Reducing Dwell Time of Malicious Actors in your Network and Formulating the Threat Hunting Methodology

Matthew Plummer
Gigamon Public Sector CTO

Introductions!

Matthew Plummer

Current Gigamon Public Sector CTO

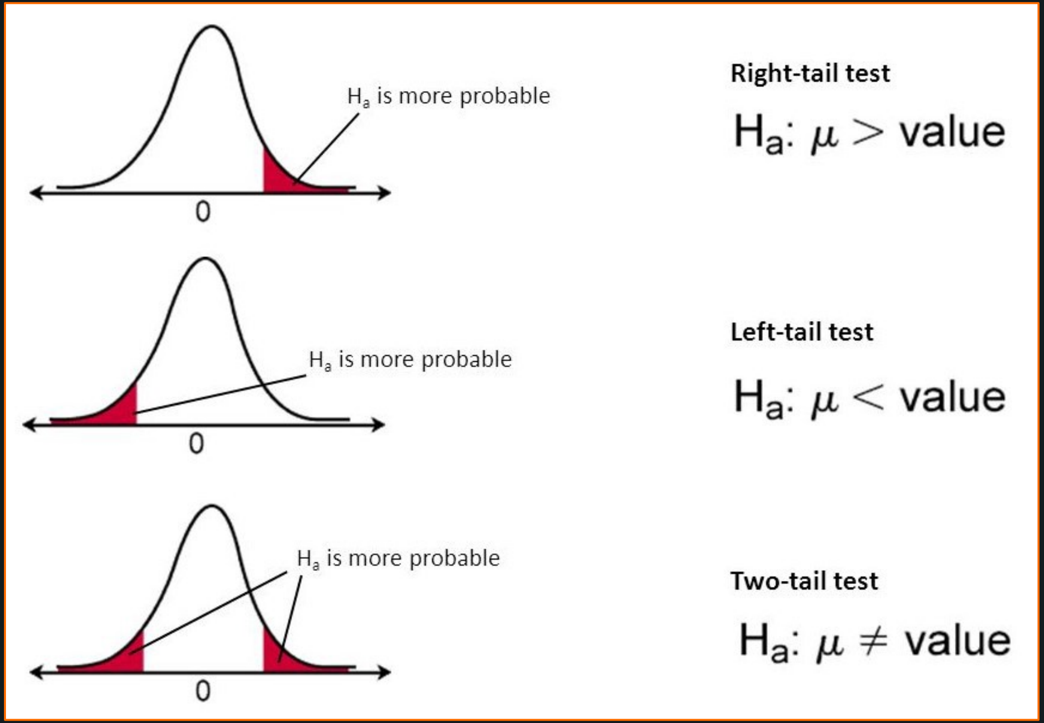
- Tasked with creating future leaning technology thought Zero Trust, DevSecOps, AI/ML, Threat Intelligence and research

24 + Years developing federal regulations and policies

- Shaping technology strategy and guiding implementation, management, and growth in technical environments
- Leading highly skilled teams in designing and producing customer aligned and failsafe cybersecurity technology solutions and then translating them for the customer
- Working with the Federal government and its technology regulators, defense contractors who work to support the Federal enterprise, and national cyber defense operators
- Continue to work adjacent to those areas in commercial, academia and financial domains

Agenda

- Introductions
- Statistics
- Dwell Time
- Example of Dwell and Ransomware Attack
- MITRE ATT&CK
- Defining Threat Hunting/Hunting In Isolation
- Q&A



*https://miro.medium.com/max/862/1*VXxdieFiYCgR6v7nUaq01g.jpeg*

Attackers Enjoy First Move Advantage

ATTACKER SPEED

9 hours

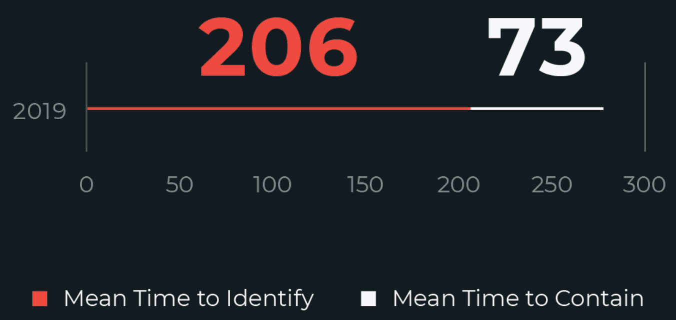
Time From Intrusion

Lateral Movement

Ultimate Objective[1]

DEFENDER SPEED

Days to Identify & Contain a Data Breach[2]



Consequences

3.9%

2019 Global Average

Abnormal Customer Turnover (Increased Churn) Following a Breach by Industry[3]

$4.2M

2019 Global Average

Average Cost Data Breach Cost Due to Increased Churn[3]

1. CrowdStrike 2020 Global Threat Report | 2. Verizon 2019 Data Breach Investigation Report | 3. Ponemon 2019 Cost of a Data Breach Report

Statistics Organizations are Facing

The Impact of Ransomware

73%

Global organizations were the target of ransomware over the past 24 months[1]

$812k

Average ransomware payment in 2022[2]

130

Different ransomware strains detected since 2020

1. CyberReason Report: Ransomware – The True Cost to Business
2. Sophos – State of Ransomware 2022 Report

Dwell time represents the length of time a cyberattacker has free reign in an environment, from the time they get in until they are eradicated.

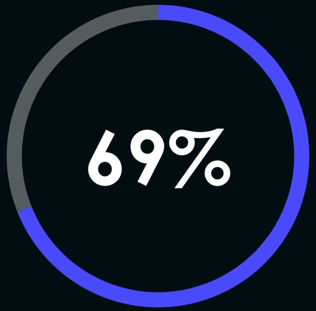
Online Definition

Dwell time is determined by adding mean time to detect (MTTD) and mean time to repair/remediate (MTTR), and is usually measured in days.

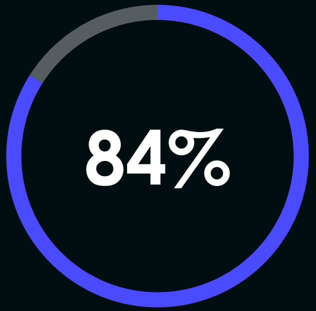
Online Definition

[illegible]

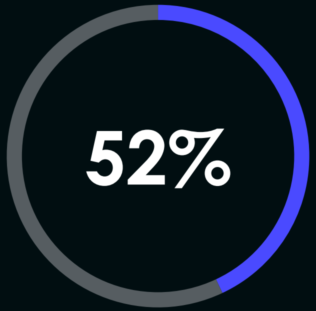
Days to identify and contain a Data Breach[1] in 2021



Of SOC analyst cite lack of visibility into network traffic as the top reason for SOC ineffectiveness[2]



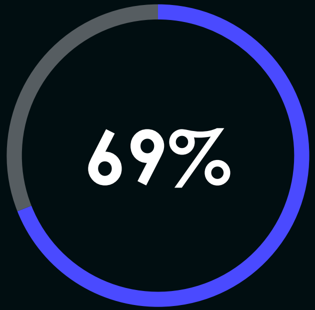
Of SOC analyst rank “Minimization of false positives” as the most important SOC activity (detection tuning) [2]



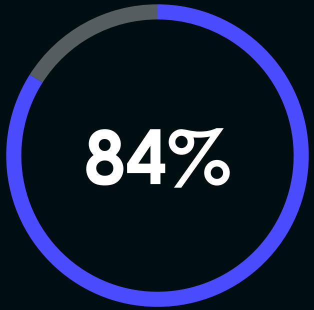
Of SOC analyst report they need access to more out-of-the-box content (i.e., rules, playbooks).[2]

1. Cost of a Data Breach Report 2021 – IBM Security 2. Ponemon: Improving the Effectiveness of the SOC, 2020

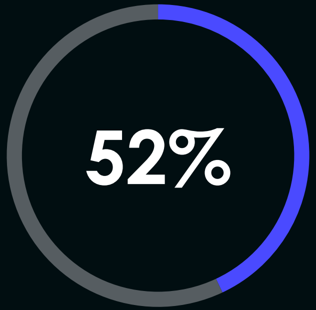
Days to identify and contain a Data Breach[1] in 2021



Of SOC analyst cite lack of visibility into network traffic as the top reason for SOC ineffectiveness[2]



Of SOC analyst rank "Minimization of false positives" as the most important SOC activity (detection tuning) [2]



Of SOC analyst report they need access to more out-of-the-box content (i.e., rules, playbooks).[2]

