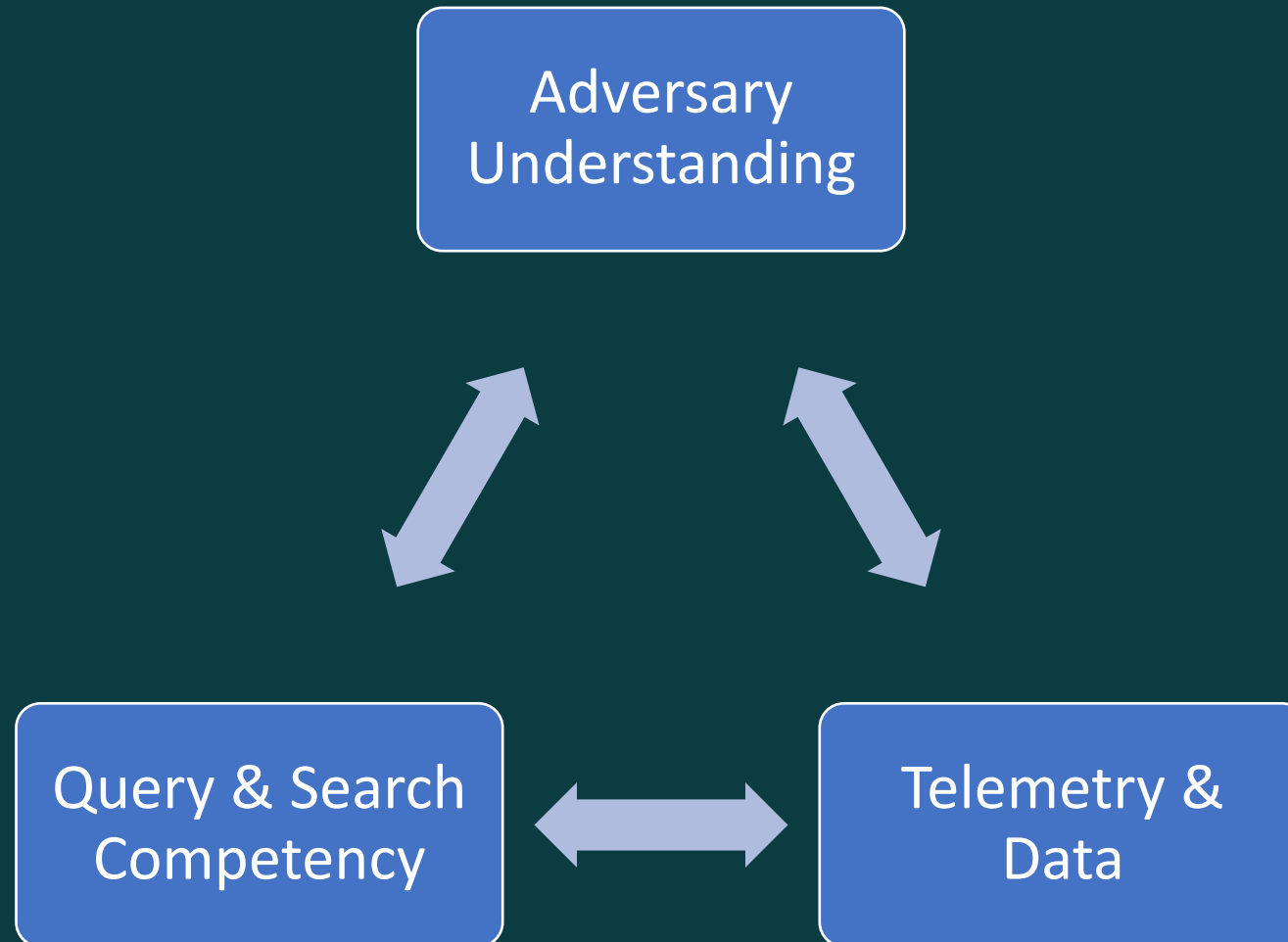
# Pre-Requisites For Hunting



<https://www.allotsego.com/wp-content/uploads/2022/03/elmer-211x300.png>



# Pre-Requisites For Hunting



# Data & Understanding

## Understand Threats

What Artifacts Exist Related To Threat Behavior?

How Do Threat Actors Operate?

What Are Threat Actor Goals And Objectives?

## Understand Visibility

What Can I See?

What Data Sources Are Available?

What Is The Time Sensitivity Of Observations?

## Understand Search Capability

How Do I Query Data?

