CWL
CyberWarFare Labs

# UNVEILING THREAT LANDSCAPES

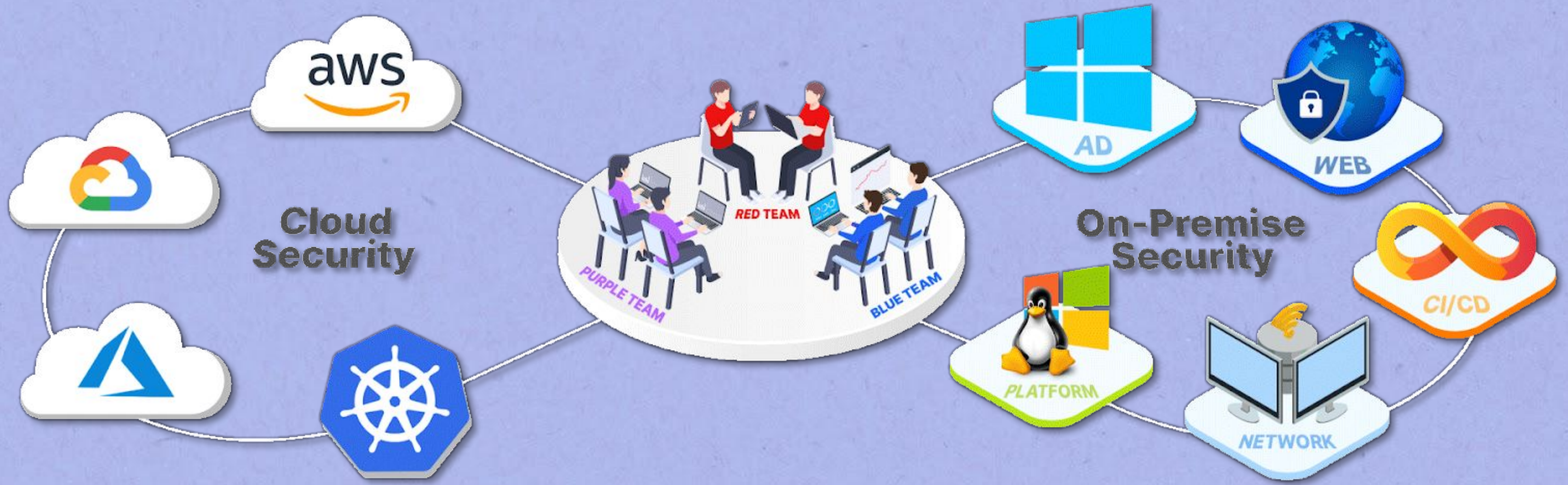
## Pivoting Through Indicators

WWW.CYBERWARFARE.LIVE

## ABOUT CYBERWARFARE LABS :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform



INFINITE LEARNING EXPERIENCE

# About Speaker

## Harisuthan S

**Senior Security Engineer**

Blue Team Security researcher, bringing over 3+ years of experience in cyber defense. possesses a deep understanding of Blue Team methodologies including investigation and detection over cyber attacks.

# Agenda

The Transformation of Security Teams

Threat Hunting vs Threat Intel

IOC vs IOB vs IOA

Pivoting Through Indicators

# The Transformation of Security Teams

**From Reactive to Proactive**

### Security Operations Center (SOC)

Monitor, detect, respond to, and investigate security incidents in real-time.

### Incident Response (IR) Team

Actively responds to security breaches and coordinates containment, eradication, and recovery

### Threat Intelligence Team

Collect, analyze, and share threat data to help predict and defend against attacks.

### Threat Hunting Team

Hunt for hidden backdoors and APT

### Digital Forensics Team

Investigate digital evidence to support incident response or legal actions

# Detection methods are techniques

Detection methods are techniques or tools used to identify suspicious or malicious activities in systems, networks, or applications.

