



Operationalizing ICS Threat Intelligence

Michael Gardner
Senior Intel TAM, Dragos

Agenda

Operationalizing ICS Cyber Threat Intelligence (CTI)

- Why ICS Threat Intelligence
- Cyber Threat Intelligence Foundations
- ICS Threat Intelligence - Background
- Value of ICS Threat Intelligence
- Operationalization
- Key Use Cases
- Q&A

The background is a blurred industrial scene, possibly a factory or warehouse, with various metal structures, pipes, and equipment. A dark, semi-transparent rectangular overlay covers the center of the image. Inside this overlay is a black rectangle with a thin, light green border. The text "CTI Foundations" is centered within this black rectangle in a light green, sans-serif font.

CTI Foundations

Why Operationalize ICS Threat Intelligence?

Understand and Educate on Your Threat Landscape

- Who adversaries are
 - Actors, sponsors, and employers
- What adversaries use
 - Capabilities, toolsets, and infrastructure
- Where adversaries target
 - Industries, verticals, and geographic regions
- When adversaries act
 - Identifying timelines; patterns of life
- Why adversaries attack
 - Motives and intent
- How adversaries operate
 - Behaviors and patterns

CTI Key Takeaways

- Insight to guide decision making
- Know stuff, so we can do stuff
- Power to “change the future”
- Threat intelligence is not a single tool
 - Data sources vary
- Many CTI processes can drive value

CTI Data Sources

First Party

- Your intelligence
- Networks; Logs; Policies, etc.

Second Party

- Friends; Trust Groups; Information Sharing & Analysis Centers (ISACs); Industry Sharing

Third Party

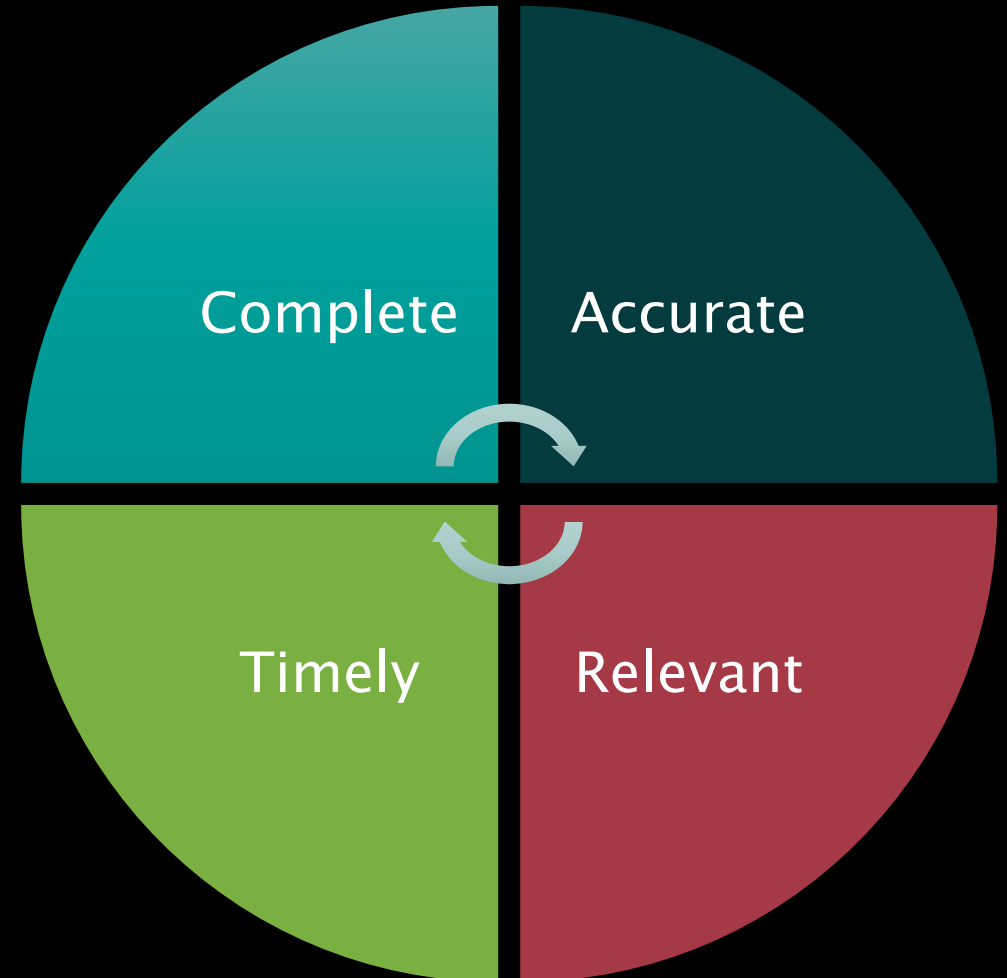
- External source of data acquired or purchased
- Vendors; Government