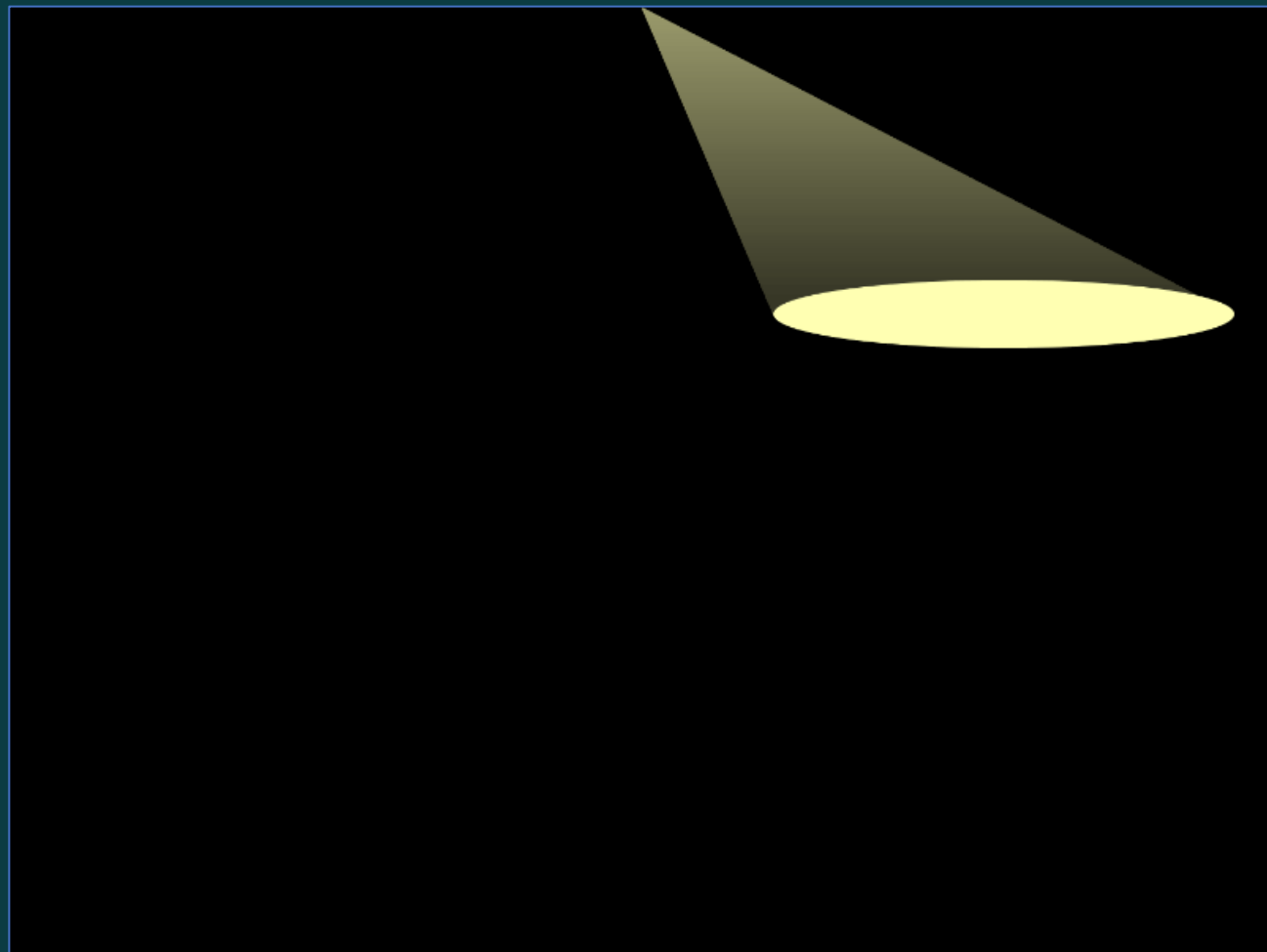
How Effectively Can I Search For Activity?

What Queries Can I Create And Pursue?