Extended dwell times don't have to be an advantage for attackers

Visibility is a foundational need

Reducing false positives should be the vendor's responsibility

Guided Playbooks and parallel hunting are foundational

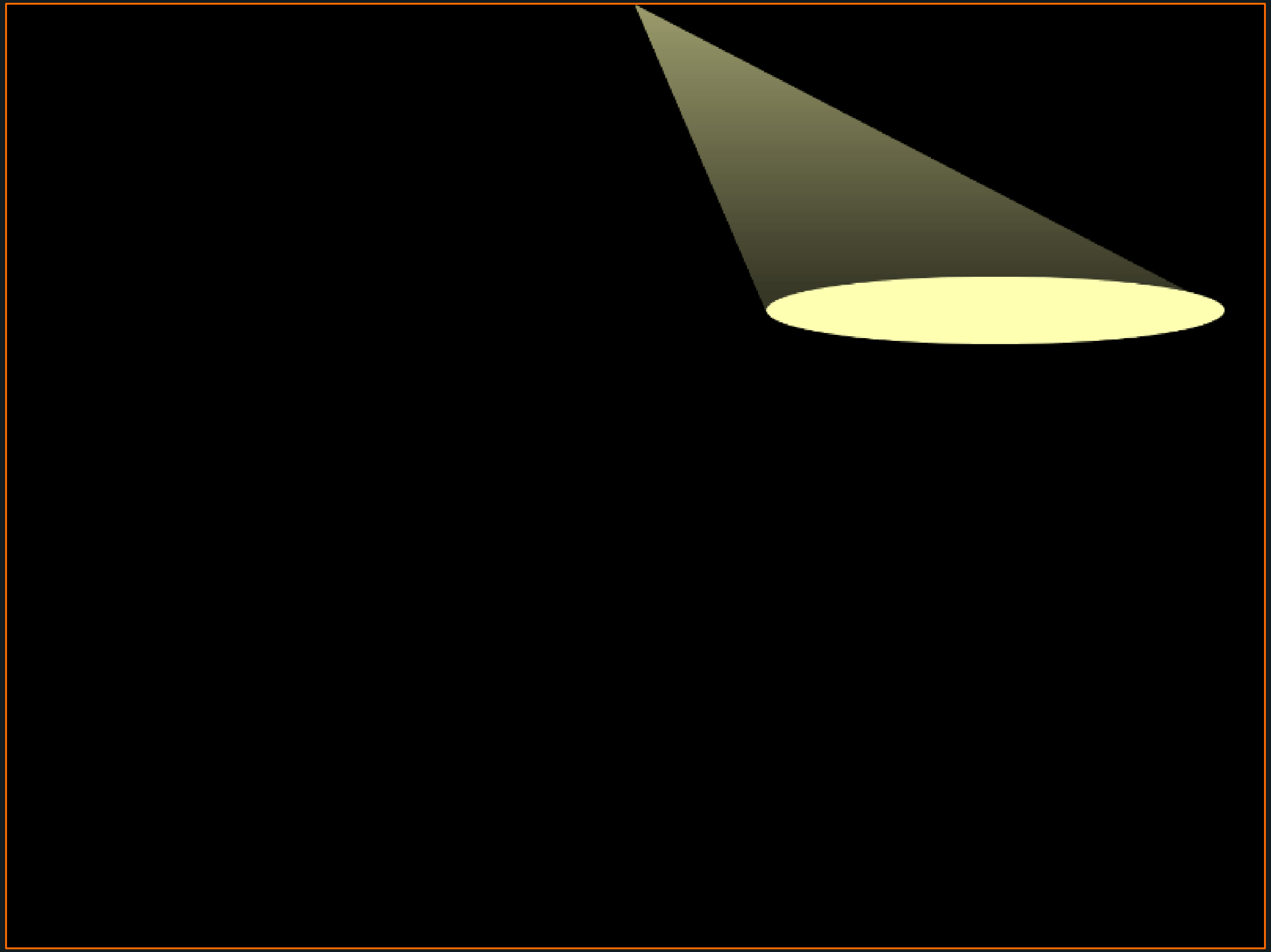
1. Cost of a Data Breach Report 2021 – IBM Security 2. Ponemon: Improving the Effectiveness of the SOC, 2020

Hunting In Isolation

Hunting Components & Requirements

Improving Visibility & Adding Context

Hunting Components & Requirements



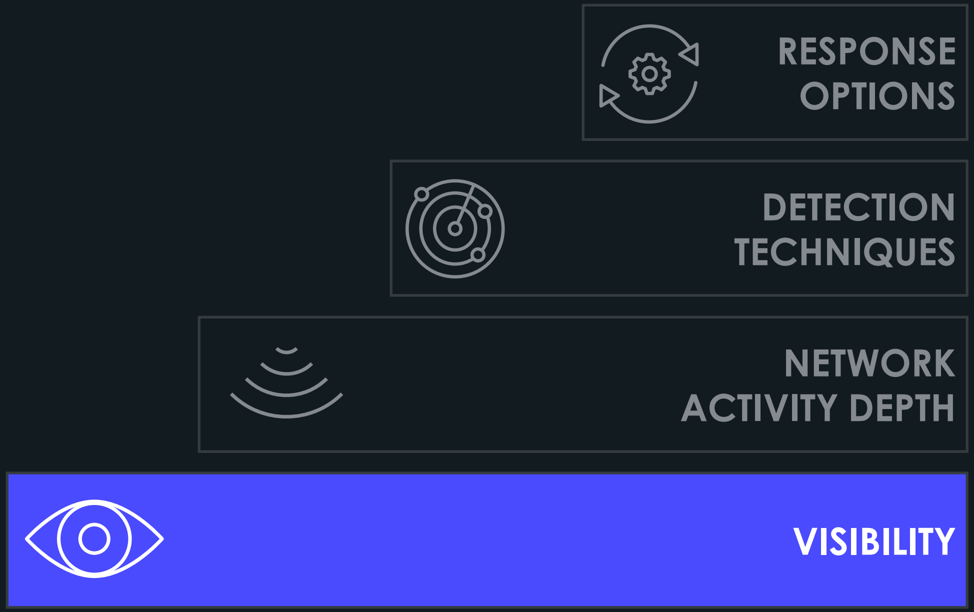
Technology Components

Visibility

- North, South, East, and West,
- Cloud network activity, teleworkers and remote sites

Visibility

- Device Visibility
- On-premise Visibility
- Cloud Infrastructure Visibility
- Teleworker & Remote Site Visibility



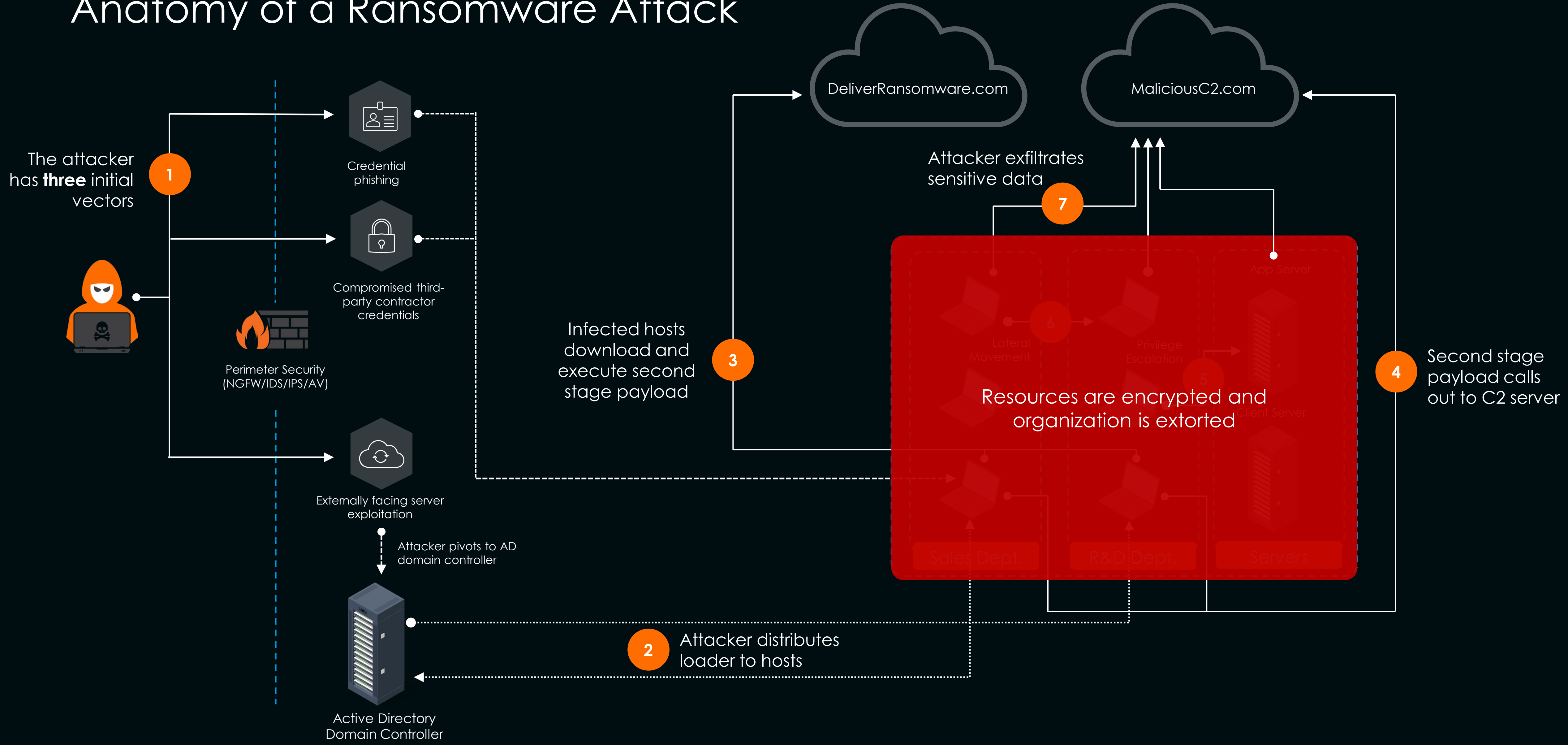
RESPONSE OPTIONS

DETECTION TECHNIQUES

NETWORK ACTIVITY DEPTH

VISIBILITY

Anatomy of a Ransomware Attack



The attacker has **three** initial vectors 1

Credential phishing

Compromised third-party contractor credentials

Perimeter Security (NGFW/IDS/IPS/AV)