Fourth Party

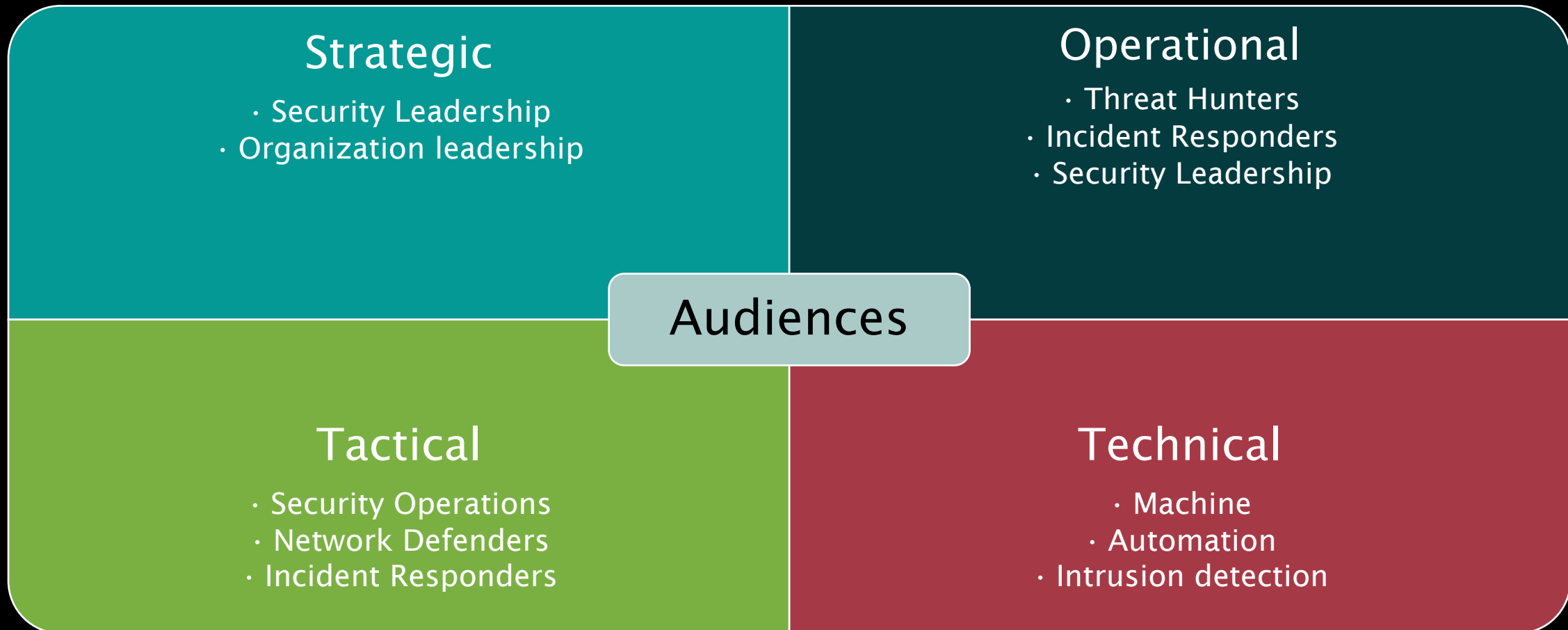
- Compromise data – may be “closed” source
- Battle damage assessment

Components of Good Threat Intelligence

- Complete - enough to guide decision making
- Accurate - inaccuracy leads to wrong decision making
- Relevant - fits into your PIRs
- Timely - enough for decisions to have impact



CTI Types and Audiences



CTI, applied

NIST Cybersecurity Framework



Identify

- PIRs, based on known threats
- Planning, policy, risk
- Vulnerability Management



Protect

- Security Controls
- Architecture & Policy
- Awareness



Detect

- Anomalies/Security Events
- Security Event Monitoring
- Threat Hunting



Respond

- Communication
- Incident Analysis
- Mitigation



Recover

- Communication
- Improvements

The background of the slide is a dark, semi-transparent image of an industrial facility, likely a refinery or chemical plant. It features various structures such as distillation columns, storage tanks, and piping. Overlaid on this background are several glowing green and yellow lines and arcs, suggesting a network or data flow. In the center, a black rectangular box with a thin green border contains the text "ICS Threat Intelligence" in a light green, sans-serif font.

ICS Threat Intelligence

ICS Threat Intelligence

The Threat Landscape has Shifted

- Civilian Infrastructure has entered the crosshairs
- ICS-Specific Malware
 - STUXNET
 - HAVEX
 - BLACKENERGY2
 - CRASHOVERRIDE
 - TRISIS
 - EKANS Ransomware

What does this shift mean for ICS defenders?