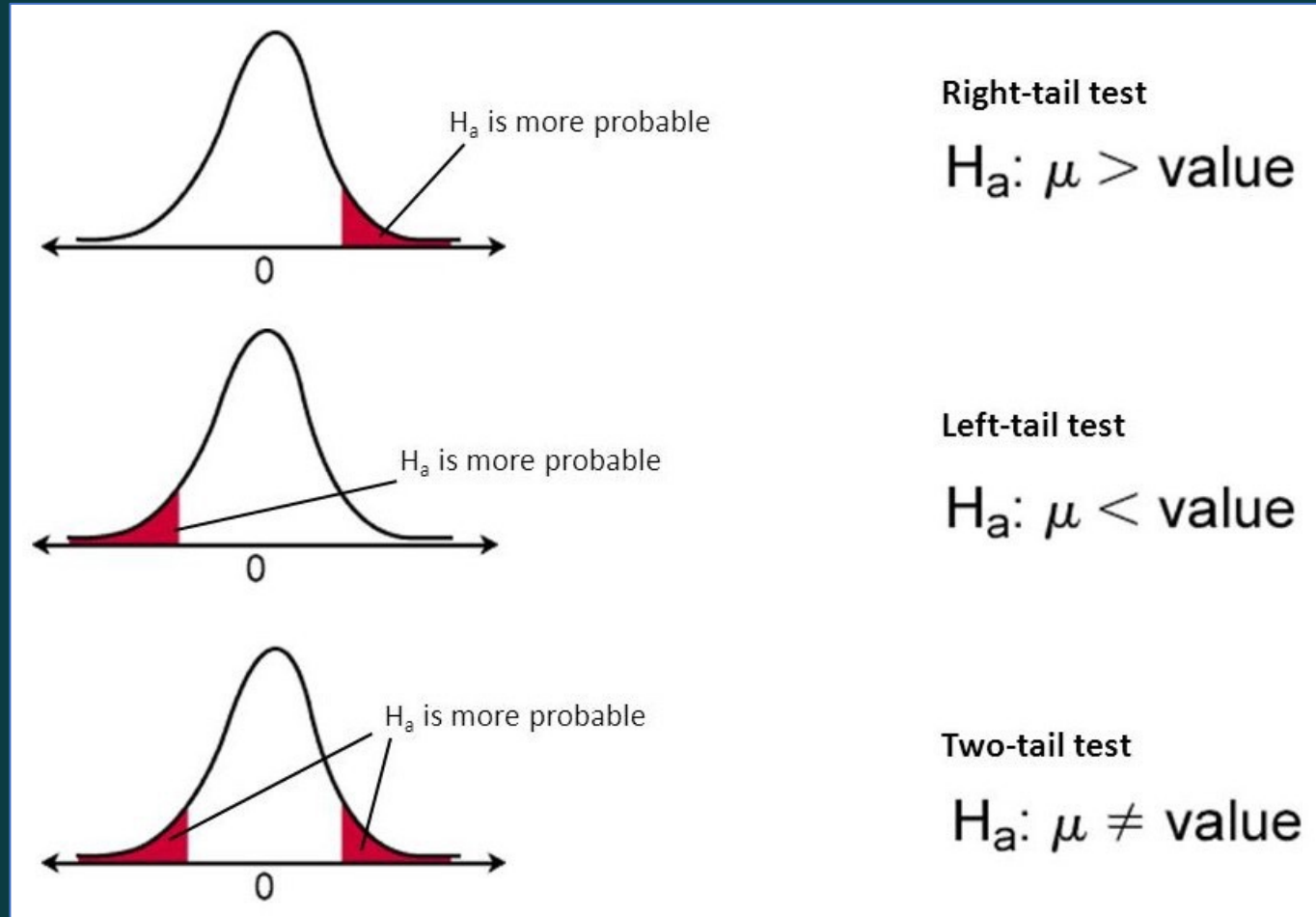
# Hunting In Isolation

HMM?

# Improving Visibility

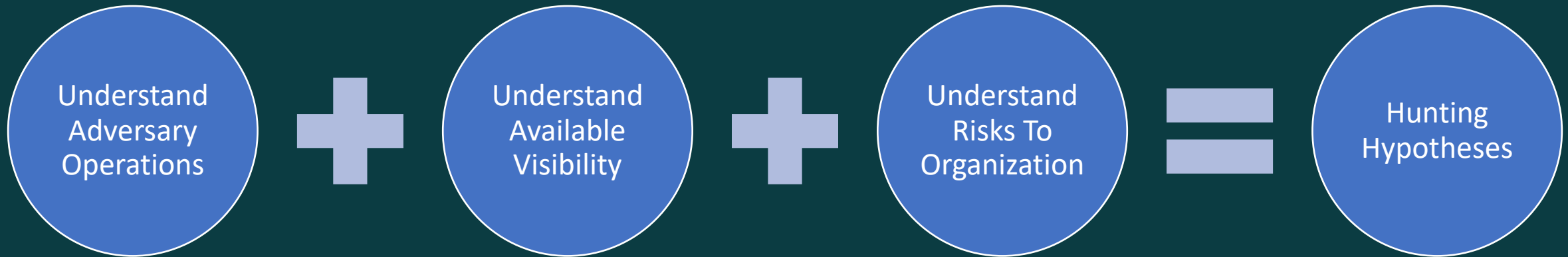


# Developing A Model?



[https://miro.medium.com/max/862/1\\*VXxdieFIYCgR6v7nUaq01g.jpeg](https://miro.medium.com/max/862/1*VXxdieFIYCgR6v7nUaq01g.jpeg)

