Project Obsidian

CTI 101: Foundations, Tradecraft & Operationalizing Intel

Left of Boom with CTI

Presented by

C4r10x_Z3r0

BLUE TEAM VILLAGE

PROJECT OBSIDIAN

Agenda

- Intel Foundations

-Core concepts & definitions

- Requirements Framework

-Driving intelligence collection

- Intelligence Lifecycle

-Process & methodology

- Structured Models

-Framework application

- Operationalizing Intel

-YARA & Sigma rules

- Threat Intel meets AI

-Practical applications

What is Intelligence?

A Product

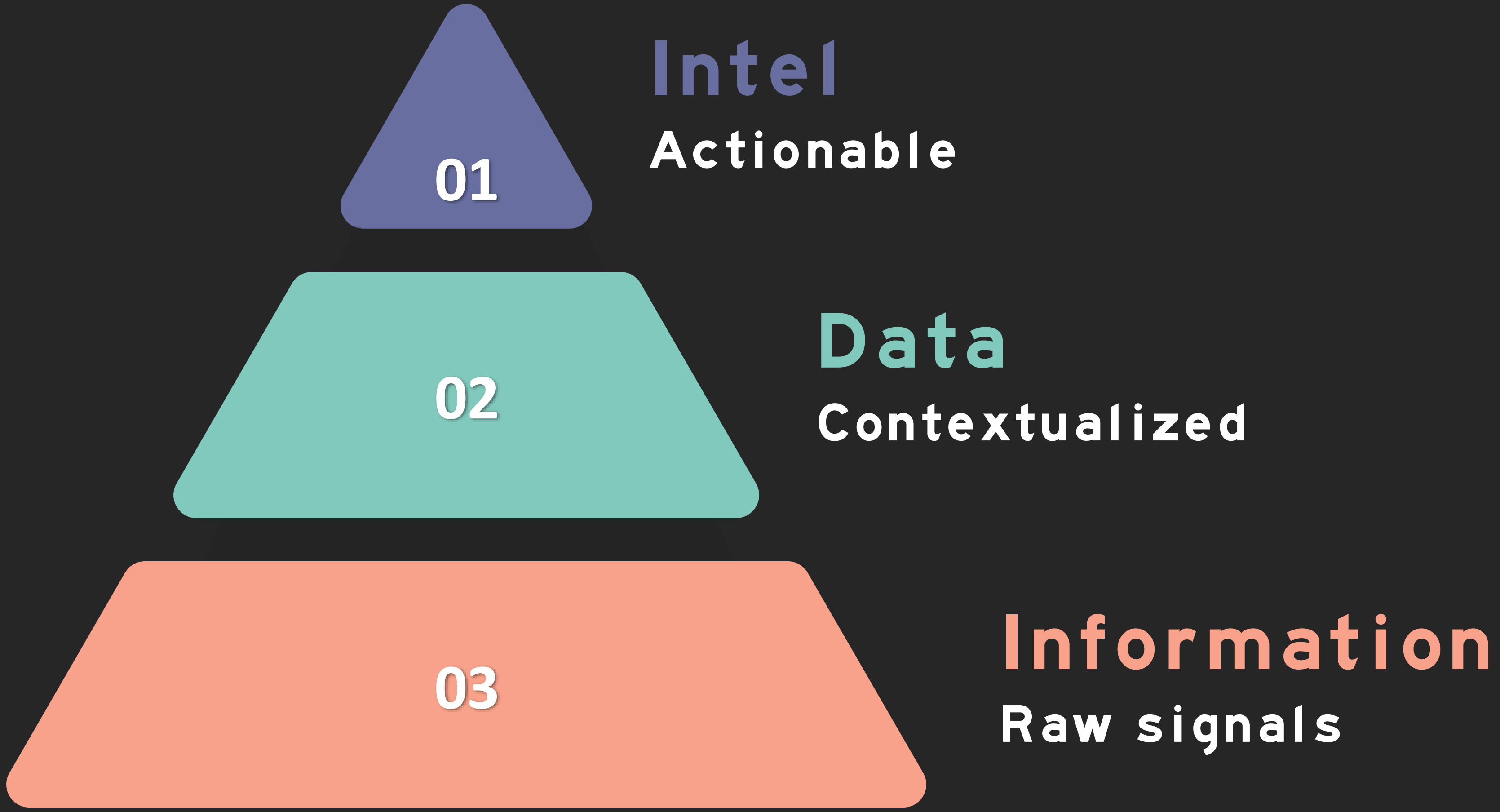
Analyzed information
ready for action

A Process

Methodology to transform
raw data

Intelligence without action is just expensive trivia

Data → Info → Intel Funnel



01 Intel
Actionable

02 Data
Contextualized

03 Information
Raw signals

Threat-Intel Requirements

Priority	Ongoing tracking of key threats
Specific	Targeted inquiry into particular TTPs
Ad-hoc	Emergent needs during incidents

Who Owns Requirements?