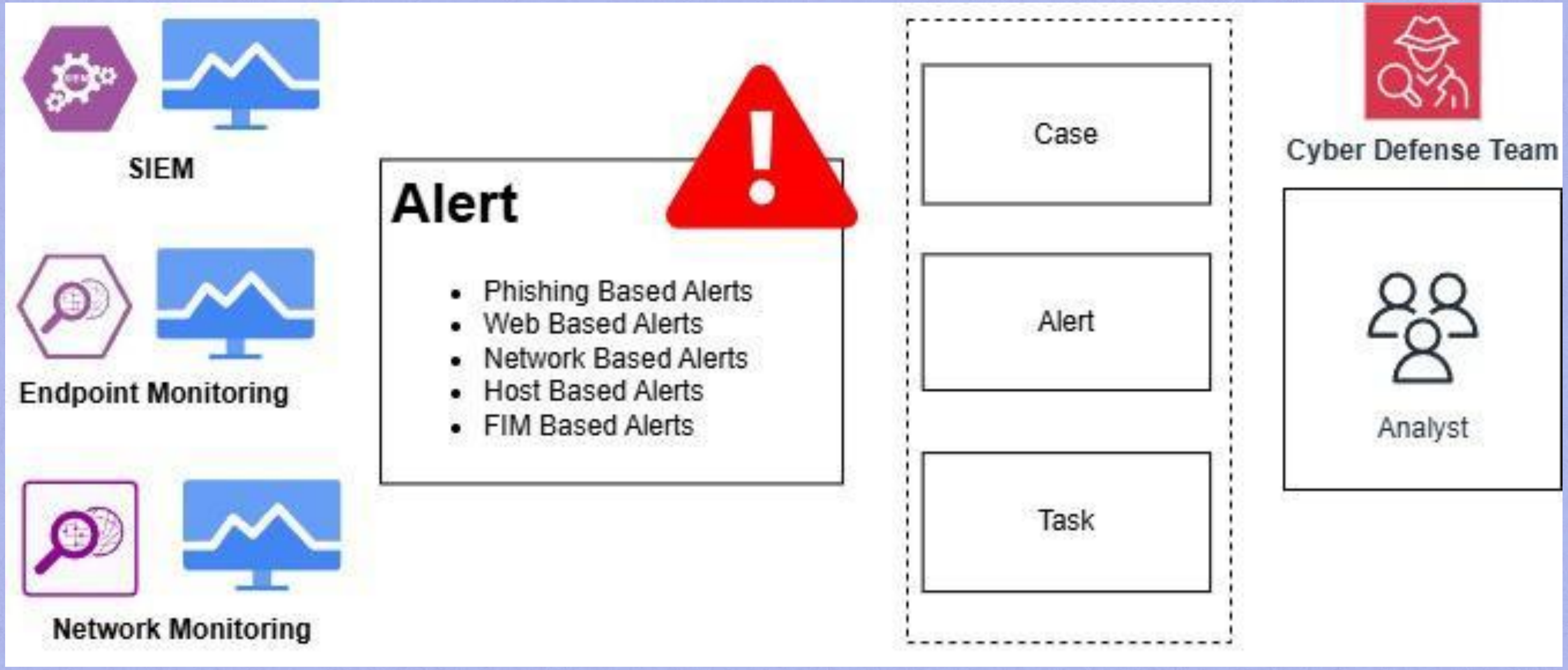
Rule-Based Detection

Heuristic/Behavioral Based Detection

Threat Intelligence Based Detection

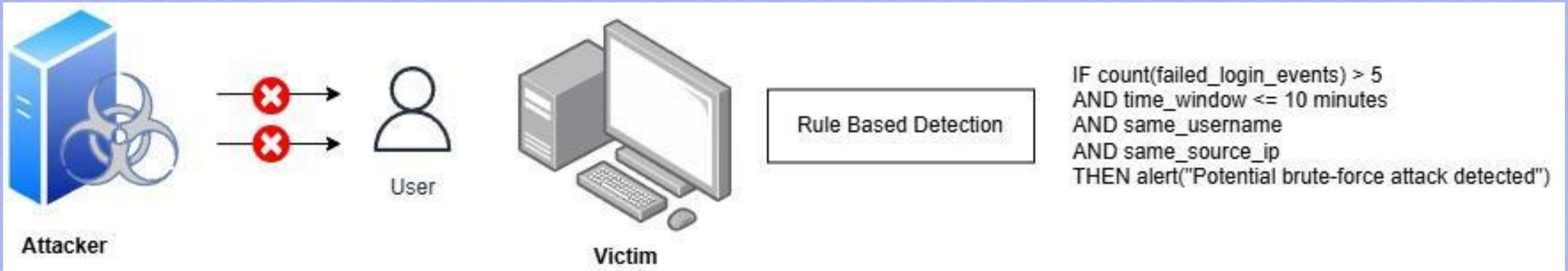
# Rule-Based Detection

Uses predefined rules or logic (often in SIEMs or SOARs) to flag suspicious activity.