# Developing A Hunting Process



# Hunting Hypothesis Criteria

Specific

Measurable

Detectable

Relevant

Timely

Testable

# Hypothesis Components: Adversaries

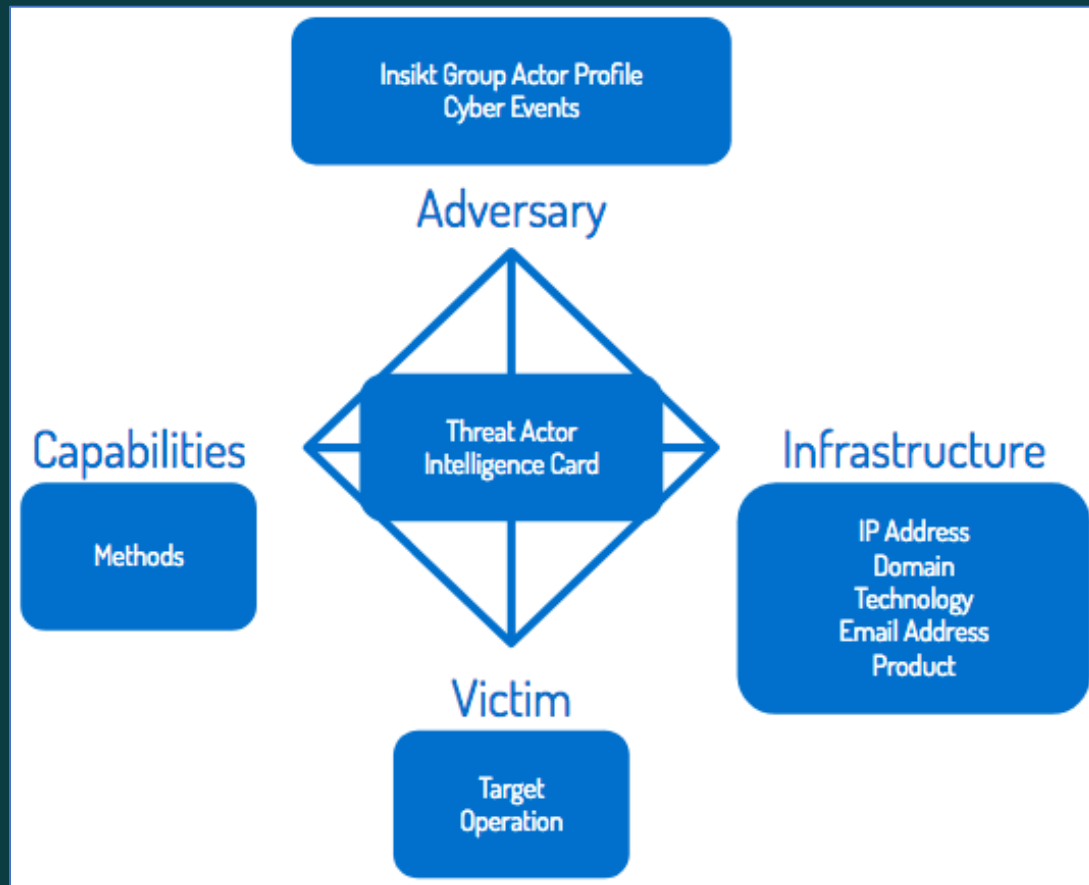
Identify Threats In  
Operating Space

Understand  
Operations &  
Tendencies Of These  
Threats

Learn Behavioral  
Aspects Of Adversary  
Operations



# Understanding Adversary Operations



<https://www.recordedfuture.com/assets/diamond-model-intrusion-analysis-6.png>

<https://thefirereport.com/wp-content/uploads/2021/08/1-10.png>

Cobalt Strike

Cobalt Strike View Attacks Reporting Help

Desktop 192.168.58.35@1512 X

Beacon 10.10.10.191@4844 X

Beacon 10.10.10.198@6984 X

```
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2888
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18
```

[DEVELOPERWS] Jamie.Grins/6984

beacon>

Last: 2s

# Intelligence-Driven Understanding

Which  
Adversaries Are  
Of Interest?

How Do These  
Adversaries  
Operate?

What Are Their  
Goals Or  
Intentions?

# Hypothesis Components: Telemetry

What Sensors Do I Have?