SecOps

- Tactical needs
- Detection gaps

Leadership

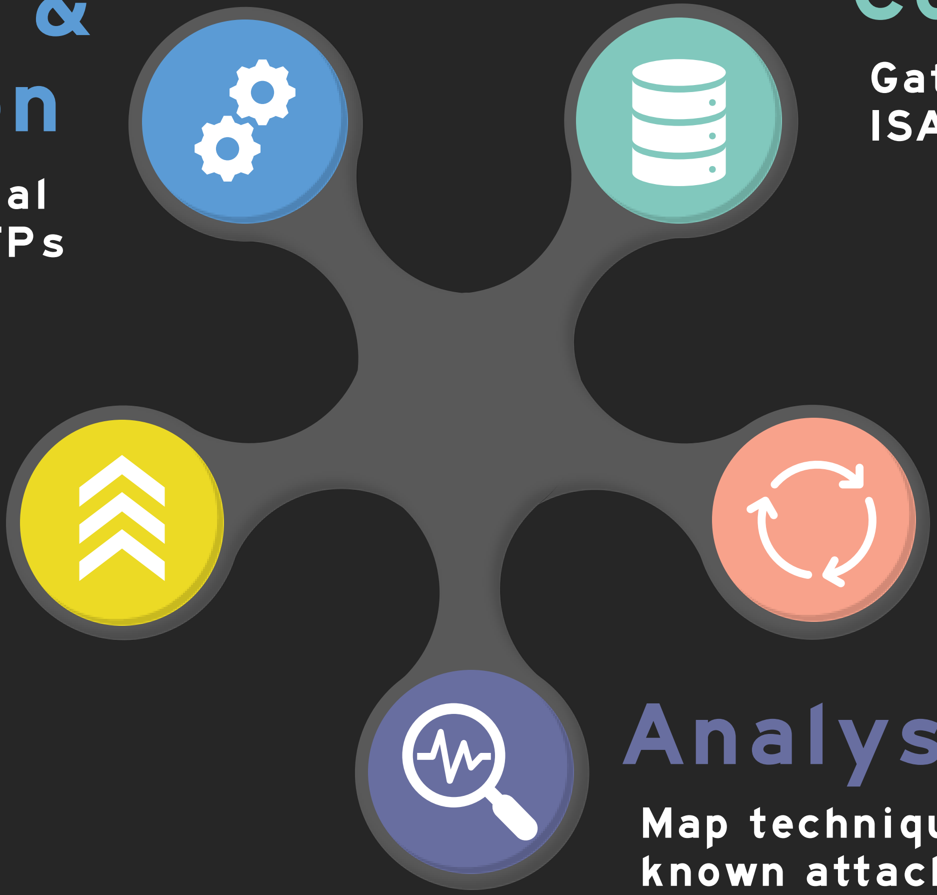
- Strategic direction

Risk tolerance guidance

Analysts

- Technical details
- Collection focus

Intelligence Life-Cycle



Planning & Direction

Identify critical ransomware TTPs

Collection

Gather IOCs from ISAC feeds

Processing and exploitation

De-duplicate and normalize data

Analysis / Production

Map techniques to known attack groups

Dissemination

Deploy detection rules to EDR

Life-Cycle In Action

Planning

Identify critical ransomware TTPs

Collection

Gather IOCs from ISAC feeds

Processing

De-duplicate and normalize data

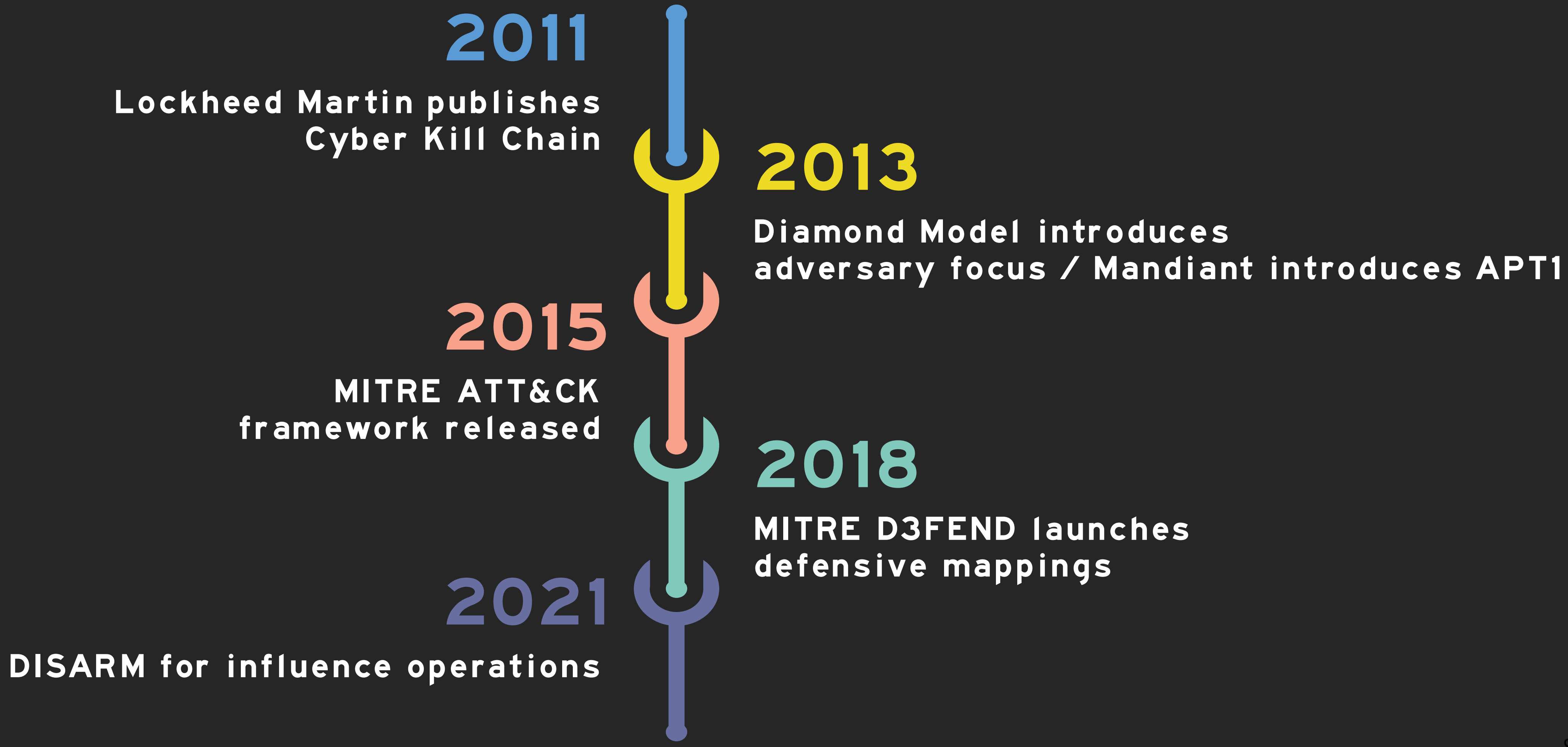
Analysis

Map techniques to known attack groups

Dissemination

Deploy detection rules to EDR

Structured Models = Buckets



2011

Lockheed Martin publishes
Cyber Kill Chain

2013

Diamond Model introduces
adversary focus / Mandiant introduces APT1

2015

MITRE ATT&CK
framework released

2018

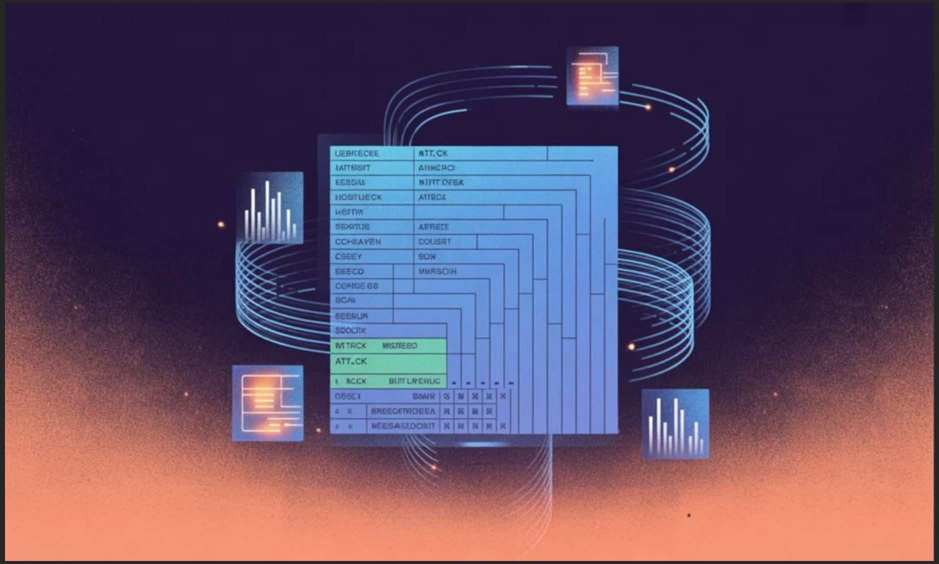
MITRE D3FEND launches
defensive mappings

