

THREAT INTELLIGENCE & THREAT HUNTING.



An IOC feed without context tells you what happened somewhere else — **it does not tell you what is already inside your own environment, right now.**

- THREAT INTEL FEEDS
- IOC/TTP ENRICHMENT
- PROACTIVE HUNTING
- DETECTION ENGINEERING

01 THE MECHANISM



Threat Intelligence Feed

Aggregating IOCs, TTPs, and adversary infrastructure from **open-source, commercial, and ISAC sources.**



Threat Hunting

Proactively searching telemetry for **behaviors that predefined detection rules don't catch.**



Detection Engineering

Converting hunt findings into **repeatable, automated detection rules.**

02 THE FLOW

The Hunted Environment PROACTIVE

- 1 A hunter forms a hypothesis **based on current threat intelligence and adversary TTPs.**
- 2 The hunter queries telemetry **across endpoints, network, and cloud logs for that behavior.**
- 3 Confirmed findings become **new detection rules that fire automatically next time.**

The Alert-Only Environment REACTIVE

- 1 A predefined rule waits **for a known signature or exact indicator match.**
- 2 Novel attacker techniques **pass through undetected until damage is already done.**
- 3 The breach surfaces **only after data loss, encryption, or exfiltration occurs.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Threat Intel Feeds	Supplies indicators of compromise, adversary infrastructure, and TTPs from external sources.
IOC/TTP Enrichment	Correlates raw indicators with tactics, techniques, and procedures mapped to MITRE ATT&CK.
Proactive Hunting	Analyst-led searches for adversary behavior that automated tools have not yet flagged.
Detection Engineering	Converts confirmed hunt findings into tuned, repeatable detection logic.

04 DETECTION APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Signature-Based Alerts Only	No	Misses novel malware variants and living-off-the-land techniques.
Generic Threat Intel Feed	No	Floods analysts with unprioritized indicators lacking environmental context.
Reactive Incident Response Only	No	Only engages the adversary after damage has already occurred.
Automated Detection Rules Alone	No	Blind to attacker behavior that falls outside predefined rule logic.
Threat Intel + Proactive Hunting + Detection Engineering	Yes	Turns hypothesis-led hunts into context-driven, continuously tuned detection.

THREAT INTELLIGENCE & THREAT HUNTING.

HUNT · DETECT · ENRICH

05 PROGRAM OPERATIONS

Threat hunting closes the gap detection rules can't reach.

Analysts search for adversary behavior that hasn't triggered any existing alert.

Intelligence without prioritization creates alert fatigue.

Feeds must be filtered against the organization's actual attack surface and asset criticality.

Hunt findings only have value once they become detections.

A one-time discovery must be converted into a rule that catches future recurrence.

MITRE ATT&CK gives hunters and defenders a shared language.

Mapping techniques to the framework standardizes what to hunt for and how to measure coverage.

06 CONTROL MAPPING

MITRE ATT&CK

Adversary tactic and technique taxonomy for structuring hunt hypotheses and detection coverage.

NIST SP 800-150

Cyber threat information sharing guidance for structured intelligence handling.

NIST CSF

Detect function requirements for continuous monitoring and anomaly identification.

CIS CONTROLS V8

Audit log management safeguards for the telemetry hunting depends on.

07 WHAT THIS DOES NOT SOLVE

Intelligence Feed Overload

More indicators without prioritization just add noise analysts learn to ignore.

Hunt Coverage Gaps

Hunters can only search telemetry sources the organization actually collects and retains.

Zero-Day Exploitation

A never-before-seen technique has no matching TTP or signature to hunt against yet.

Analyst Skill Shortage

Hunting quality depends entirely on the experience of the analyst running the hypothesis.

08 MYTHS VS. REALITY

MYTH	REALITY
"Threat intelligence feeds work automatically once purchased."	Feeds require prioritization, deduplication, and mapping to your own environment to be useful.
MYTH	REALITY
"Threat hunting is the same as monitoring SIEM alerts."	Hunting is hypothesis-driven and looks for what alerts were never built to catch.
MYTH	REALITY
"More indicators of compromise means better detection."	Unfiltered IOC volume increases analyst fatigue without improving actual coverage.
MYTH	REALITY
"MITRE ATT&CK is only useful for red teams."	Defenders use the same framework to map hunt coverage and find detection blind spots.
MYTH	REALITY
"A hunt that finds nothing was a waste of time."	A clean hunt still validates detection coverage and confirms the hypothesis was wrong.

09 SPEAK THE PROGRAM — KEY TERMS

IOC

An observable artifact, like a file hash or IP address, that suggests a system may be compromised.

TTP

Tactics, techniques, and procedures — the behavioral patterns describing how an adversary operates.

THREAT HUNTING

Analyst-led, hypothesis-driven search for adversary activity that automated tools missed.

DETECTION ENGINEERING

The discipline of building and tuning repeatable detection rules from hunt findings.

MITRE ATT&CK

A publicly maintained knowledge base of adversary tactics and techniques.

THREAT INTEL PLATFORM

A system that aggregates, correlates, and operationalizes threat data feeds.