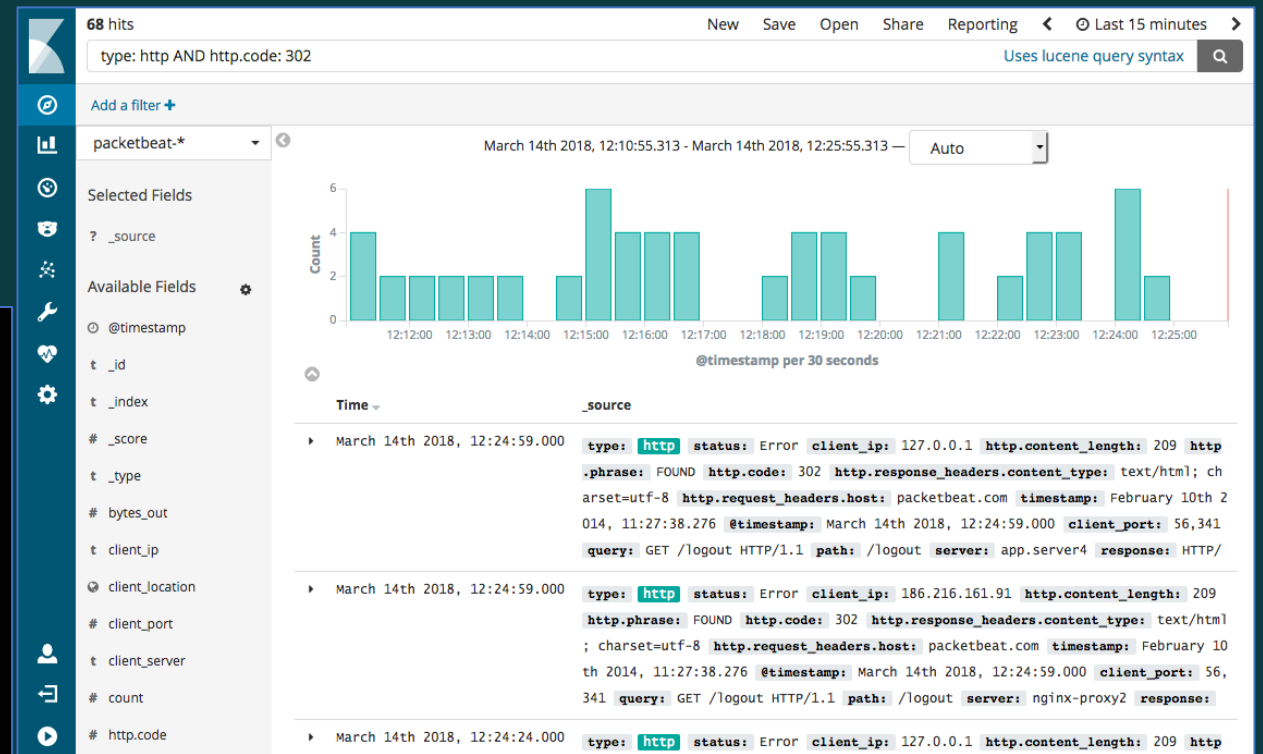
What Activity Can I See?



How Can I Identify Adversary Behaviors Of Interest?