Externally facing server exploitation

Attacker pivots to AD domain controller

Active Directory Domain Controller

2 Attacker distributes loader to hosts

Infected hosts download and execute second stage payload 3

DeliverRansomware.com

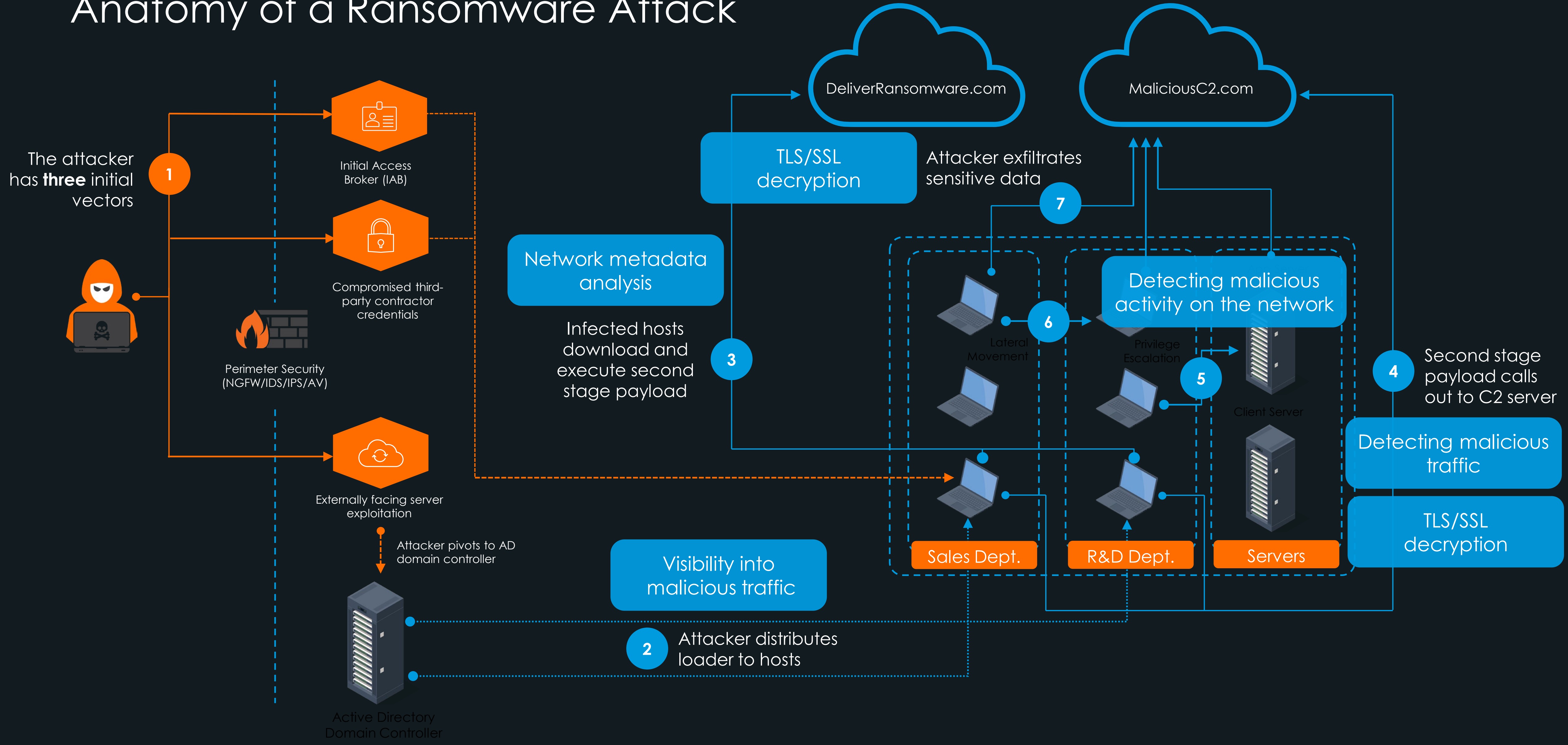
MaliciousC2.com

4 Second stage payload calls out to C2 server

Attacker exfiltrates sensitive data 7

Resources are encrypted and organization is extorted

Anatomy of a Ransomware Attack



1 The attacker has **three** initial vectors

Initial Access Broker (IAB)

Compromised third-party contractor credentials

Externally facing server exploitation

Perimeter Security (NGFW/IDS/IPS/AV)

Attacker pivots to AD domain controller

2 Attacker distributes loader to hosts

3 Infected hosts download and execute second stage payload

4 Second stage payload calls out to C2 server

5

6

7 Attacker exfiltrates sensitive data

Network metadata analysis

TLS/SSL decryption

Visibility into malicious traffic

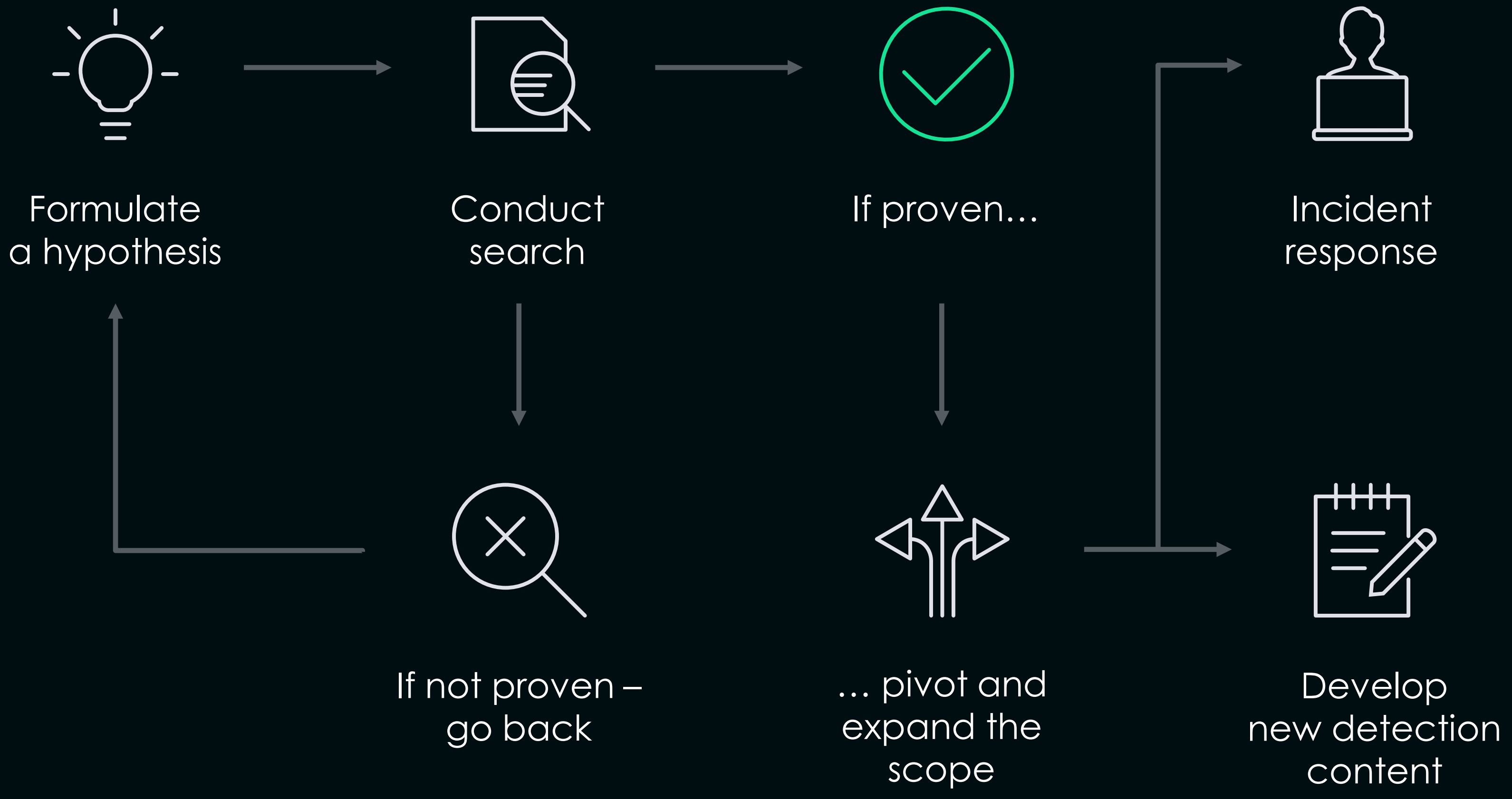
Detecting malicious activity on the network

Detecting malicious traffic

TLS/SSL decryption

Proactive Hunting Defined

Position to *proactively* hunt for threats before they become an alert

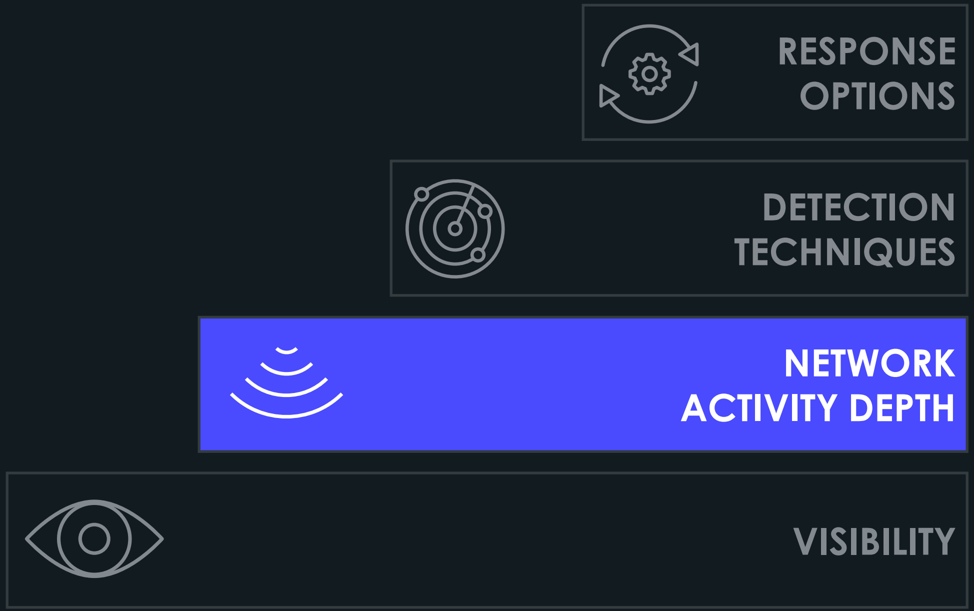


Technology Components

Activity Depth

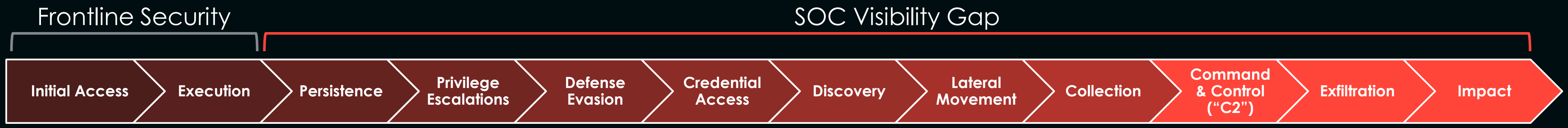
Detections and Response activities are only as good as the richness of the data available from the observed network traffic:

- N/S Activity
- N/S/E/W Flow Activity
- N/S/E/W Packet Activity



MITRE ATT&CK Framework

A comprehensive matrix of attacker tactics and techniques used by defenders to better classify incidents and assess an organization's risk



