4D5ASecurity.com

CTI THREAT HUNTING

KEN DUNHAM, CEO

4D5A SECURITY

TLP:CLEAR – DISCLOSURE IS NOT LIMITED

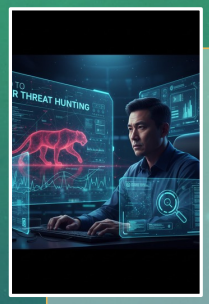
KEN DUNHAM

Ken Dunham has over three decades of combined business, technical, and global leadership experience in cybersecurity, incident response, and cyber threat intelligence. His career path is non-traditional, starting with education, consulting, and programming.

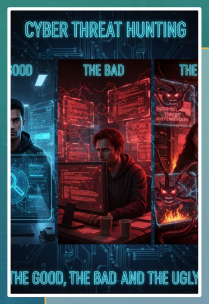
Mr. Dunham has extensive experience with all sectors and business sizes and former TS-SCI US DOD experience (redacted). He has led many of the largest global investigations in the history of computing and countered emergent threats to counter actors, campaigns, and payloads of all types as the threat of the unknown are discovered and countered.

- 1997 Innovator of U2, Warthog, and Predator (drone) training programs USAF area 51
- 1998 Global leading anti-virus software, website, and book
- 2003 Pioneer of Responsible Disclosure & Cyber Threat Intel
- 2006 Top Quoted Global Security Expert
- 2014 International Distinguished Fellow
- 2016 Article of the Year "Trouble Trends of Espionage"
- 2020 Innovator of Optiv Threat DNA Platform as-a-Service (PaaS) ™
- 2024 Cyber CISO Marksmanbship

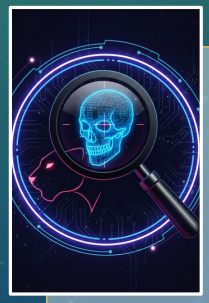
AGENDA



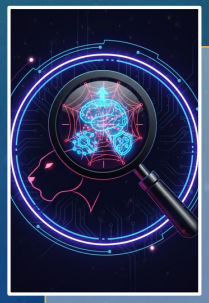
Introduction to Threat Hunting



Good, Bad, & Ugly Threat Hunting



Threat Hunting Process



Threat Hunting Tactics

WHAT IS CYBER THREAT INTELLIGENCE?

Cyber Threat Intelligence is systematic collection, analysis and dissemination of information pertaining to a company's operation in cyberspace and to an extent physical space. It is designed to inform all levels of decision makers.

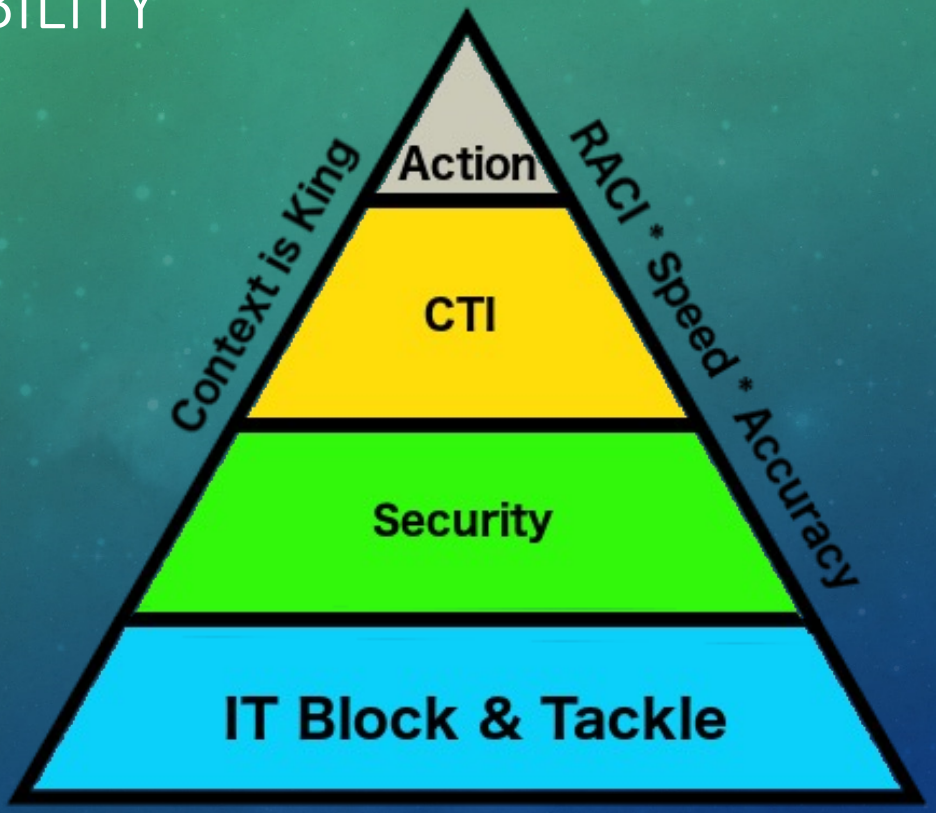
The analysis is designed to help keep situational awareness about current and arising threats.