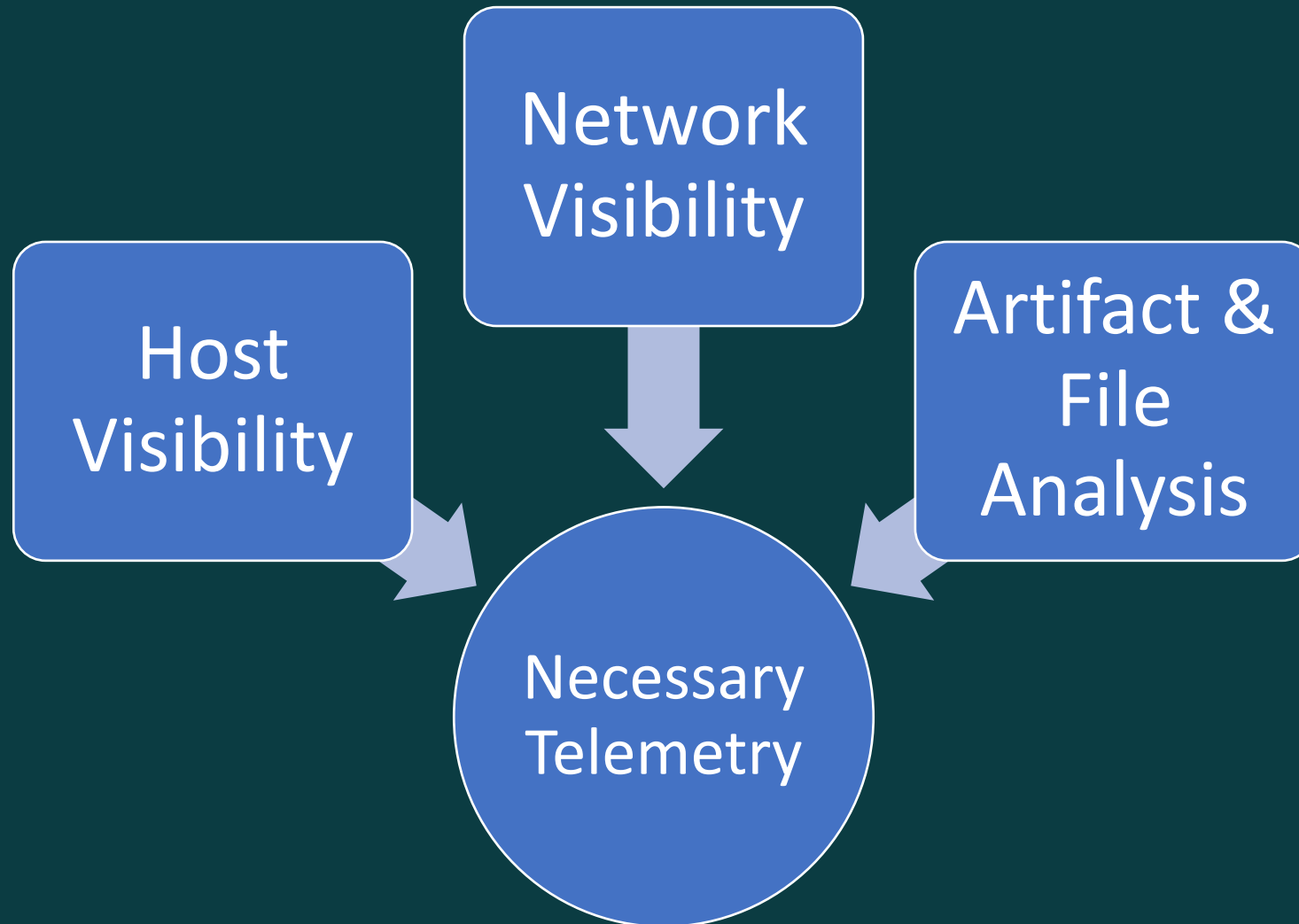
# Visibility & Telemetry

<https://static01.nyt.com/images/2018/05/21/business/21WARROOMS-norse/00WARROOMS-norse-articleLarge.gif?quality=75&auto=webp&disable=upscale>



<https://www.elastic.co/guide/en/beats/packetbeat/current/images/kibana-query-filtering.png>

# Pillars Of Visibility



# Compensating For Visibility Gaps

***Where Visibility Gaps Exist, Leverage Existing Tools And Telemetry To Make Up For Missing Items As Best You Can!***

# Hypothesis Components: Organizational Value



What Purpose Does The Organization Serve?

How Can The Organization's Primary Mission Be Impacted?

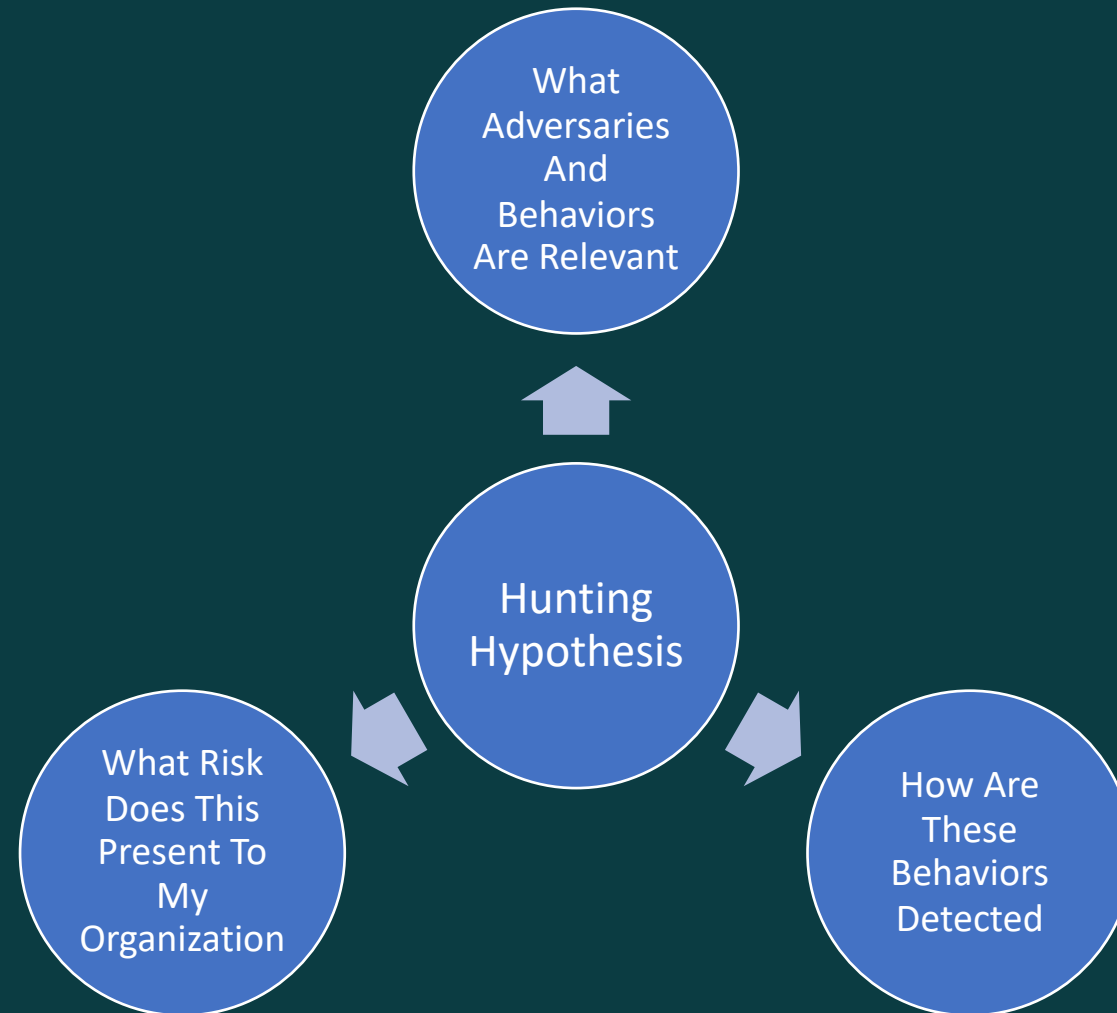
What Are The Most Significant Risk Scenarios?