- Phishing Based Alerts
- Web Based Alerts
- Network Based Alerts
- Host Based Alerts
- FIM Based Alerts

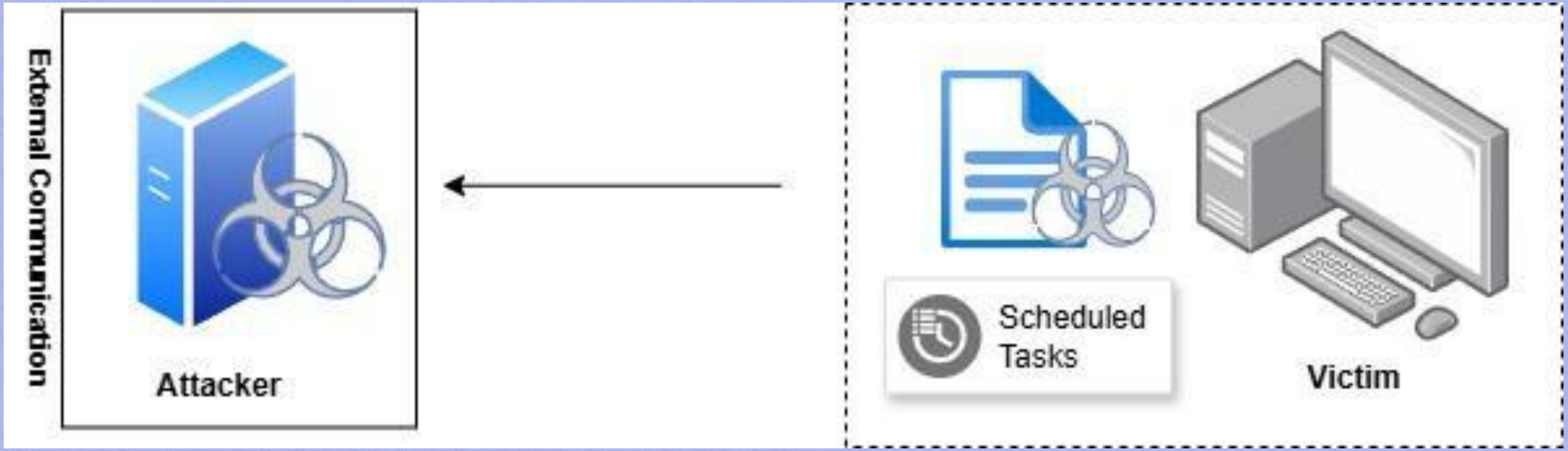
# Rule-Based Detection



```
IF count(failed_login_events) > 5
AND time_window <= 10 minutes
AND same_username
AND same_source_ip
THEN alert("Potential brute-force attack detected")
```

