ASPIRE

# Security Operations Center
## *Cyber Threat Intelligence Unit*

## Understanding Cyber Threat Intelligence

By: Portia Cole – CTI Threat Researcher

**November 6, 2024**

# Agenda

ASPIRE

- Introduction
- What is Cyber Threat Intelligence?
- The Cyber Threat Intelligence Lifecycle
- Emergency Flash Notices
- Threat Intelligence Reports
- Monthly Threat Briefings
- Aspire Case Studies

# What is Cyber Threat Intelligence?

# Understanding Cyber Threat Intelligence

## Before we talk about Aspire's Cyber Threat Intelligence (CTI) deliverables, let's first define CTI:

- Cyber Threat Intelligence (CTI) is information gathered, processed, and analyzed to understand the motives, goals, and tactics of cybercriminals.
- By using CTI, organizations can better anticipate cyber threats and take action to prevent attacks before they happen, rather than just reacting to them after the fact.
- This helps businesses stay one step ahead of attackers, protect sensitive data, and make smarter, faster security decisions.

# Why is CTI Important?

**Prevents Data Loss** - Early identification of threats reduces the risk of breaches.

**Improves Security Posture** - Informs strategic security decisions and helps apply preventive measures.

**Collaboration** - Sharing intelligence within the community helps everyone stay ahead of emerging threats.

# Key Differences – Threat Data vs. Threat Intelligence

ASPIRE

## Threat Data

- Analysts see threat data all the time. This is called raw information like IP addresses or malware signatures
- Yes, threat data can be a starting point for CTI but it lacks actionable insight.

## Threat Intelligence

- Analyzes the data contextually to inform decision-making.
- Helps construct a narrative about who is attacking, why, and how.
- Results in actionable recommendations.

# Types of Threat Intelligence

## Strategic Threat Intelligence

- Complete SIEM optimization for all Managed Services Clients by the end of Q2.

## Tactical Threat Intelligence

- Immediate, actionable intelligence for IT/security teams.
- Indicators of Compromise (IoCs): suspicious IPs, domains, and abnormal traffic patterns.