# Focus & Operational Significance

***Resources Are Limited – Focus Hunting Activity  
On Items Necessary To Maintaining  
Organization's Security Posture & Operations!***



# Putting It All Together



# Threat Hunting in Practice



# Simple Example: BEC

**“BEC-Focused Adversaries Will Attempt To Extract Financial Value From The Organization By Spoofing Or Injecting Into Legitimate Communication Channels, We Can Identify This Activity Through Email Headers And Lack Of Proper Signatures And DKIM”**

# Simple Example: BEC

Identify Threat - BEC

```
graph TD; A[Identify Threat - BEC] --> B[Determine Impact - Monetization]; B --> C[Develop Way To Flag Activity - Email Observables];
```

Determine Impact - Monetization

Develop Way To Flag Activity - Email  
Observables

# More Complex Examples: Ransomware

## THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

ANALYSTS CONTACT US SERVICES

adfind cobaltstrike icedid psexec quantum ransomware

### Quantum Ransomware

April 25, 2022

In one of the fastest ransomware cases we have observed, in under four hours the threat actors went from initial access, to domain wide ransomware. The initial access vector for this case was an IcedID payload delivered via email. We have observed IcedID malware being utilized as the initial access by various ransomware groups. Examples from some of our previous cases include:

- XingLocker – [IcedID to XingLocker Ransomware in 24 hours](#)
- Conti – [Stolen Images Campaign Ends in Conti Ransomware](#) and [Conti Ransomware](#)
- REvil – [Sodinokibi \(aka REvil\) Ransomware](#)

Once the initial IcedID payload was executed, approximately 2 hours after initial infection, the threat actors appeared to begin hands-on-keyboard activity. Cobalt Strike and RDP were used to move across the network before using WMI and PsExec to deploy the Quantum ransomware. This case exemplified an extremely short Time-to-Ransom (TTR) of 3 hours and 44 minutes.

# Intrusion Techniques & Behaviors

Cobalt Strike

PSEXec

WMI

Credential  
Harvesting

ADFind

DC  
Compromise

Admin Share  
Copy

Scheduled  
Task  
Persistence

# Hunting Considerations

## Focus

- What Behaviors Are Covered By Existing Detections?
- Where Do Gaps Exist?

## Possibility

- What Data Exists?
- What Can You See?

## Resources

- How Is Your Hunt Team Organized & Deployed?
- Do You Have Time to Hunt Effectively?