2021

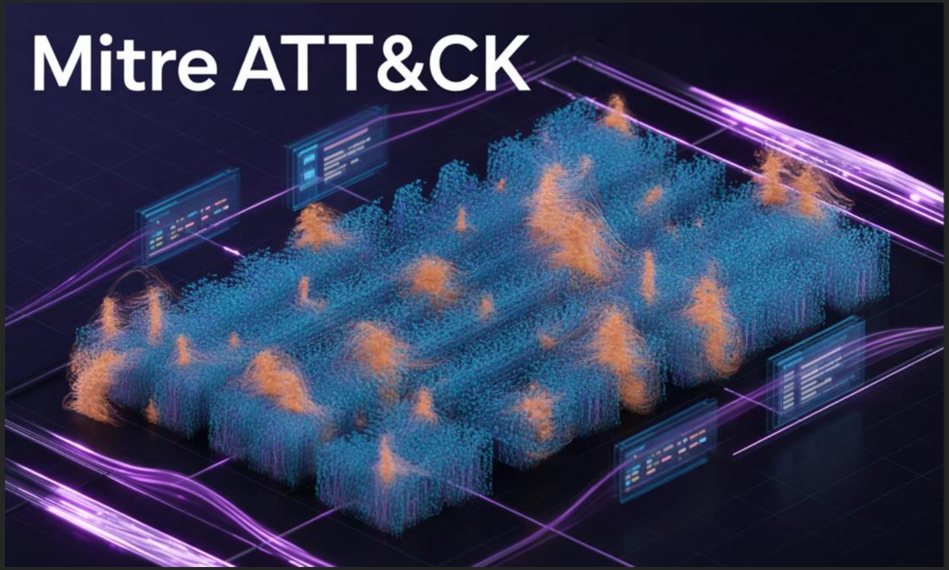
DISARM for influence operations

MITRE ATT&CK Heat-Map Mini-Exercise

Before Analysis



After Intelligence



Mapping observed behaviors reveals adversary patterns

Transition to Operationalizing Intel

Intel that never hits a sensor is trivia

1. **Intelligence Reports**
   Written analysis only
2. **Detection Rules**
   Automated alerting
3. **Active Hunting**
   Proactive discovery

YARA 101

Anatomy

- Meta: author, description
- Strings: patterns to match
- Condition: logical operators

```
rule Ransomware_Mutex {
meta:    author = "CTI Team"
strings:    $mutex =
"Global\\MsWinZonesCacheCoun
terMutexA"
condition:    $mutex}
```

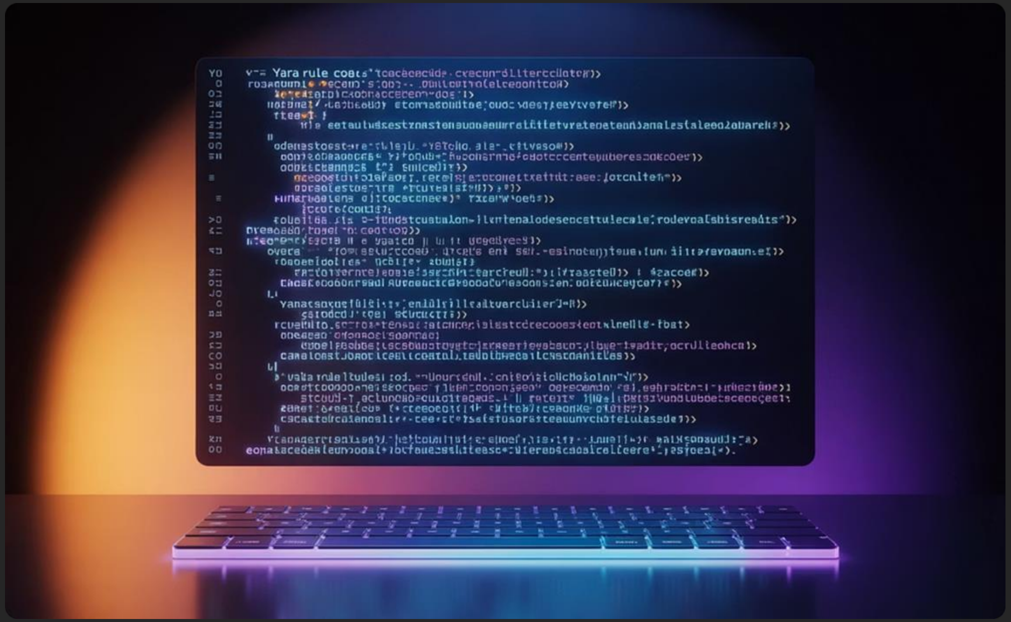
Sigma 101

Key YAML Fields

- title, description
- status, level
- logsource details
- detection conditions
- falsepositives notes

```
title: Suspicious PowerShell
Downloadid: 5fd1e8cd-d5c0-4a1c-
b3ac-5045a10b01dfstatus:
experimentalauthor: CTI
Teamtags:   - attack.execution
- attack.t1059.001logsource:
product: windows  service:
powershelldetection:
selection:    EventID: 4104
ScriptBlockText|contains:
- "DownloadString"       -
"WebClient"  condition:
selectionfalsepositives:  -
Legitimate admin scriptslevel:
medium
```

YARA vs Sigma



YARA

- Targets files & memory
- Pattern matching
- Hunting & response

Sigma

- Targets logs
- SIEM integration
- Detection & alerting

Knowing Normal to Find Evil

Establish Baselines

Document normal behaviors, traffic patterns, and system activities before you can effectively identify malicious anomalies.

Context is Critical

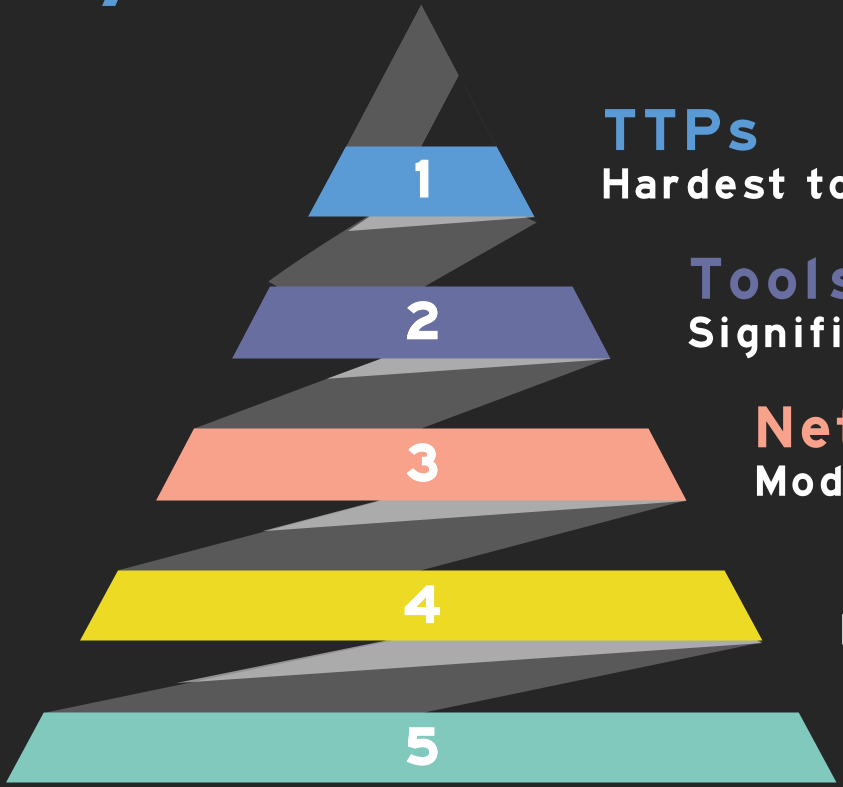
What appears suspicious in one environment may be perfectly normal in another. Environmental awareness drives accurate detection.