Accepted Fact:

Attackers are good at getting past preventative-based security tools

The SOC Visibility Gap risks:

- Ineffective security team time chasing phantom alerts from frontline tools
- Business interruptions (ransomware / cryptoware / system outages)
- Cyber espionage (corporate secrets, customer PII, intellectual property)
- Financial impacts (brand damage, employment risks, bottom line losses)

Once inside, attackers remain hidden and carry out their mission

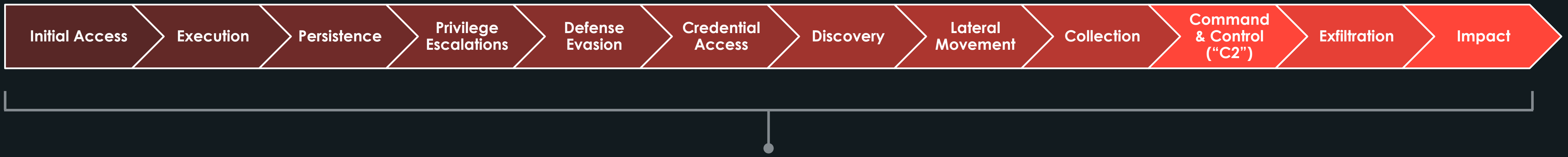
Attackers move freely within an organization, undetected

Stealing credentials, accessing systems, & stealing intellectual property

Exfiltrating what they have stolen or causing damage

WHY NETWORK DETECTION & RESPONSE IS IMPORTANT

Attacker Tactics & Techniques (start to finish)



Initial Access → Execution → Persistence → Privilege Escalations → Defense Evasion → Credential Access → Discovery → Lateral Movement → Collection → Command & Control ("C2") → Exfiltration → Impact

NDRs identify behaviors of hidden, unknown threats that other solutions can't

Attackers are good at getting past preventative-based security tools

If successful, attackers remain hidden and carry out their mission

Attackers move freely within an organization

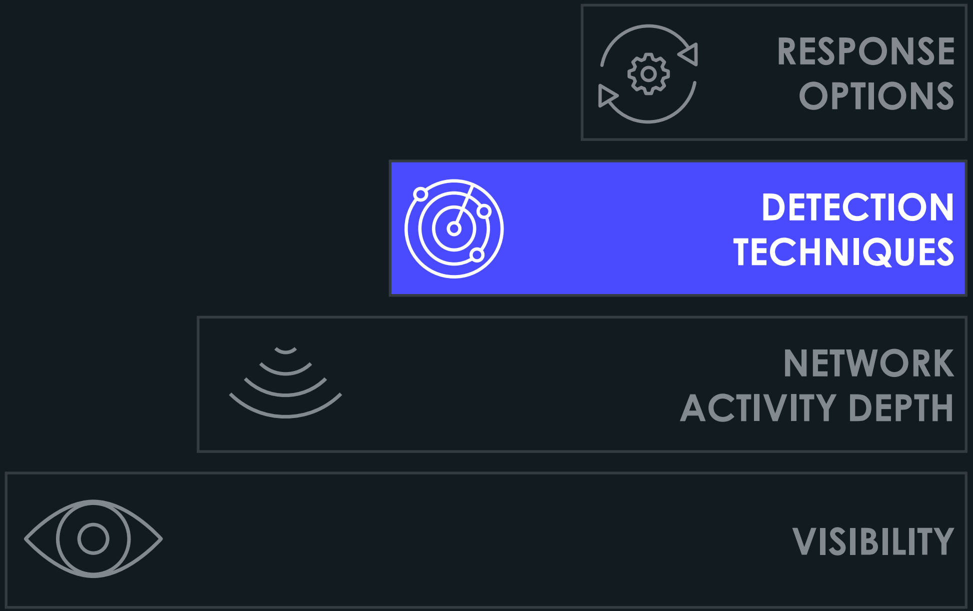
Stealing credentials, accessing systems, and stealing intellectual property

Exfiltrating what they have stolen or causing damage

Technology Components

Detection

- Curated Threat Intelligence
- Machine Learning & Behavioral Analysis
- Attack Spectrum



RESPONSE OPTIONS

DETECTION TECHNIQUES

NETWORK ACTIVITY DEPTH

VISIBILITY

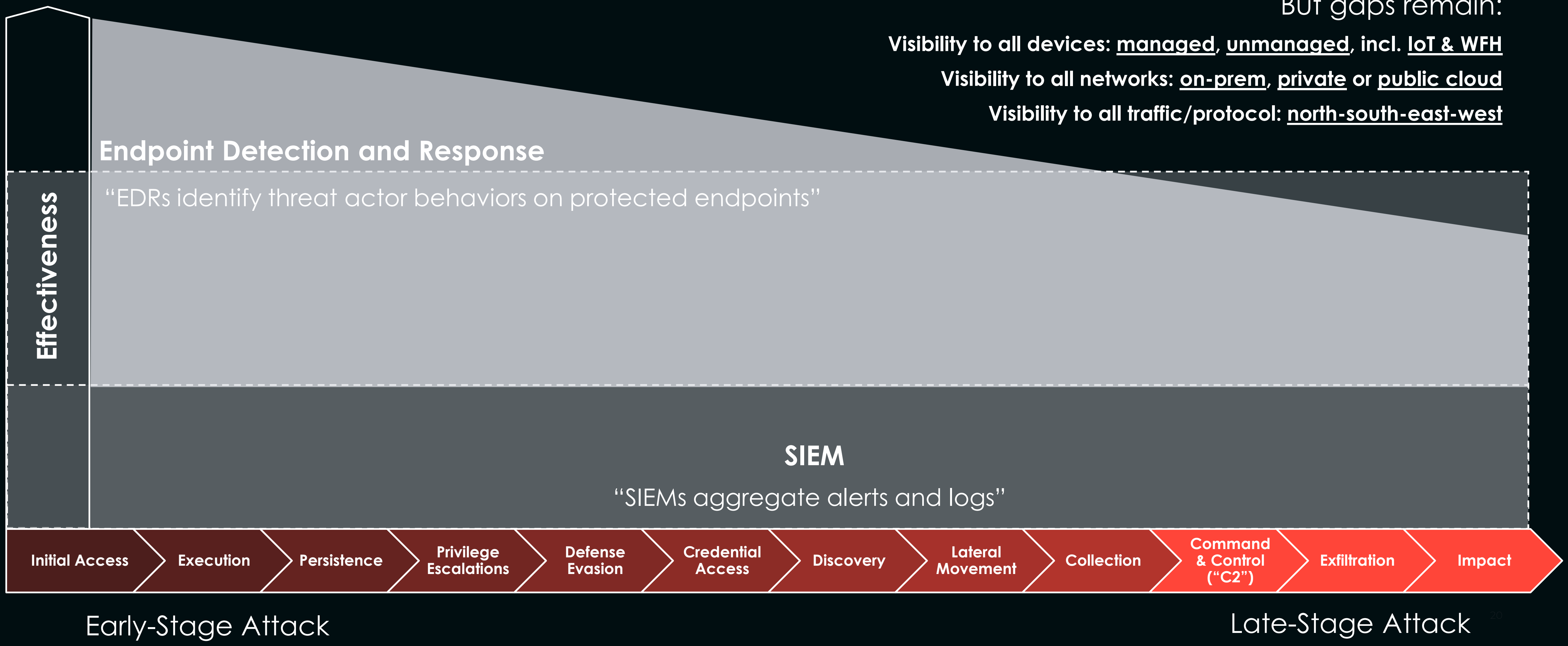
SOC Visibility Gap

But gaps remain:

Visibility to all devices: managed, unmanaged, incl. IoT & WFH

Visibility to all networks: on-prem, private or public cloud

Visibility to all traffic/protocol: north-south-east-west



Effectiveness

Endpoint Detection and Response

"EDRs identify threat actor behaviors on protected endpoints"

SIEM

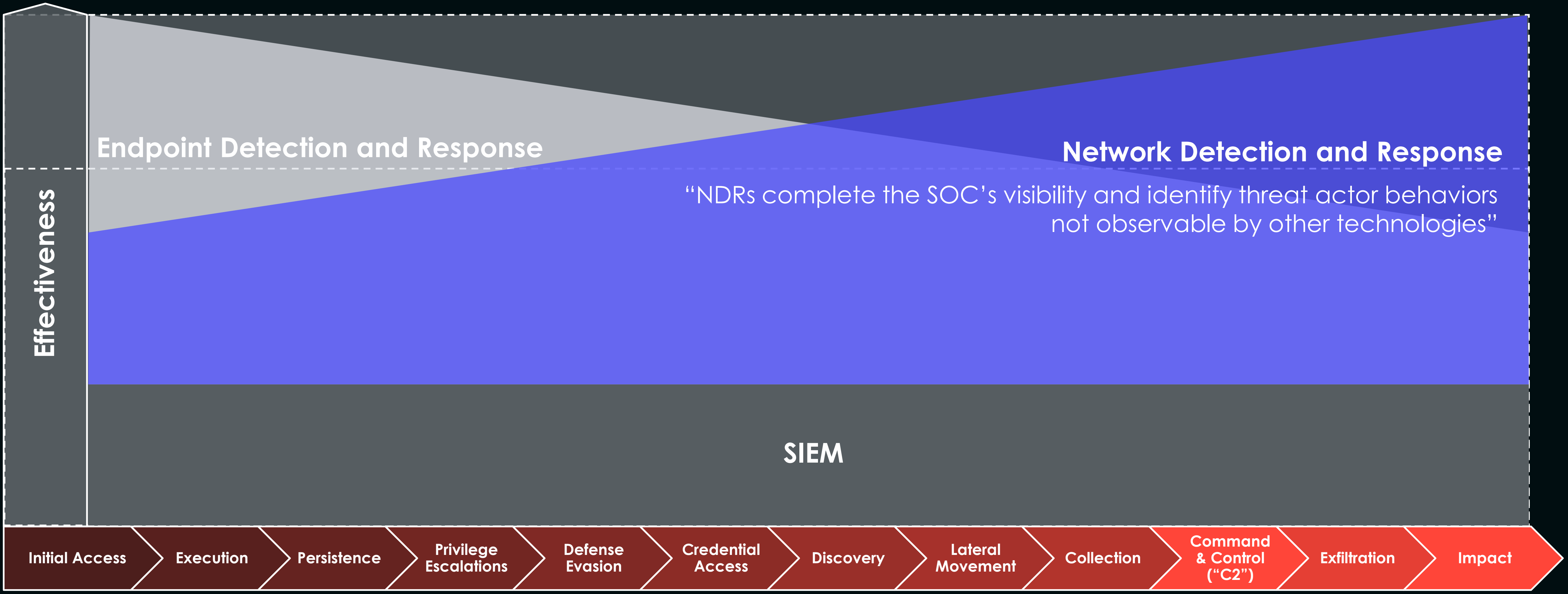
"SIEMs aggregate alerts and logs"