WHAT IS THREAT HUNTING?

Threat hunting is a proactive iterative Cyber Threat Intelligence (CTI) function that aims to reduce the risk to organization's physical or virtual assets in scope, by assuming compromise, to continually seek unknown or undetected tactics, techniques, and procedures (TTP) or identify threat actors that have gained unauthorized access.

This activity may be structured or unstructured, hypothesis-driven or investigation-based, and require a proactive engagement of the responders.

CTI ACTIONABILITY



“Cyber Threat Intelligence (CTI) Actionability” - LinkedIn Article

THREAT HUNTING CTI CYCLE

Intelligence Lifecycle

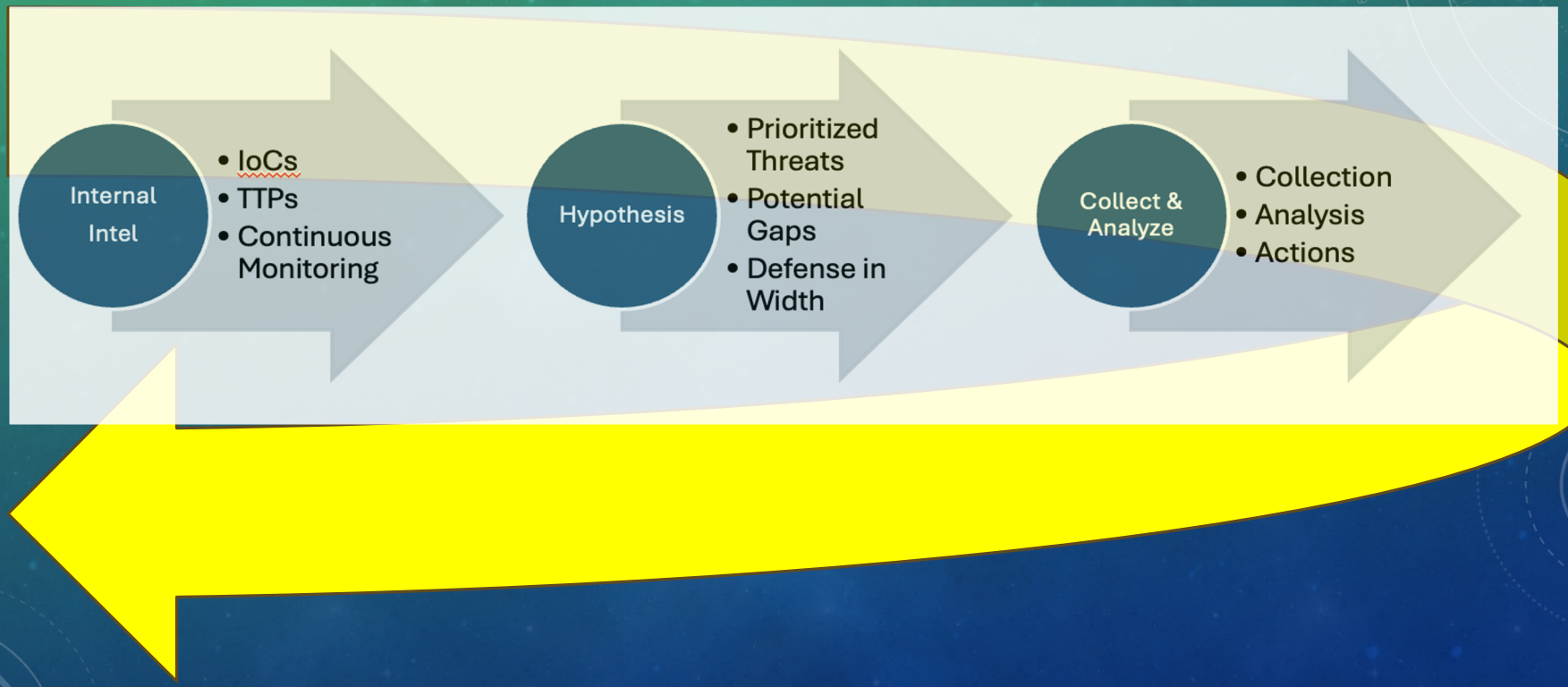
Planning & Direction
Collection
Processing and Exploitation
Analysis and Production
Dissemination & Integration