Continuous Learning

As environments evolve, your understanding of "normal" must adapt. Regular baselining prevents alert fatigue and false positives.

Adversaries hide in the noise. Only by understanding the baseline can we separate signal from noise.

Pyramid of Pain → Why TTP-Level Rules Matter



TTPs
Hardest to change

Tools
Significant effort

Network/Host Artifacts
Moderate effort

Domain Names
Minor inconvenience

IP Addresses & Hash Values
Trivial to change

When we detect and block at the TTP level (using YARA and Sigma rules), we force adversaries to completely change their methodologies—not just their infrastructure. This creates maximum defensive impact and return on investment.

The higher you can disrupt in the pyramid, the more pain you cause the adversary.

Indicator Sources & Threat Intelligence Platforms

Open Source Platforms

- MISP (Malware Information Sharing Platform)
- Open Threat Exchange (OTX)

- Feedly Threat Intelligence
- ThreatConnect

These platforms aggregate indicators from multiple sources, enabling teams to collect, share, and collaborate on threat data in standardized formats.

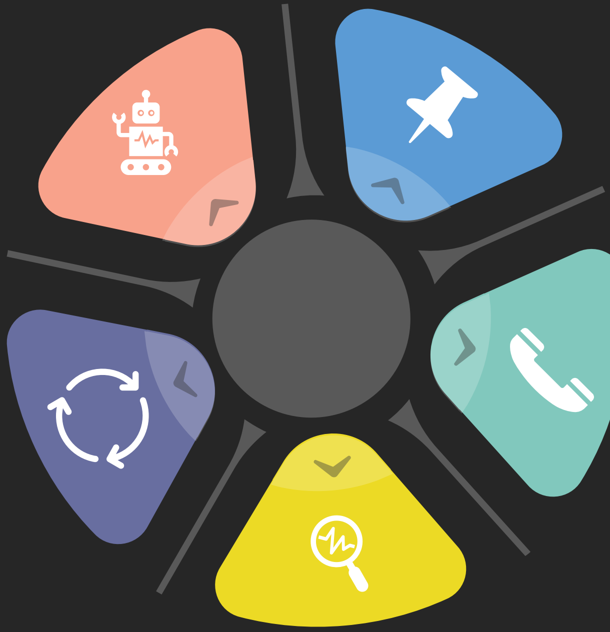
Commercial Solutions

- Anomali ThreatStream
- Recorded Future
- Mandiant Advantage
- CrowdStrike Intelligence

Commercial TIPs provide enriched context, automated workflows, and integration capabilities that transform raw indicators into actionable intelligence.

The value isn't in the indicators themselves, but in how you contextualize, prioritize, and operationalize them across your security stack.

The Fusion Wheel: Integrating Security Functions



Threat Intelligence (TI)

Informs detection rules, enriches context, and feeds hunting and incident response efforts. Draws from OSINT, commercial feeds, and internal telemetry.

Threat Hunting (TH)

Detects unknown threats by establishing baselines and identifying anomalies ("knowing normal to find evil"). Leverages Sigma/YARA rules, Chainsaw log analysis, and MFT parsing.

Reverse Engineering (RE)

Deconstructs malware artifacts, binaries, and scripts to feed intelligence and detection development. Supports incident response and root cause analysis.

Incident Response (IR)

Executes playbooks based on identified threats, driven by both TI and Hunting outcomes. Performs investigations on impacted hosts to extract evidence.

Digital Forensics (DF)

Performs in-depth investigations on impacted hosts, extracting evidence to support incident response and reverse engineering efforts.

AI-powered automation amplifies each function—from extracting indicators to suggesting hunting hypotheses, accelerating malware analysis, and predicting attacker movements through behavioral modeling.

When these disciplines collaborate continuously rather than operate in silos, defensive capabilities mature exponentially, creating a force multiplier effect against sophisticated threats.

Purple-Team Validation: Intel-Driven Testing

Operationalizing Intelligence Through Validation

Purple teams merge offensive (red) and defensive (blue) capabilities to validate controls against specific threat actors and TTPs identified by your intelligence program.

Intel Selection

Choose relevant adversary TTPs based on industry targeting and current threat landscape

Scenario Design

Craft exercises emulating specific threat behaviors from your intel sources

Validation

Test effectiveness of YARA, Sigma, and other detection rules in real-time

Purple teaming closes the intelligence feedback loop, proving whether your threat intel translates to actual defensive capability.

Benefits of Intel-Driven Exercises

- Validates detection engineering effectiveness
- Prioritizes control gaps based on real-world threats
- Feeds findings back into intelligence lifecycle
- Demonstrates security ROI through measurable outcomes

CTI 101: Threat Intel Meets AI

Welcome to the Choose Your Own Detection Adventure

Blue Team Village @ DEFCON 33

What is CTI in 2025?