Initial Access → Execution → Persistence → Privilege Escalations → Defense Evasion → Credential Access → Discovery → Lateral Movement → Collection → Command & Control ("C2") → Exfiltration → Impact

Early-Stage Attack

Late-Stage Attack

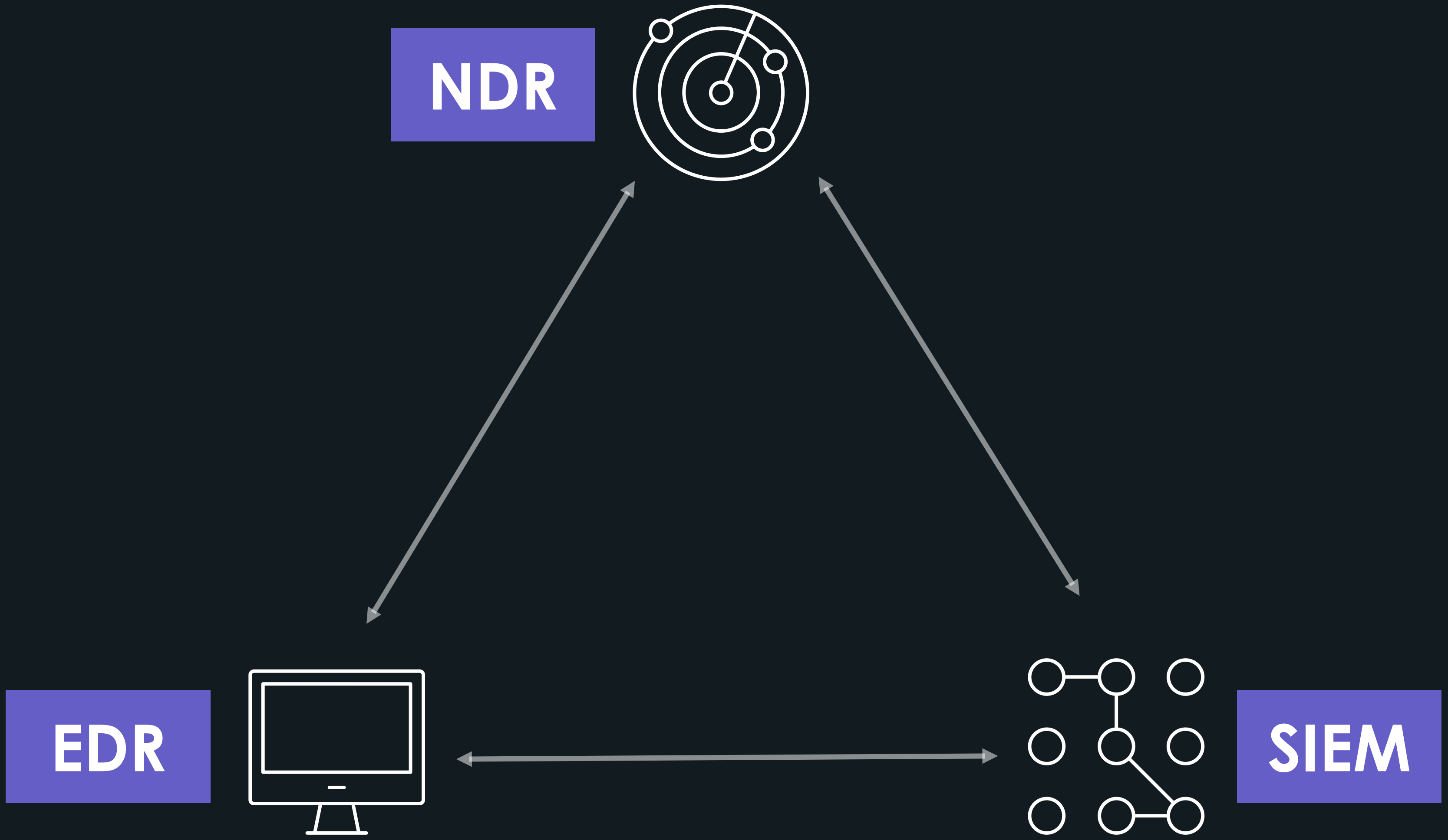
Full SOC Visibility Achieved



"NDRs complete the SOC's visibility and identify threat actor behaviors not observable by other technologies"

Early-Stage Attack

Late-Stage Attack



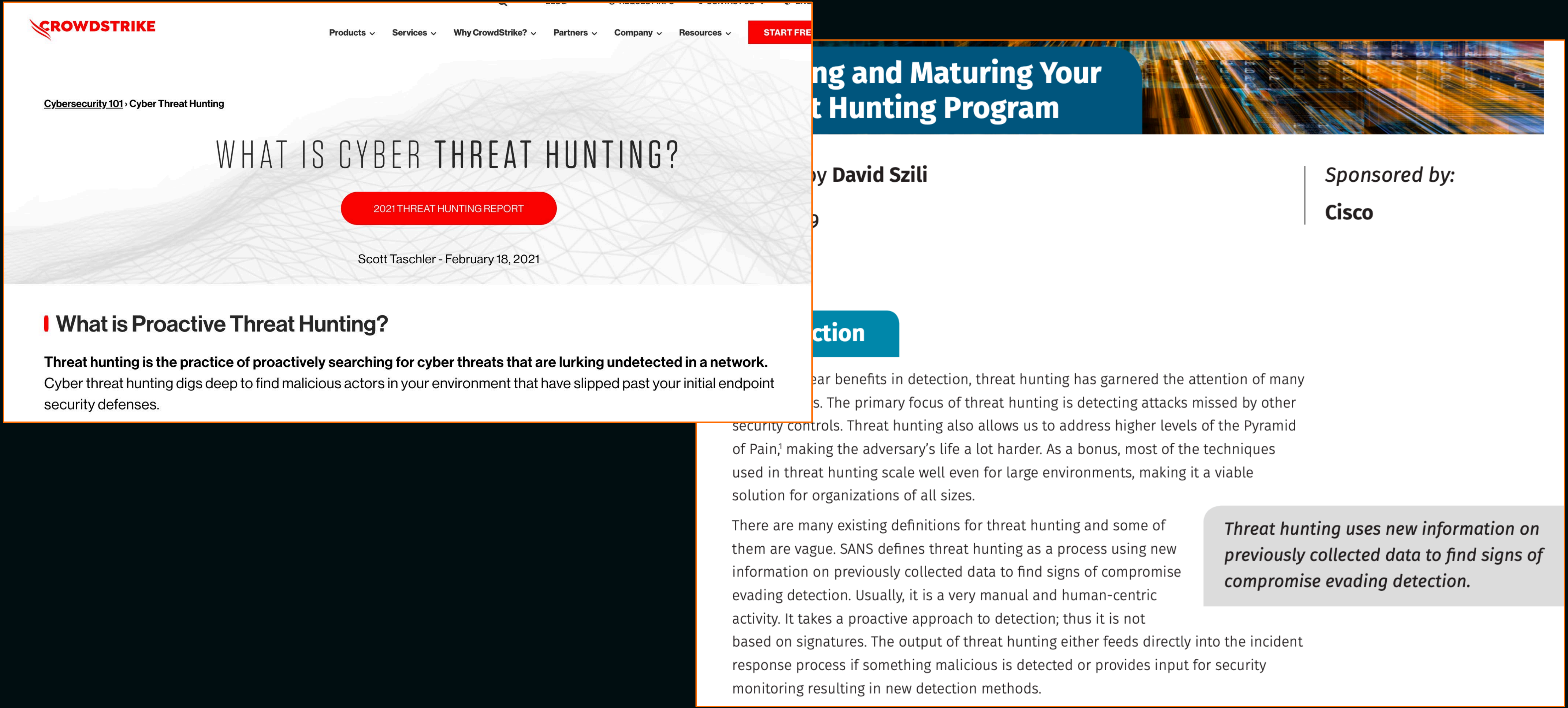
NDR

EDR

SIEM

Formal Definitions?

Understanding "Hunting"



Cybersecurity 101 › Cyber Threat Hunting

WHAT IS CYBER THREAT HUNTING?