Integrated into operations and business units to reduce risk

TTPs / MITRE ATT&CK

Continual & Iterative

THREAT HUNTING PROCESS



WHAT IS A CTI HYPOTHESIS?

A specific TTPs-driven supposition based upon limited information to further a Cyber Threat Intelligence (CTI) investigation.

e.g. hypothetical hypothesis example below:
Adversaries are concealing Command and Control (C2) communications by communicating over TCP port 443, which is not monitored by our organization because it is normally associated with encrypted HTTPS (Hypertext Transfer Protocol Secure) protocol communications.

CHALLENGES OF THREAT HUNTING DEFINITIONS

- NOT External Indicators of Compromise (IOCs)
  - 8.8.8.8; agent.abc; spam@corporate.com
- NOT Dark Web
  - havelbeenpwnd; Russian Forum; Telegram
- Must be Proactive
  - Before full payload/attack is performed by adversary
- Purple Teaming
  - An excellent way to weave into CTI and threat hunting operations for advanced mature counterintelligence outcomes
- Context is King!
  - Create context and pivot quickly to another hypothesis as needed.
  - Fail quickly, if you must fail!

E.G. THE GOOD, THE BAD, THE UGLY

SANS 2018 Threat Hunting Study

Starting with Tools, Techniques or Procedures (TTPs) or a vulnerability, develop hypotheses to determine whether our infrastructure is impacted, and then test those hypotheses.

GOOD

E.G. THE GOOD, THE BAD, THE UGLY

SANS 2018 Threat Hunting Study

First, baseline the environment for normal activity. Create a hypothesis based on the kill chain. Utilize ATT&CK framework for TTPs. Run IOC sweeps from threat intel reports.

GOOD

E.G. THE GOOD, THE BAD, THE UGLY

SANS 2018 Threat Hunting Study

Notice an alert in the system and slowly tear it apart from endpoint to endpoint.

BAD

E.G. THE GOOD, THE BAD, THE UGLY

SANS 2018 Threat Hunting Study

Spend a lot of time reviewing logs from the SIEM and formulating custom queries in the SIEM.

BAD

E.G. THE GOOD, THE BAD, THE UGLY

SANS 2018 Threat Hunting Study

Gather intel, develop a hypothesis, create a scope and execute the hunt.

GREAT

E.G. THE GOOD, THE BAD, THE UGLY

SANS 2018 Threat Hunting Study

Our entire operation is constantly monitoring the environment to establish its baseline. As soon as we detect something odd or we are made aware of something risky in our environment (such as a malicious IP address communicating with us), we start an analysis on that resource: network behavior, processes behaviors, logs and possible strange evidence through the filesystem and registry. If we confirm something 'evil' we move on with the process of containment, eradication, recovery and then the lessons learned.

UGLY

WHAT IS NOT THREAT HUNTING

Tactical Research and Response

e.g. IOC queries and enrichment and ‘hunting’

Dark Web Monitoring

e.g. Looking for company related leaks, dumps, and threat data on the Dark Web related to an organization.

Enrichment

e.g. Starts with a data point, is reactive, used to create more context.

THREAT HUNTING TACTICS

Threat & TTPs Driven

- **Proactive**
  Exhaustive and continual hunting of enterprise logs. Identify and remove threats and reduce risk and attack surface. Search logs to see what is attacking and blocked to prioritize threats and actor counterintelligence.

- **Campaign, Family, or Actor(s)**
  Identify all related threats and TTPs related to a campaign, family, or actor(s) for a threat and hunt all logs and tools for visibility and counterintelligence.

- **VIP**
  Focus upon Very Import Person(s) and related threats to reduce risk.

- **Targeted & Zero-Day**
  Focus upon targeted attacks and zero-day emergent threats to reduce risk.

THANK YOU!

KEN@4D5ASECURITY.COM

4D5ASECURITY.COM