OSINT Collection

Manual gathering from forums, blogs, social media

IOC Feeds

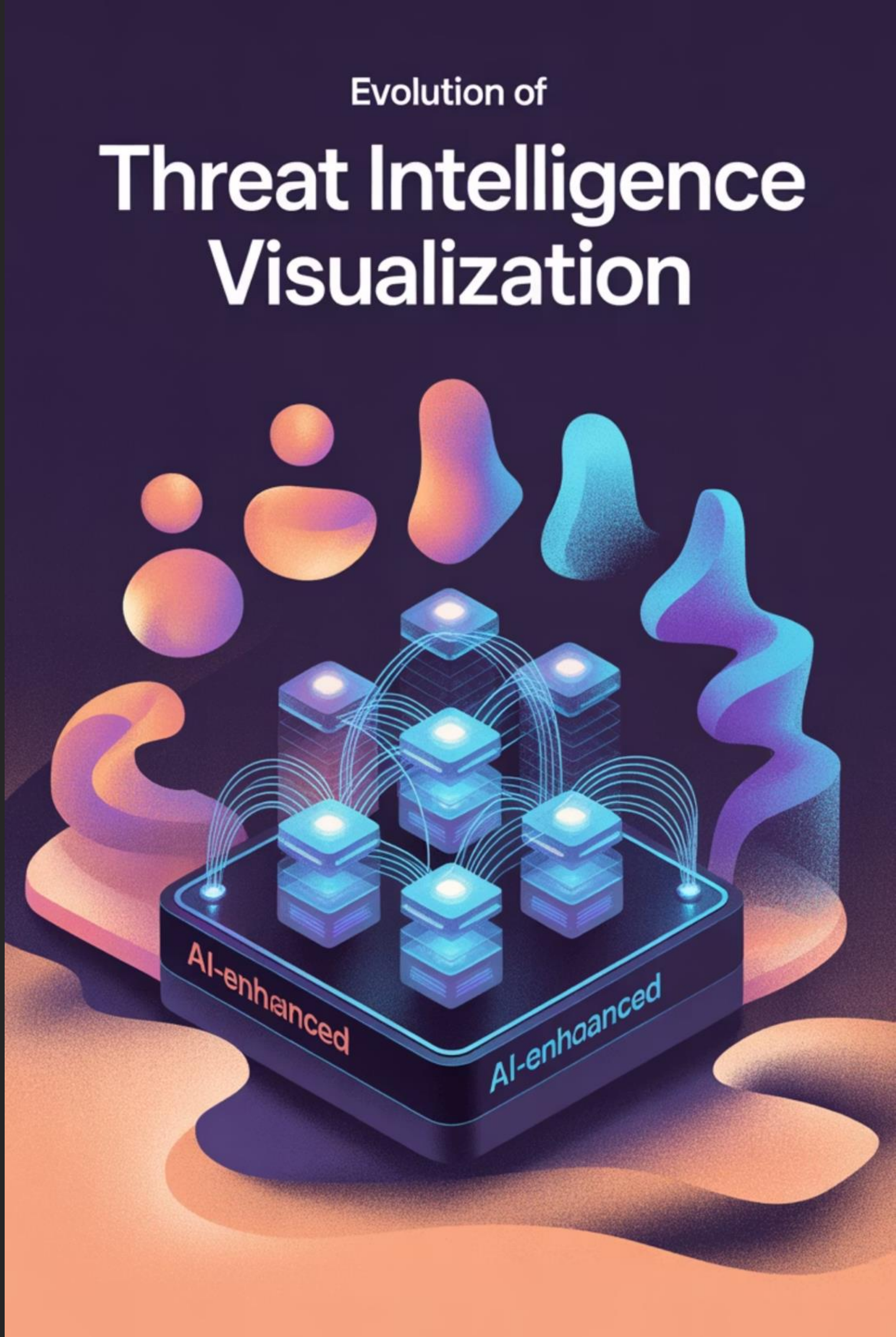
Automated sharing of indicators across platforms