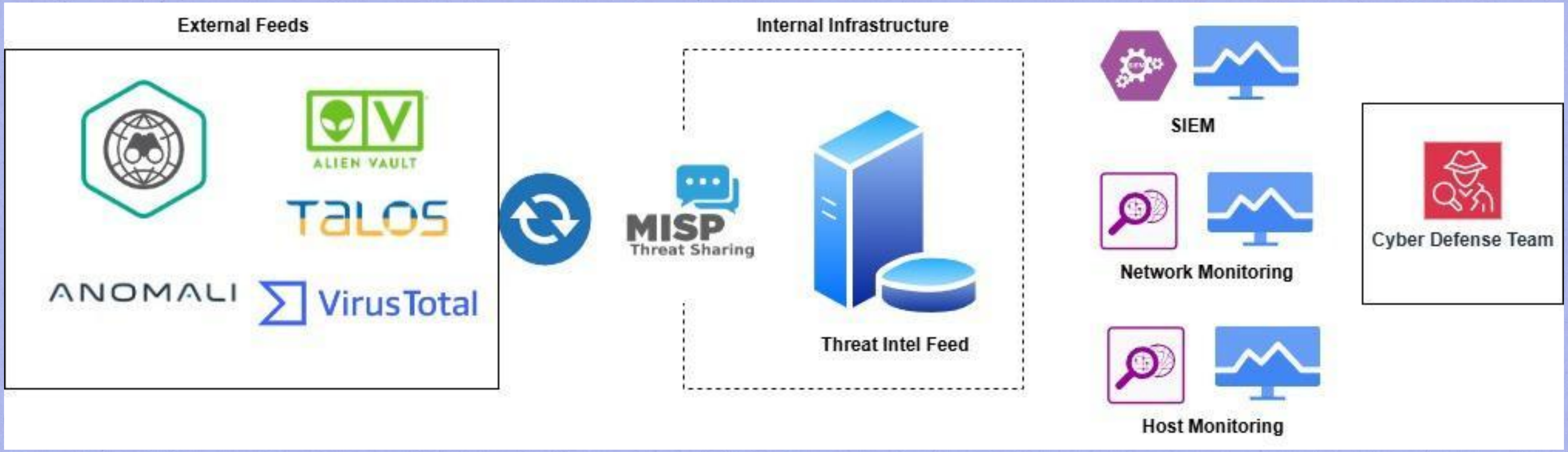
# Heuristic/Behavioral Based Detection

Uses rules or algorithms to detect suspicious behavior patterns.

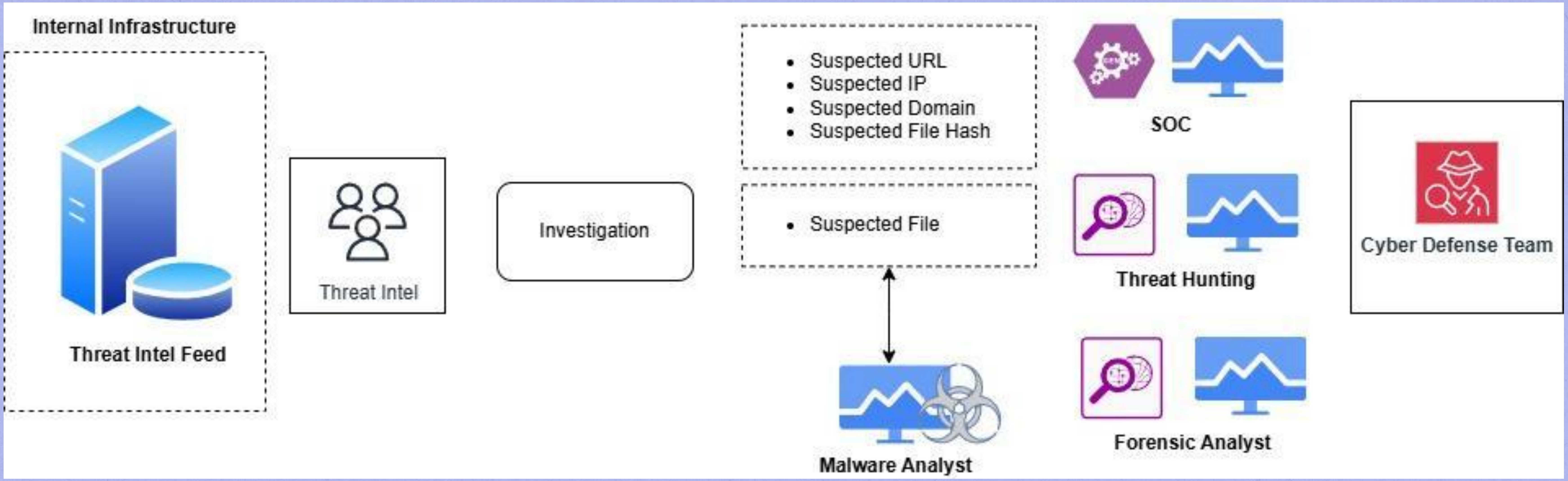


# Threat Intelligence Based Detection

Uses rules or algorithms to detect suspicious behavior patterns.