# Possible Hunting Hypothesis

**“Ransomware Affiliates Will Utilize Active Directory Enumeration Tools Such As ADFind, BloodHound, Etc., For Discovery And Reconnaissance Purposes. If Logs Or Visibility Are Available, Identifying Excessive AD-Related Activity Or LDAP Queries Can Identify This Precursor To Ransomware Deployment.”**



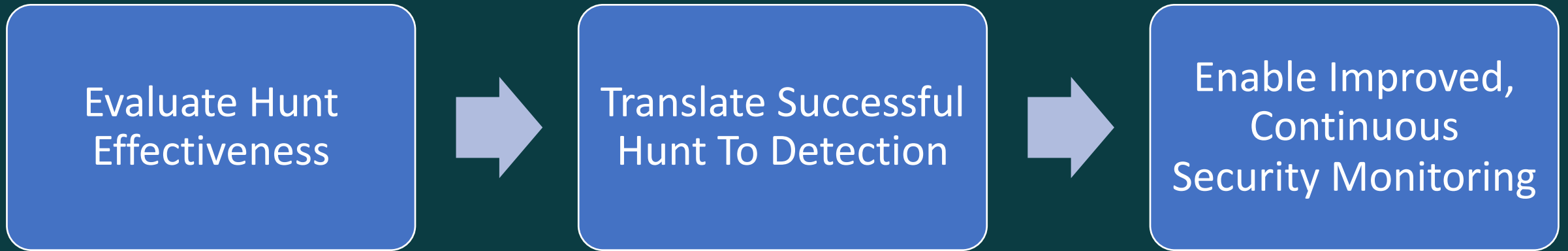
# Hunting to Detections



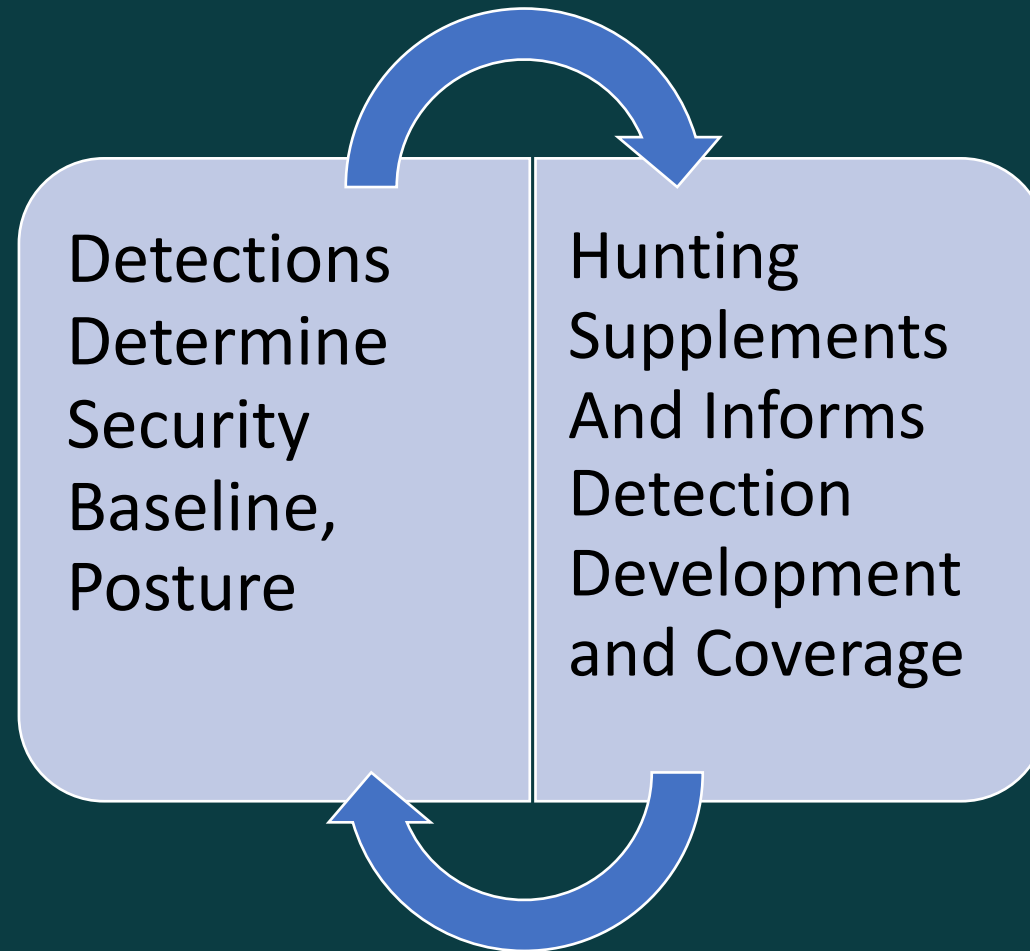
# Repetitive Hunting Is Wasteful!



# Hunting As Process



# Threat Hunting & Detection Engineering



# Conclusion

Understand Adversaries!



Know Visibility And Monitoring Capabilities!



Leverage Above To Hunt For Threats, Improve Security Posture!



Capture Successful Hunts As Detections To Codify Security Success!

# Questions?

Joe.Slowik@gigamon.com  
@jfslowik