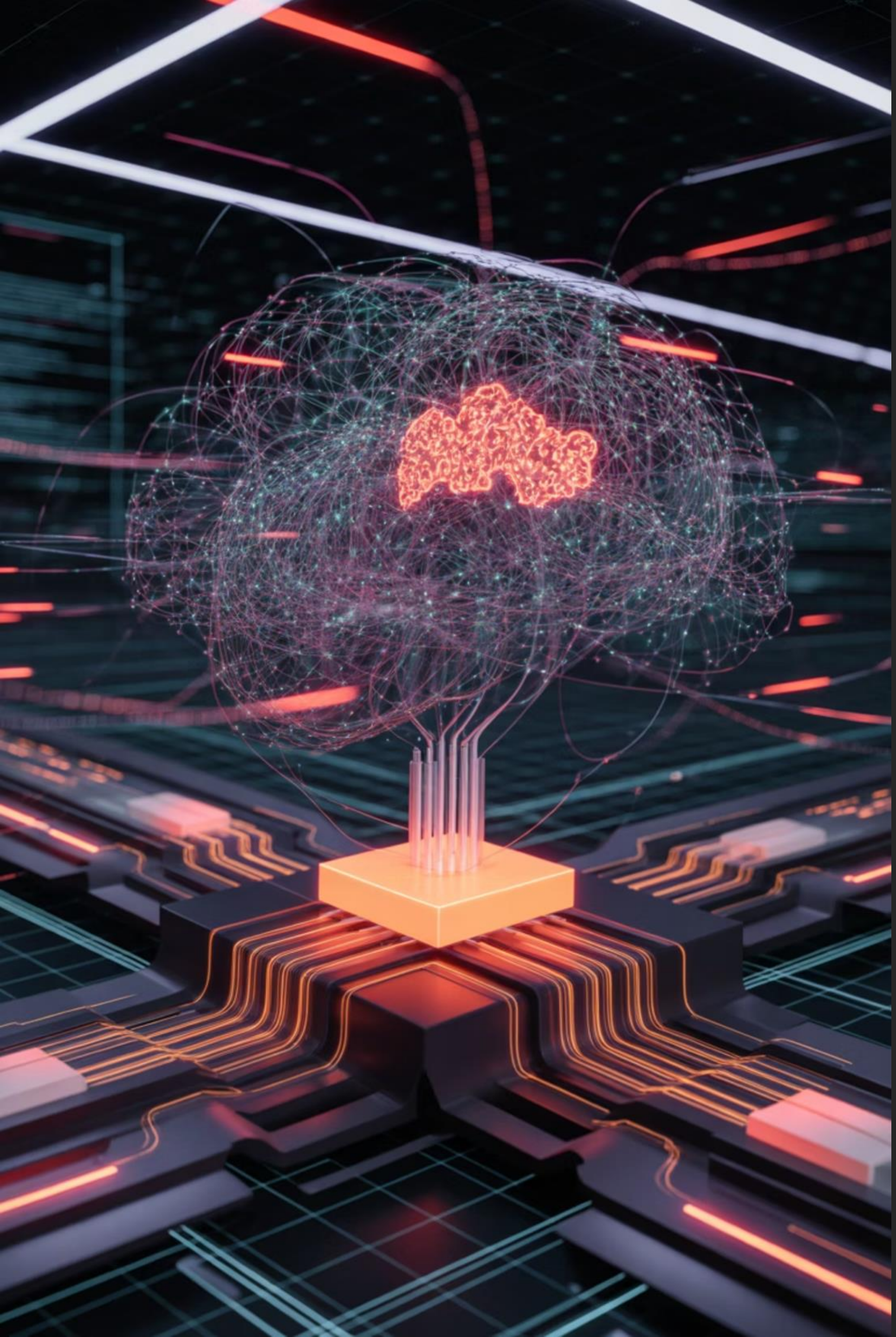
Threat Modeling

Structured analysis of actor behaviors and patterns

AI-driven Intel

Predictive analysis and autonomous detection capabilities





AI's Role in Modern CTI

NLP Processing
Extracts insights from unstructured threat reports

Anomaly Detection
Identifies outliers in network traffic patterns

ML Clustering
Groups related incidents by TTPs

LLM Enhancements
Recognizes sophisticated phishing content

Choose Your Adventure

Initial Detection

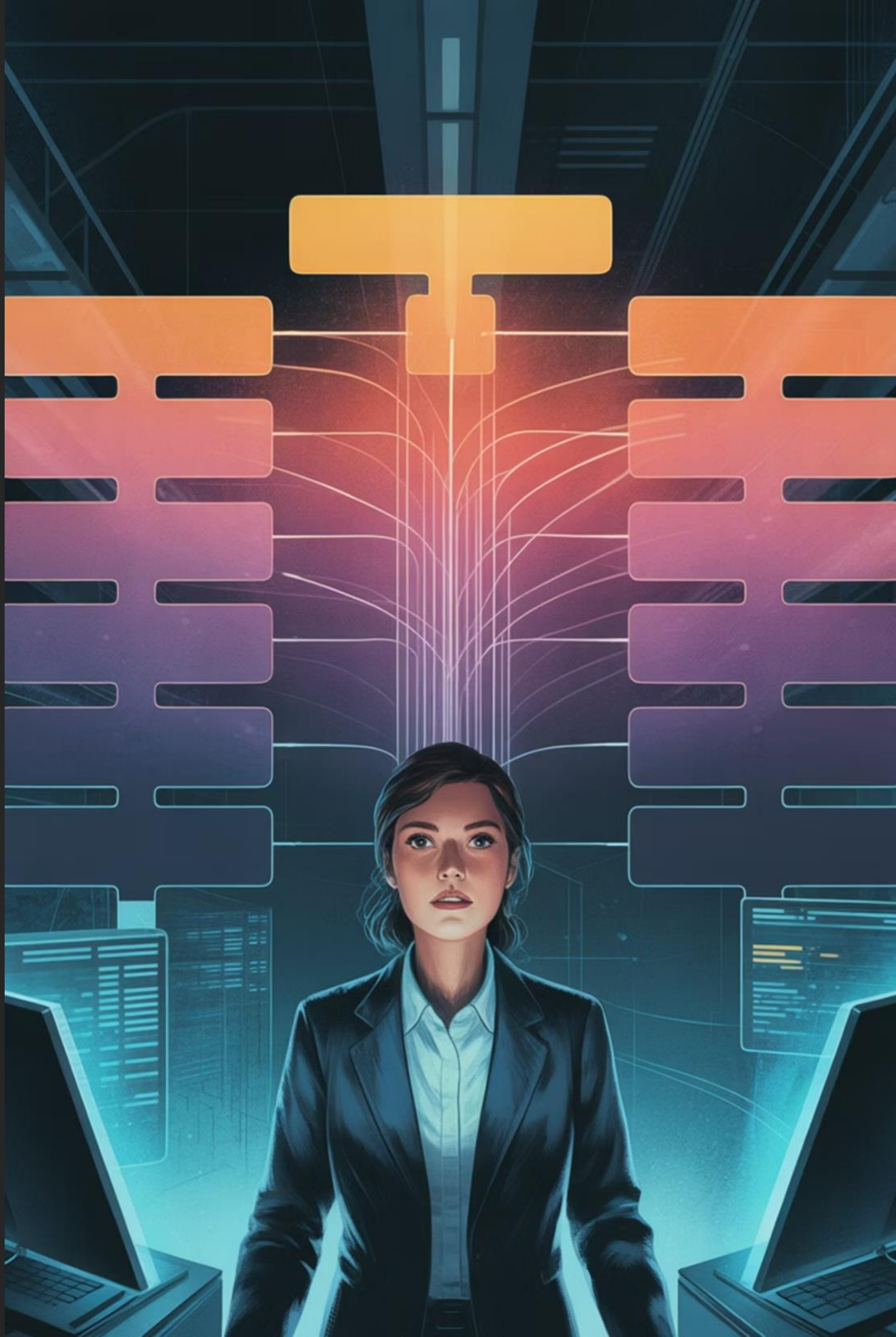
Zeek alert indicates possible DNS tunneling

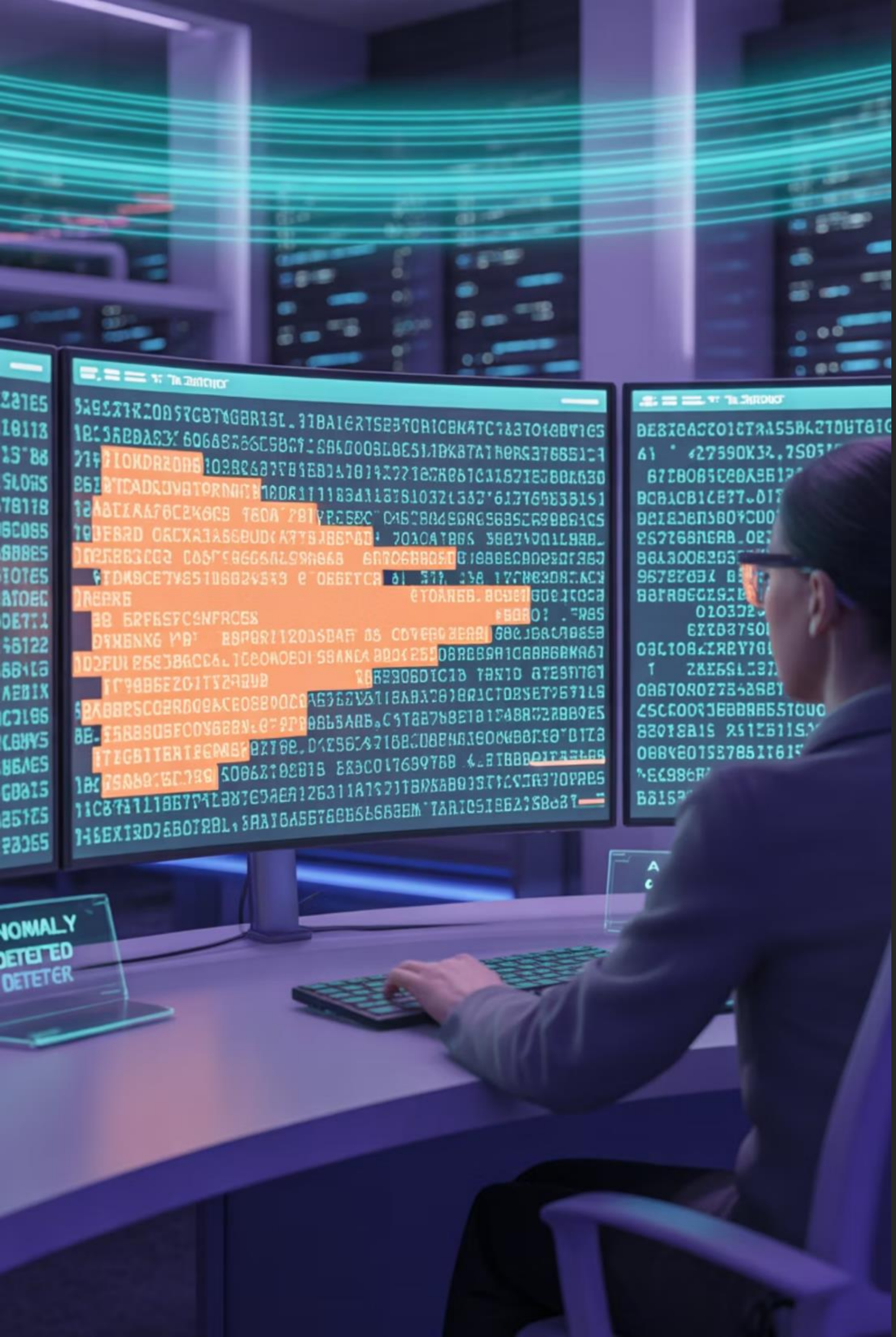
Decision Point

Analyze PCAP, run IOC sweep, or deploy AI model?