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.

ng and Maturing Your t Hunting Program

y David Szili

9

Sponsored by:

Cisco

ction

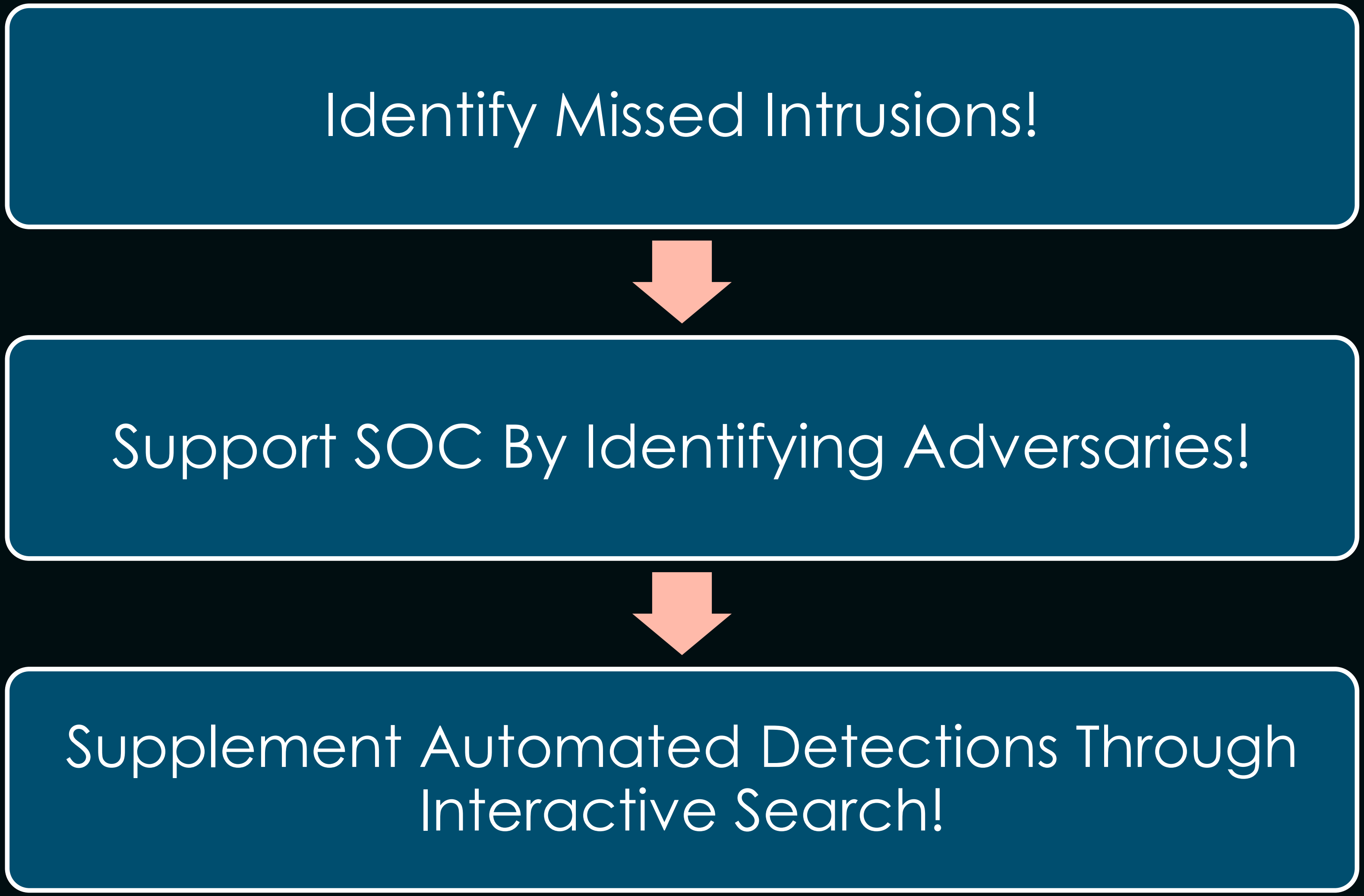
ear benefits in detection, threat hunting has garnered the attention of many s. The primary focus of threat hunting is detecting attacks missed by other security controls. Threat hunting also allows us to address higher levels of the Pyramid of Pain,[1] making the adversary's life a lot harder. As a bonus, most of the techniques used in threat hunting scale well even for large environments, making it a viable solution for organizations of all sizes.

Threat hunting uses new information on previously collected data to find signs of compromise evading detection.

There are many existing definitions for threat hunting and some of them are vague. SANS defines threat hunting as a process using new information on previously collected data to find signs of compromise evading detection. Usually, it is a very manual and human-centric activity. It takes a proactive approach to detection; thus it is not based on signatures. The output of threat hunting either feeds directly into the incident response process if something malicious is detected or provides input for security monitoring resulting in new detection methods.

Threat Hunting In Brief

Understanding “Hunting”



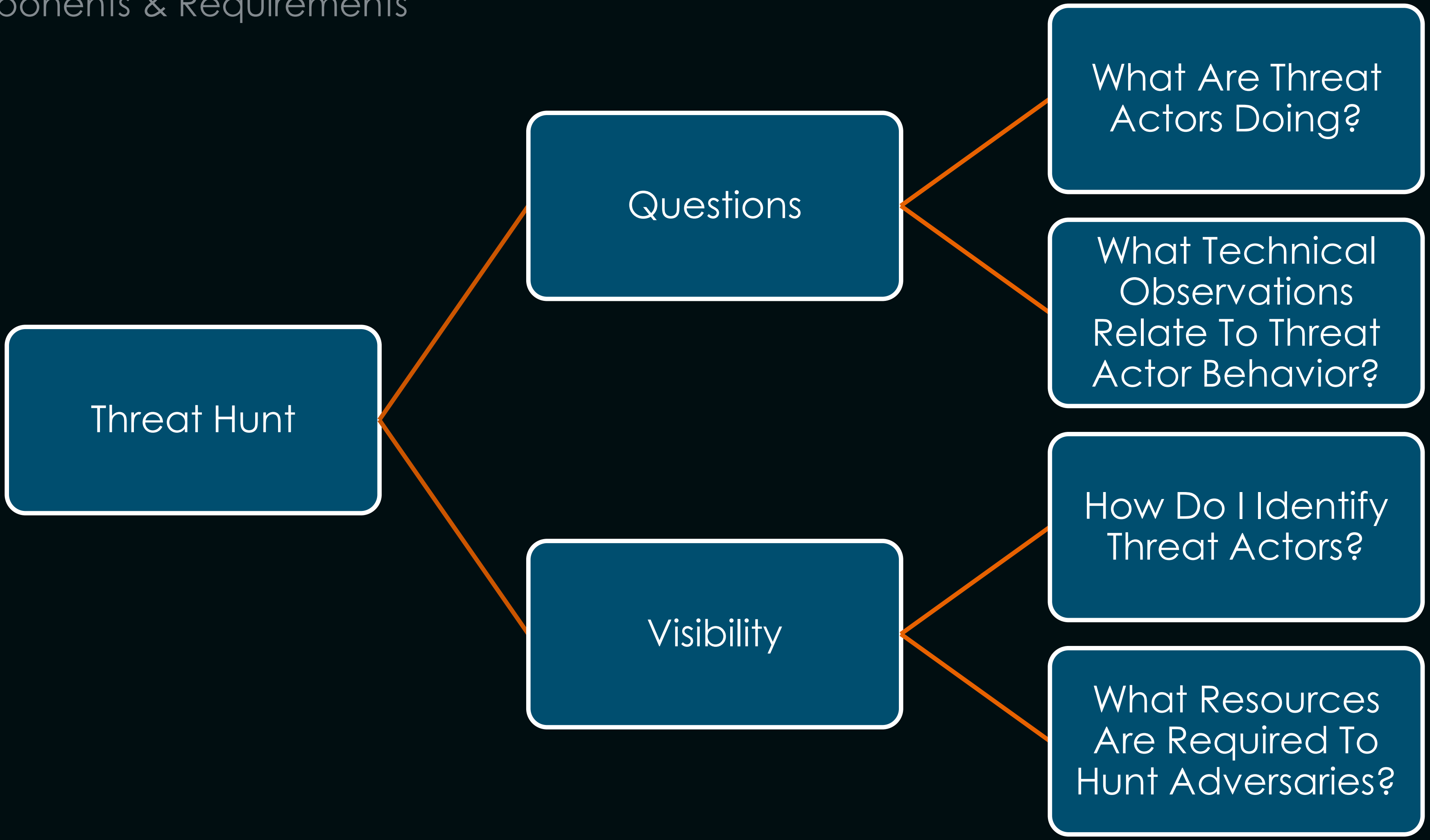
Identify Missed Intrusions!

Support SOC By Identifying Adversaries!

Supplement Automated Detections Through Interactive Search!

Threat Hunting Components

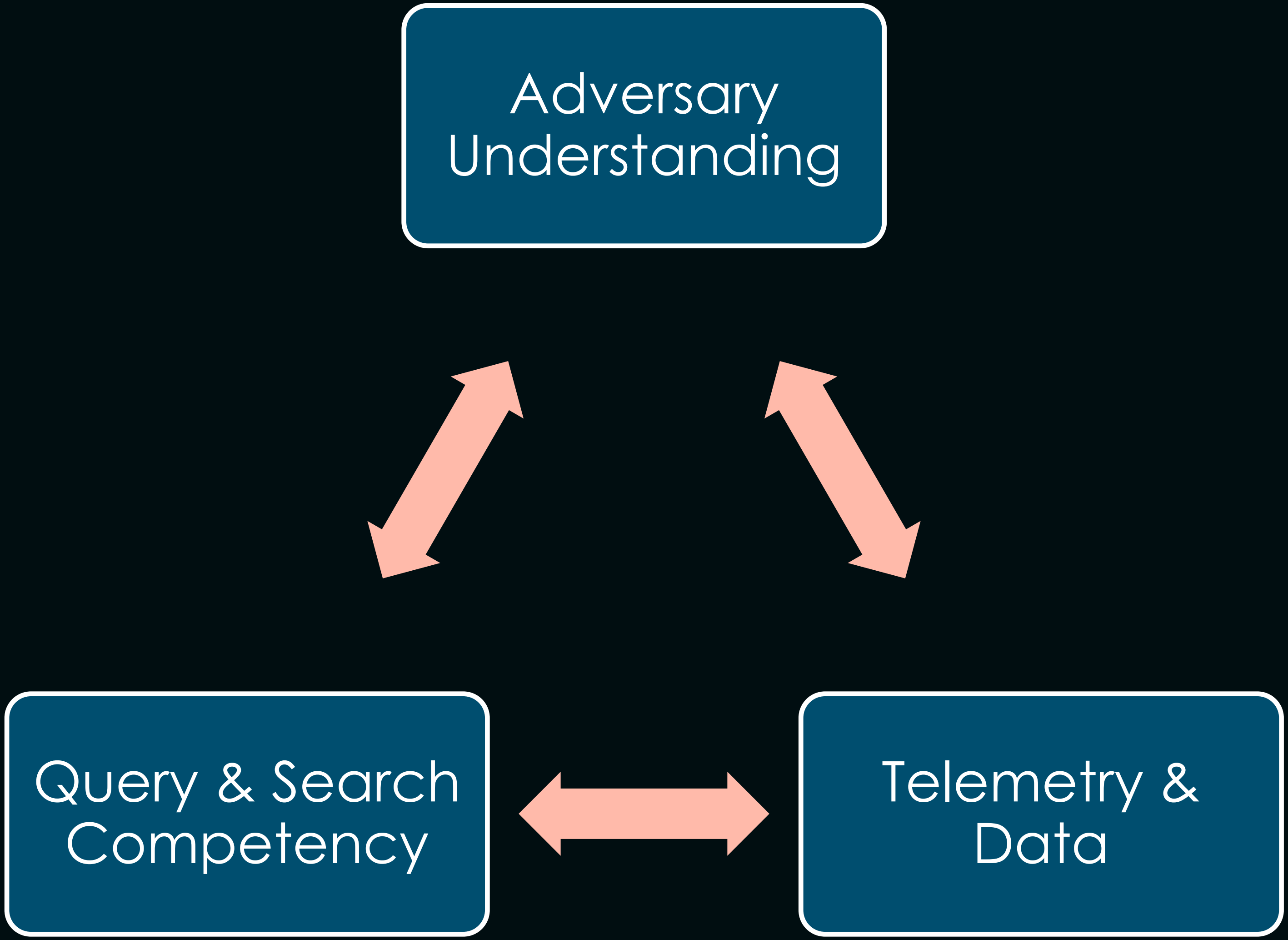
Hunting Components & Requirements



Threat Hunt
Questions
Visibility
What Are Threat Actors Doing?
What Technical Observations Relate To Threat Actor Behavior?
How Do I Identify Threat Actors?
What Resources Are Required To Hunt Adversaries?