# Threat Intelligence Based Detection



# IOC vs IOB vs IOA

### Indicator Of Compromise

An Indicator of Compromise (IOC) is a forensic artifact or piece of data that suggests that a system may have been breached or is under attack.

### Indicator Of Behavior

An Indicator of Behavior (IOB) is a high-fidelity signal based on the actions or behavior patterns of an attacker, rather than static artifacts like file hashes or IP addresses

### Indicator Of Attack

An Indicator of Attack (IOA) is a pattern of behavior or sequence of actions that reveals an attacker’s intent, even before the system is fully compromised

# Types Of IOC

Indicators of Compromise (IOCs) are pieces of forensic data that identify potentially malicious activity on a system or network. They help security teams detect, investigate, and respond to breaches. Common types include:

- Network IOCs
- File-Based IOCs
- Host-Based IOCs
- Email-Based IOCs

# Network IOCs

These relate to communication between the compromised host and external entities.

- IP addresses (e.g., known C2 servers)
- Domain names (malicious or suspicious)
- URLs (malicious links, phishing pages, etc.)
- HTTP Host headers
- Unusual traffic patterns (e.g., beaconing behavior)

# File-Based IOCs

These point to files that are known to be malicious or suspicious.

File hashes (MD5, SHA1, SHA256)

File names (e.g., invoice.exe, svch0st.bat)

File paths (e.g., C:\Users\Public\)

File size anomalies

File signatures (mismatched or unsigned binaries)

# Host-Based IOCs

These relate to communication between the compromised host and external entities.

Processes and parent-child process relationships

Registry keys (Windows-specific persistence mechanisms)

Scheduled tasks or services

Startup folder artifacts

# Email-Based IOCs

Commonly associated with phishing or malware-laden emails.

Sender email addresses

Subject lines or keywords

Malicious attachments (e.g., .exe, .js, .xlsm)

Links inside email bodies

Email headers or SMTP metadata

# Indicator Of Behavior

Indicators of Behavior (IOBs) are observable patterns or sequences of actions that adversaries perform during an attack — not just artifacts like file hashes or IPs (which are IOCs), but behavioral clues that suggest malicious intent, even if the specific tools or infrastructure vary.

Multiple failed login attempts followed by a successful login

Use of living-off-the-land binaries (LOLBins), like: rundll32.exe, mshta.exe, certutil.exe

Command-line tools launched with base64-encoded commands

Scheduled task creation or abuse of Windows Management Instrumentation (WMI)

Large data transfers to external IPs or over non-standard ports (e.g., TCP 4444)

Registry changes for autorun programs (e.g., HKCU\Software\Microsoft\Windows\CurrentVersion\Run)

# Pivoting Through Indicators

| LockBit | BlackCat (ALPHV) | Cl0p |
|---|---|---|
| Type: Ransomware-as-a-Service (RaaS) | Type: Ransomware-as-a-Service (RaaS) | Type: Ransomware + Data Extortion |
| IP: 185.172.128.10 | IP: 185.225.69.69 | IP: 185.141.63.120 |
| lockbitblog[.]com | HKCU\Software\BlackCat<br>HKLM\SYSTEM\ControlSet001\Services\BlackCatService | 3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207 |
| http://lockbitapt2[.]xyz/login.php | f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb | 3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207 |

# Why Indicators Matter in Threat Detection

### 01 Early Detection Capabilities

Early detection of threats is crucial for minimizing the impact of cyberattacks. One effective way to achieve this is by leveraging Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).

### 02 Faster Response Times

Compared to rule-based detection, indicators offer a faster and more responsive approach to identifying threats early.

### 03 Informed Decision-Making

Indicators play a critical role in enabling informed and timely decision-making during threat detection and response.

### 04 Proactive Defense

Indicators are not just for post-incident analysis—they are powerful tools for building a proactive defense strategy that helps detect and disrupt threats before they cause harm.

# Drawbacks of Relying Solely on Indicators

- Reactive by Nature (Especially IOCs)
- High Risk of False Positives
- Evasion by Attackers
- Lack of Context and Intent
- Limited Use Against Zero-Day or Novel Threats

# THANK YOU

**WWW.CYBERWARFARE.LIVE**