Branching Paths

Each choice leads to different detection strategies





Path A: PCAP Analysis

Extract Packet Data

Pull raw network traffic containing DNS requests

Identify Patterns

Look for abnormal query frequency and encoding

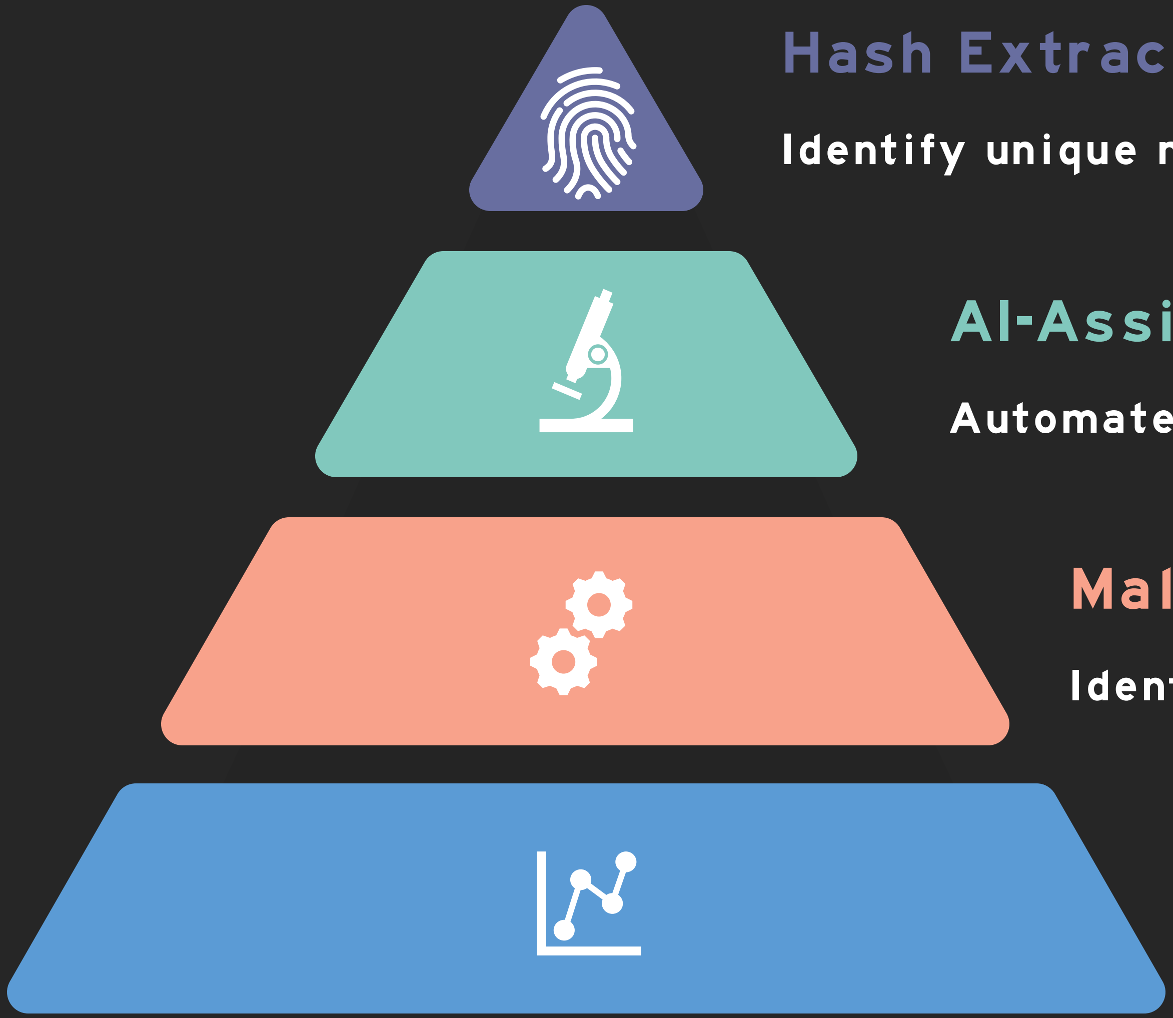
Apply AI Analysis

Use behavior-based models to identify anomalies

Extract Payload

Decode and analyze hidden commands in DNS queries

Path B: IOC Sweep Results



Hash Extraction

Identify unique malware fingerprints

AI-Assisted Analysis

Automated reverse engineering of suspicious code

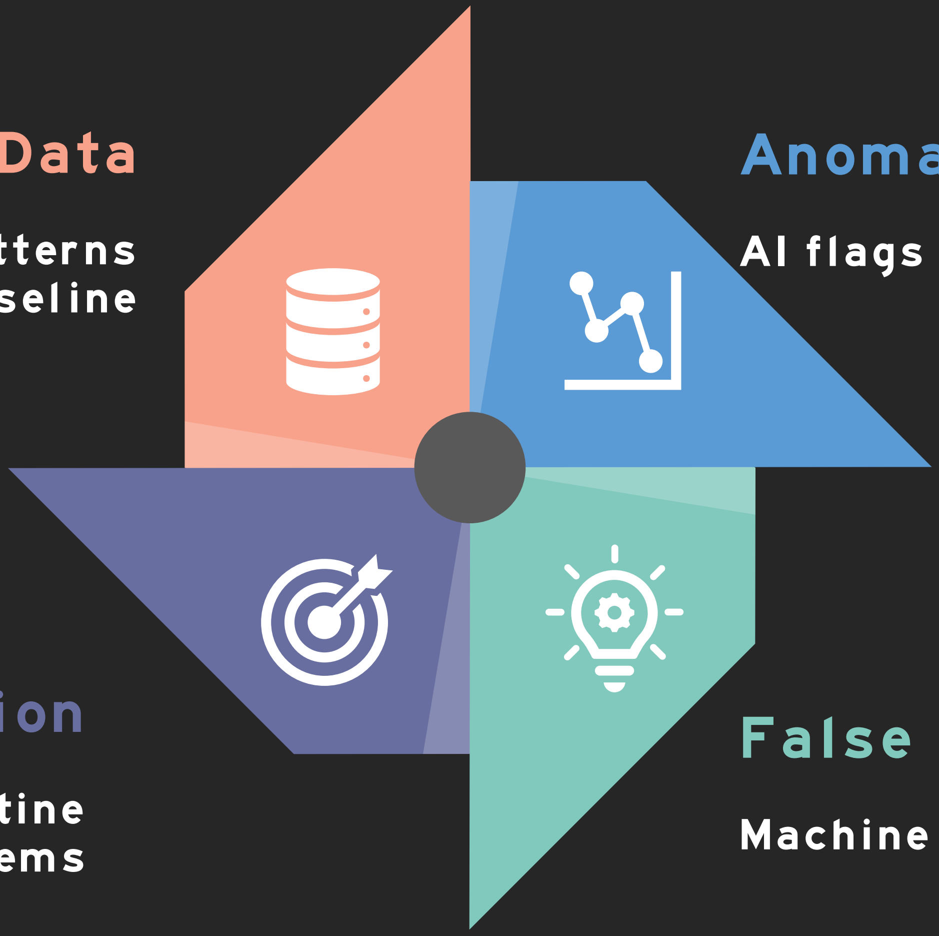
Malware Classification

Identify malware family and capabilities

Threat Intelligence Correlation

Link to known threat actors and campaigns

Path C: AI Traffic Profiling



Training Data

Historical network patterns establish baseline

Anomaly Detection

AI flags statistical outliers in traffic

Endpoint Isolation

Automatic quarantine of suspicious systems

False Positive Filtering

Machine learning reduces alert fatigue

LLM Threat Report Demo

Raw Threat Report

Unstructured text from multiple sources

- Technical details buried in narrative
- Mixed formats and terminology
- Varying levels of confidence