Pre-Requisites For Hunting

Hunting Components & Requirements



Adversary Understanding

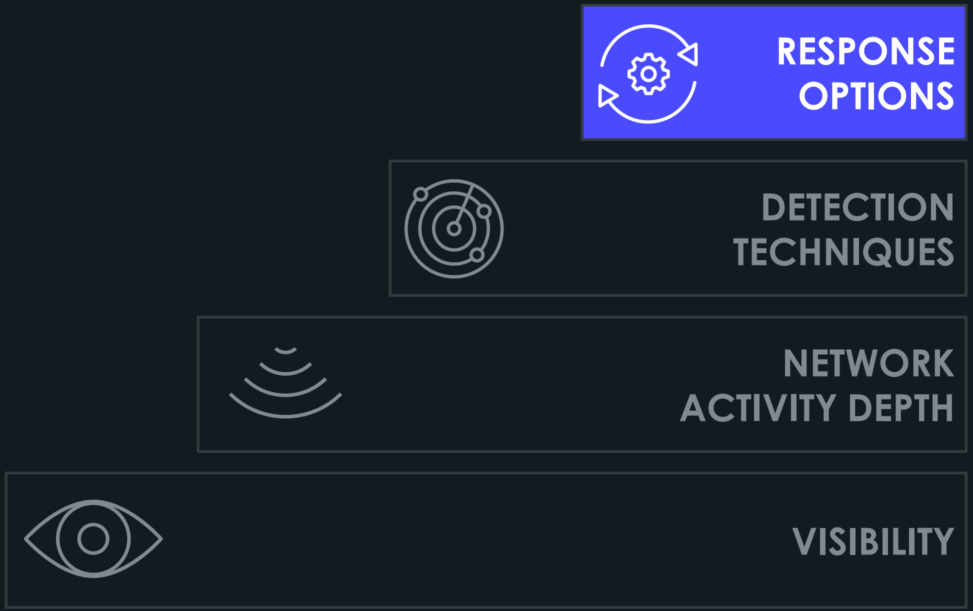
Query & Search Competency

Telemetry & Data

Technology Components

Response

- Triage / Validation With Confidence
- Threat Hunting / Conclusive Investigations
- Guided Response Actions
- Integrations



RESPONSE OPTIONS

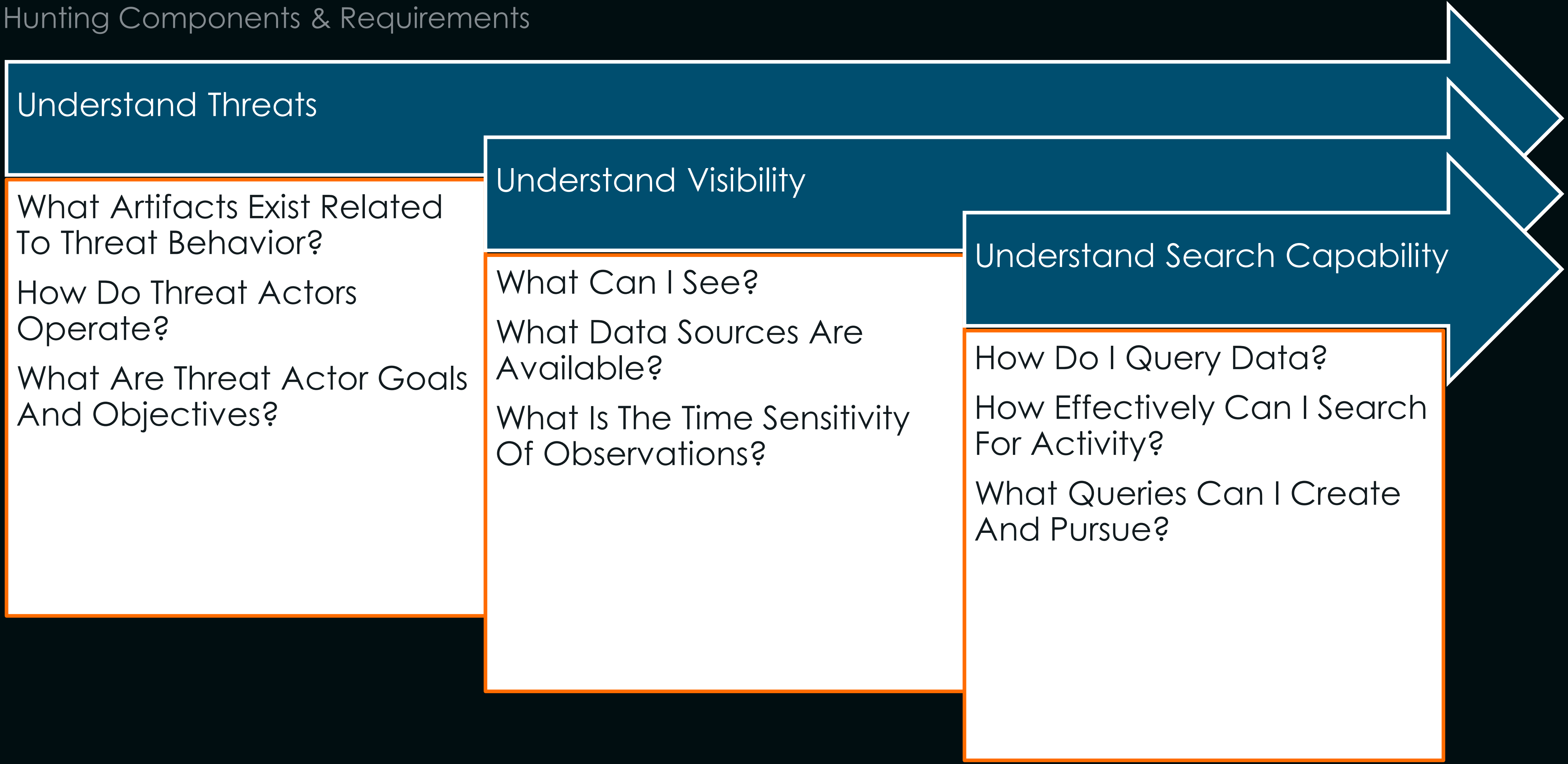
DETECTION TECHNIQUES

NETWORK ACTIVITY DEPTH

VISIBILITY

Data & Understanding

Hunting Components & Requirements



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

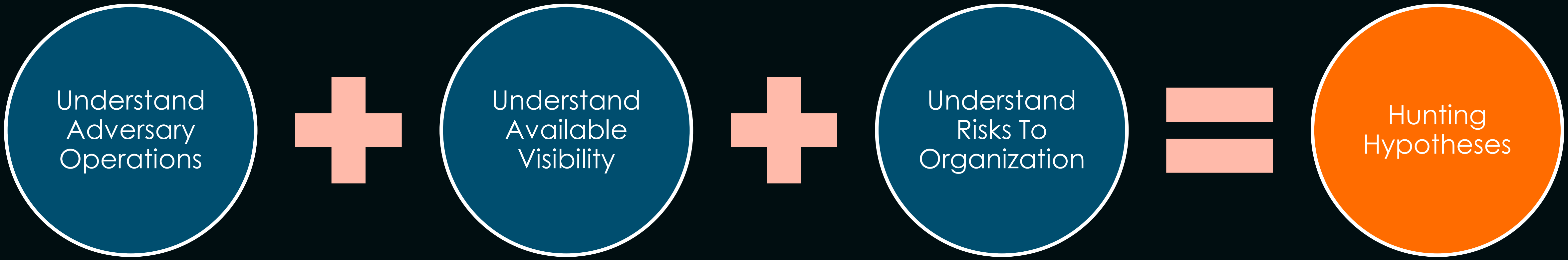
How Do I Query Data?

How Effectively Can I Search For Activity?

What Queries Can I Create And Pursue?