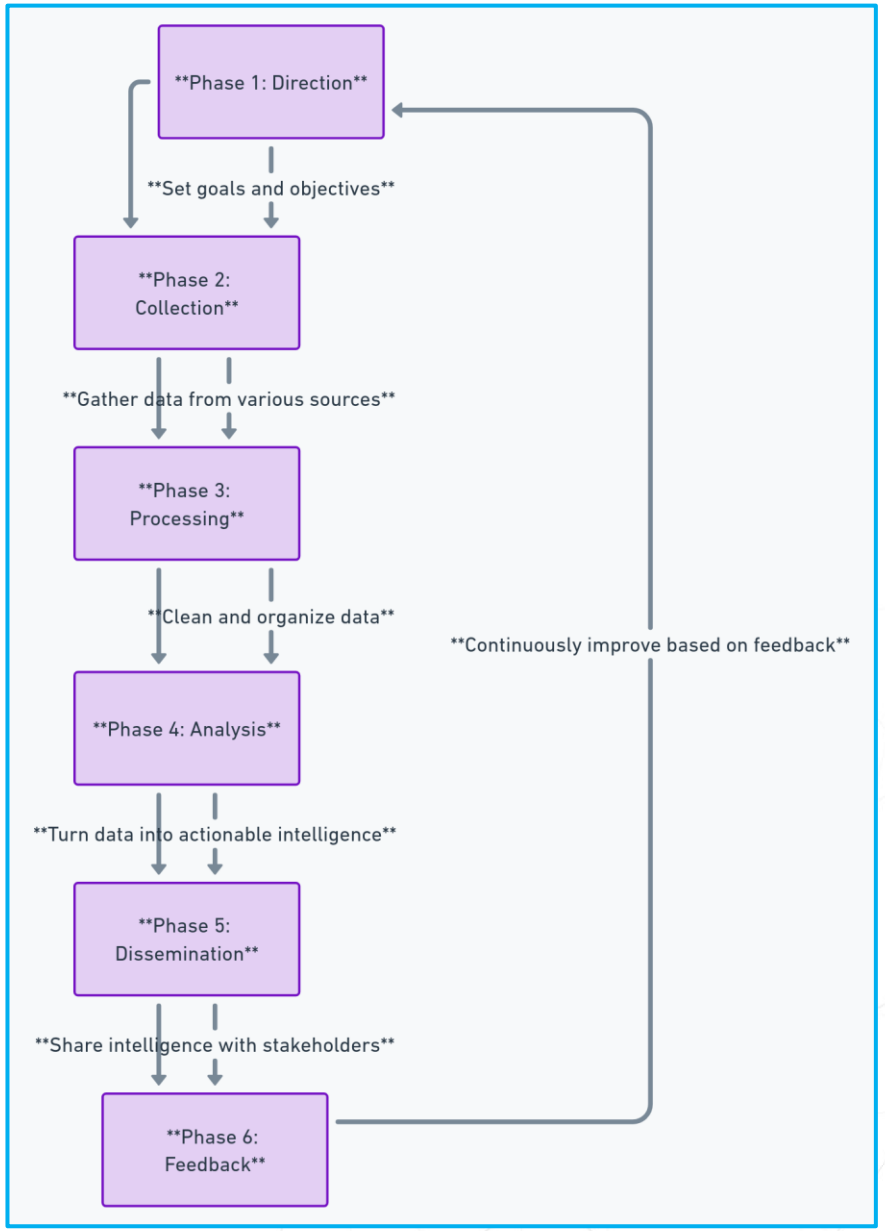
## Operational Threat Intelligence

- Provides in-depth understanding of attacker TTPs (Tactics, Techniques, and Procedures).
- Focuses on past attack patterns and adversary behavior.

# Cyber Threat Intelligence Lifecycle

ASPIRE

- **Phase 1 (Direction)** – Set goals and objectives for CTI program (e.g., what assets need protection?).
- **Phase 2 (Collection)** - Gather data from internal networks, threat feeds, open sources.
- **Phase 3 (Processing)** - Clean, structure, and organize data into usable formats.
- **Phase 4 (Analysis)** - Turn raw data into actionable intelligence that guides decisions.
- **Phase 5 (Dissemination)** - Share intelligence with relevant stakeholders (e.g., IT, C-suite, security teams).
- **Phase 6 (Feedback)** - Continuous improvement of CTI program based on stakeholder input.



# Who Benefits From CTI?

- **Business Leaders** - Reduced risk of financial and reputational damage from breaches.
- **Security Teams** - Improved ability to identify and mitigate emerging threats.
- **The Organization as a Whole** - Better preparation for and response to cyberattacks. Enhanced overall security posture.

# How Will CTI Help Me?

- **Preventing Data Breaches** - Monitoring suspicious domains/IPs to block malicious communications.
- **Reducing Costs** - Proactively preventing attacks avoids the high costs of breach recovery.
- **Information Security Strategy** - Intelligence on evolving threats informs investment in defensive technologies.

# Threat Intelligence in Action

- **Example -** An organization blocked a phishing campaign by analyzing and sharing IoCs of a known attack group.
- **Example -** Threat intelligence helped a company avoid a costly ransomware attack by recognizing suspicious file downloads from known bad IPs.

# CTI Deliverables

# Emergency Flash Notice

- An **Emergency Flash Notice** is an emergency communication vehicle used to deliver information to Aspire's customers, as well as internal staff, surrounding active threats.
- Those threats include information about **vulnerabilities** found within software and servers that are being exploited in the wild or have a low attack complexity score.
- The notice has a general turnaround time between **24 and 48 hours** and is sent out via ServiceNow (SNOW) and is published on Aspire's customer portal.
- The audience for these notices are **customers**, **Aspire staff**, and **executive staff**.

# Threat Intelligence Report

- Aspire's Cyber Threat Intelligence (CTI) team develops Threat Intelligence Reports (TIR) to provide context regarding **adversaries** and **other threats** to the cybersecurity landscape.

- The CTI team actively **hunts** for and **researches emerging threats** and **threat actors** to help you better understand the threat landscape and individual profiles of threat actors.

- Our reports are **generated bi-weekly** and may feature specific threats on an array of topics including, but not limited to, ransomware, cryptojacking, malware, phishing, worms, and other threats. The CTI team also develops TIR reports that feature specific threat actors who are actively exploiting vulnerabilities.

- The content of these reports is based on the CTI Monthly Threat Brief, and the audience for these reports includes **customers**, **Aspire staff**, and **executive staff**.

# CTI Monthly Threat Briefing

- Briefings that give **insight** into the cyber threat landscape and are comprised of information that did not make it into an Emergency Flash Notice or a Threat Intelligence Report.

- The briefing provides **current information** regarding recent **threats**/**vulnerabilities**, threat actors, security breaches, and industry specific threats.

- The briefing comes out on a **monthly basis** and the audience is generally Aspire staff, especially Account Managers who may want to keep their customers up to speed with the threat landscape.

# Aspire Case Studies

- Aspire will publish case studies detailing **real security incidents** that our team has investigated and mitigated.

- Authored by Aspire **engineers**, **analysts**, or **other experts**, these case studies will be based either on original content by the incident expert, with co-authorship support by the CTI Threat Researcher, or structured as interviews where the CTI Threat Researcher will consult with subject matter experts to capture technical insights.

- These case studies will position Aspire as a **cybersecurity authority**, offering customers and stakeholders a clear view of Aspire's protection in action.

# Where Can I find these deliverables?

## Aspire’s customer Portal

# Aspire’s Customer Portal

- Aspire’s customer portal
  - The portal will be your go to source for Emergency Flash Notices, Threat Intelligence Reports, CTI Briefings, and General CTI Communications.
  - The portal is easy to access:
    - https://aspiretech.service-now.com/csm

# Thank You

**Portia Cole**

**CTI Threat Researcher**

**Aspire Technology Partners**

pcole@aspiretransforms.com