LLM Processing

AI extracts structured intelligence

- Identifies TTPs and maps to MITRE
- Generates detection rules automatically
- Assigns confidence scores

Red Team Twist

Adversarial AI

Attackers using ML to generate believable fake IOCs

Deception Tactics

AI-generated decoys to distract defenders

Detection Challenge

Distinguishing real from synthetic indicators

Red vs Blue Mindset

Understanding attacker psychology improves defense

Red Team Twist

Intel Requirements

AI prioritizes collection based on your threat landscape

Integrated Toolchain

Zeek + YARA + LLM + Maltego + MISP

Automation Framework

Orchestration reduces manual analysis time

Cognitive Augmentation

Human analysts paired with AI assistants

Key Takeaways

Intelligence is a Process

Cyclical methodology, not a one-time product

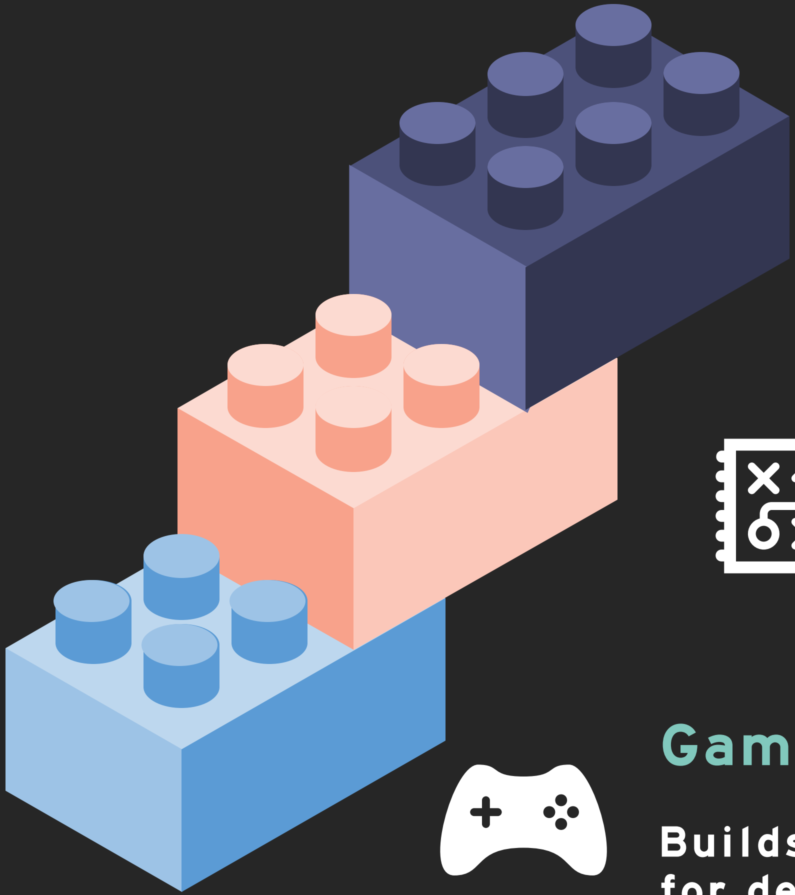
Requirements Drive Value

Focus collection on what matters to your org

Operationalize Everything

Convert insights to detection rules

Key Takeaways



Enhanced Visibility

AI expands detection capability but requires human insight

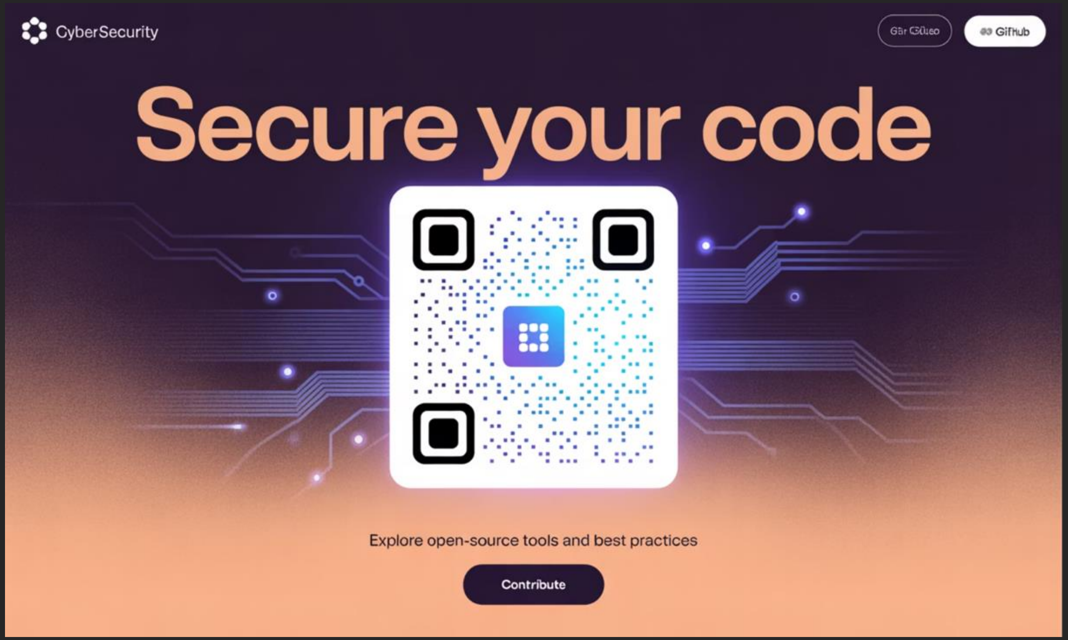
Decision Pathways

Choose-your-path mirrors real-life pressure decisions

Gamified Learning

Builds muscle memory for detection scenarios

Resources & QR Link



GitHub Repo
Code examples & templates

Discord Channel
Community support

Rule Library
Pre-built detections

Thank You / Q&A

Twitter
@carloanez

Email
info@carloanez.com

Slack
BlueTeamVillage

Thank you

Join The Conversation
https://discord.gg/blueteamvillage

Questions?

Did you enjoy the session?
Did we miss something?
Was anything unclear or confusing?

Please Provide Feedback
feedback-obsidian@blueteamvillage.org