Developing A Realistic Model

Devising A Hunting Methodology



Understand Adversary Operations

+

Understand Available Visibility

+

Understand Risks To Organization

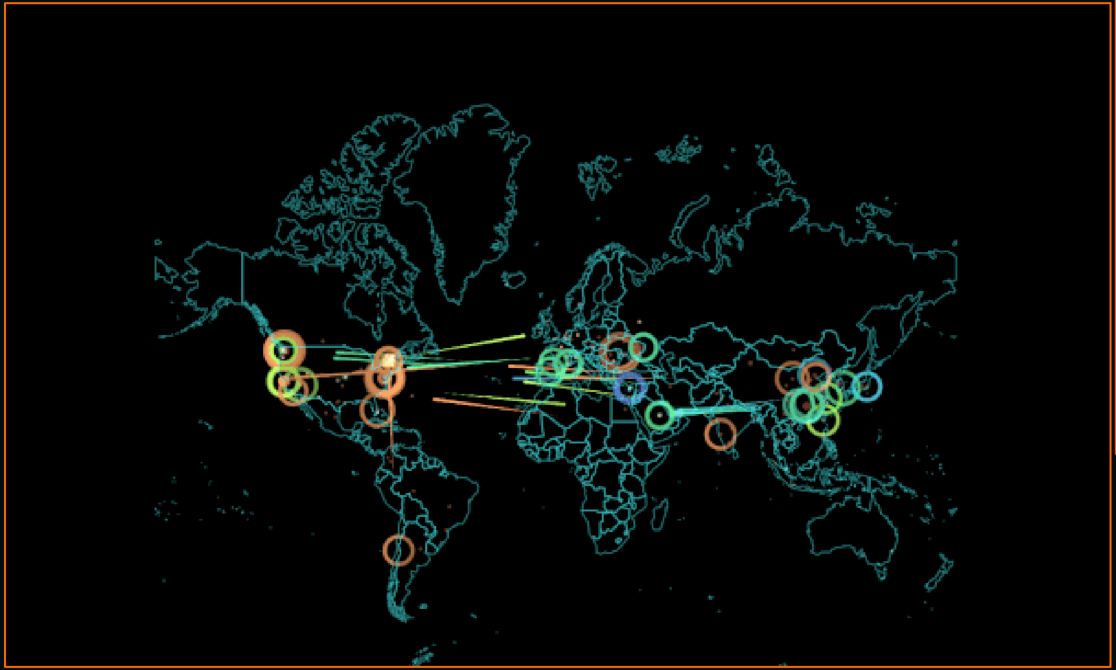
=

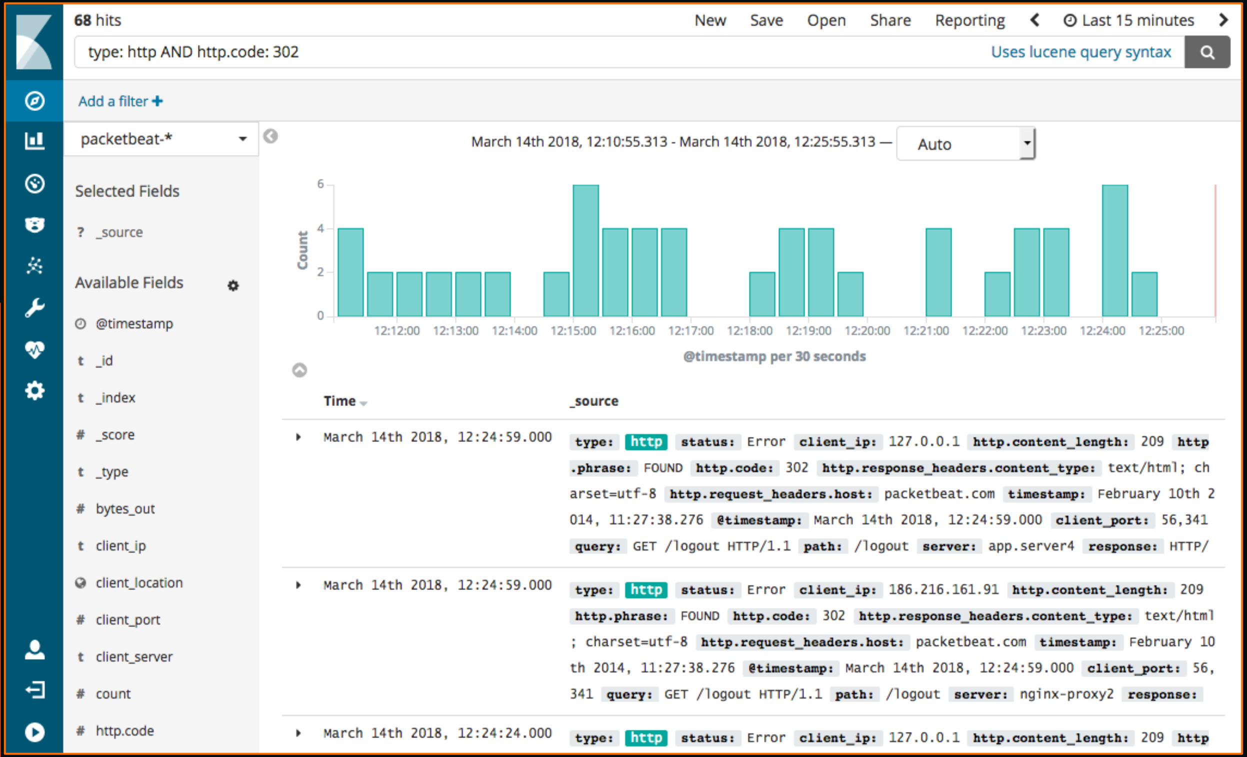
Hunting Hypotheses

Visibility & Telemetry

Devising A Hunting Methodology

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





68 hits

type: http AND http.code: 302

packetbeat-*

March 14th 2018, 12:10:55.313 - March 14th 2018, 12:25:55.313 —

Selected Fields

- ? _source

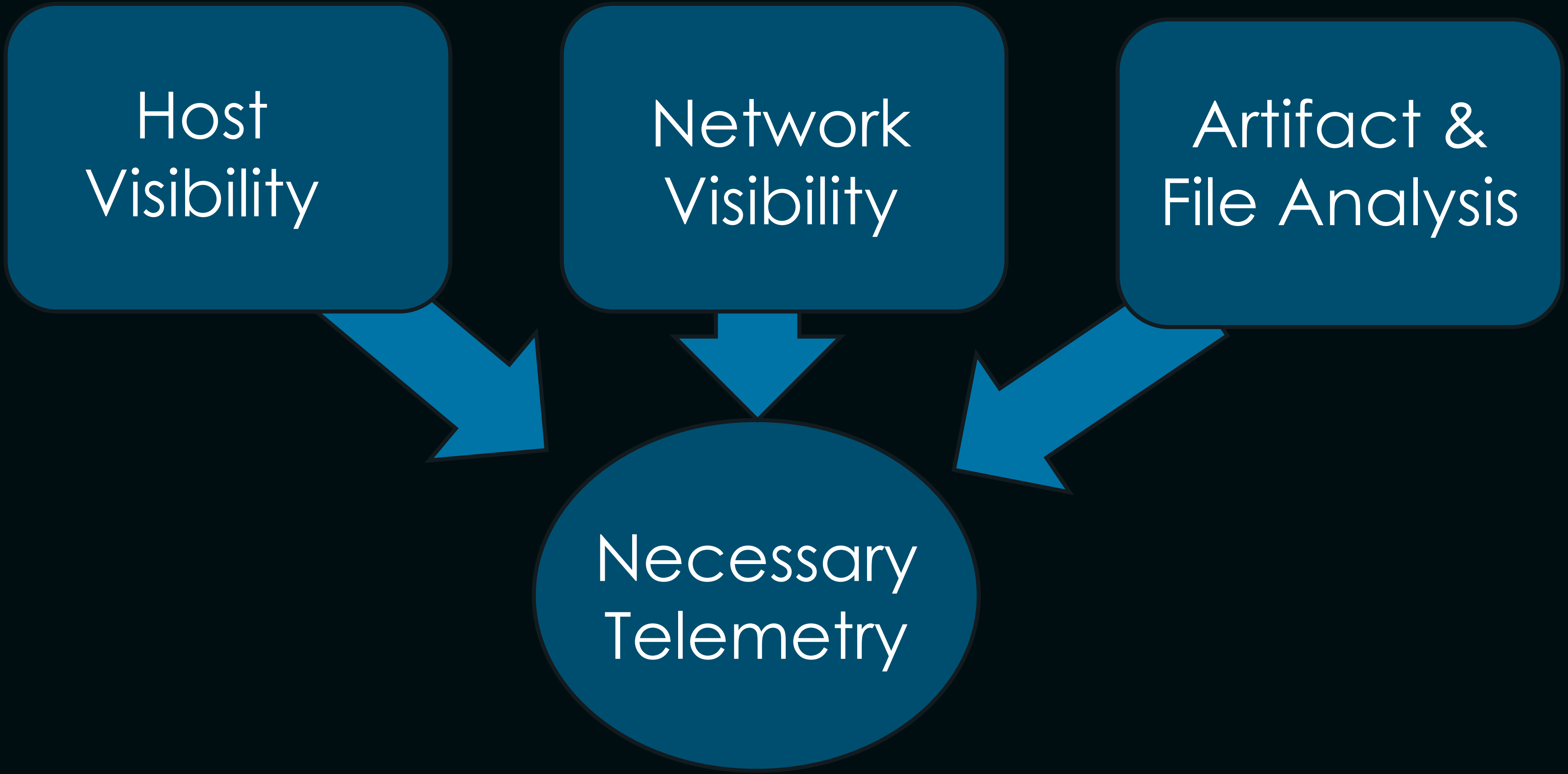
Available Fields

- @timestamp
- t _id
- t _index
- # _score
- t _type
- # bytes_out
- t client_ip
- client_location
- # client_port
- t client_server
- # count
- # http.code

```
Time      _source

March 14th 2018, 12:24:59.000   type: http status: Error client_ip: 127.0.0.1 http.content_length: 209 http
                                .phrase: FOUND http.code: 302 http.response_headers.content_type: text/html; ch
                                arset=utf-8 http.request_headers.host: packetbeat.com timestamp: February 10th 2
                                014, 11:27:38.276 @timestamp: March 14th 2018, 12:24:59.000 client_port: 56,341
                                query: GET /logout HTTP/1.1 path: /logout server: app.server4 response: HTTP/

March 14th 2018, 12:24:59.000   type: http status: Error client_ip: 186.216.161.91 http.content_length: 209
                                http.phrase: FOUND http.code: 302 http.response_headers.content_type: text/html
                                ; charset=utf-8 http.request_headers.host: packetbeat.com timestamp: February 10
                                th 2014, 11:27:38.276 @timestamp: March 14th 2018, 12:24:59.000 client_port: 56,
                                341 query: GET /logout HTTP/1.1 path: /logout server: nginx-proxy2 response:

March 14th 2018, 12:24:24.000   type: http status: Error client_ip: 127.0.0.1 http.content_length: 209 http
```

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

Pillars Of Visibiity



Compensating For Visibility Gaps

Devising A Hunting Methodology

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

Thank you

Matthew.Plummer@Gigamon.com