- Defense in Depth must shift beyond IT, into OT
 - It's not either/or, it's both!
- Proactive security measures must be taken to prevent security incidents
 - Enter threat intel
- Stakes can be higher for OT
 - Potential for loss of life or environmental disaster

The background features a dark, teal-toned image of a Ferris wheel, likely the London Eye, with its intricate metal framework visible. Overlaid on this are faint, light-colored technical diagrams, including circular patterns with dots and various geometric shapes, suggesting a theme of engineering or technology.

Why Operationalize ICS CTI?

Why Operationalize ICS Threat Intelligence?

- Detection and Policy Guidance
 - Threat intelligence produces insights on adversaries and their malicious activity
 - Understanding adversary behavior allows for adequate preparation at the security policy level
- Enable Defender Efficacy
 - Detective guidance of activity support identifying breaches in an environment
 - Knowledge of detailed threat behavior enables improved threat hunts
- Reduction in Time-to-Recover during Incident Response
 - CTI integrated into a security program reduces mean time to recover, and adversary dwell time - critical to ICS asset owners and operators
 - Understanding of previous threat scope leads to quicker eradication of adversary

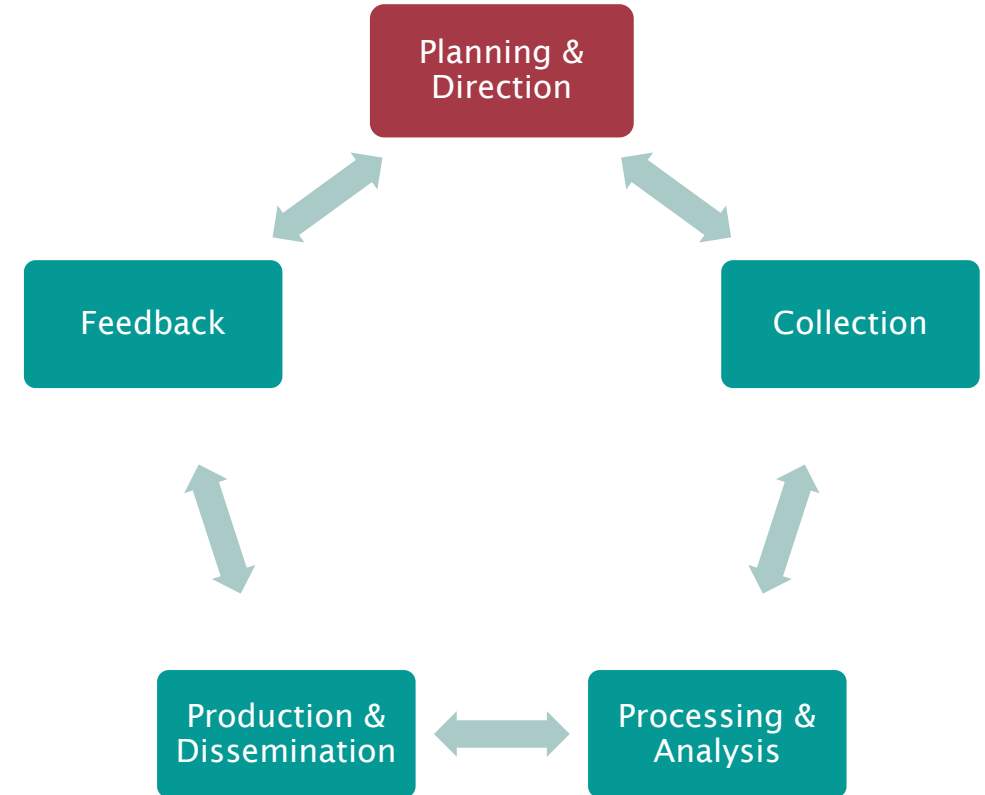
The background is a photograph of an industrial facility, possibly a power plant or refinery, with complex piping, structural steel, and various equipment. A dark, semi-transparent rectangular overlay covers the center of the image. Inside this overlay is a black rectangle with a thin, light-colored border. The text "Let's Operationalize" is centered within the black rectangle in a light green, sans-serif font.

Let's Operationalize

Back to Basics - CTI Cycle

Planning & Direction

- Develop Starting PIRs
 - Start Small; No need to cover every threat
 - "What nation-state sponsored activity groups target LNG operations?"
- Build simple threat models
 - Choose your top 5 adversaries of concern to your vertical
- Identify stakeholders
 - Collect their requirements
- Determine your desired outcome
 - What action should you or stakeholders take?



Planning & Direction - PIRs

- PIR 01 – Will Nation-State sponsored activity groups target North American LNG operations?
 - EEI 01: Have Nation-State sponsored threat actors targeted North American LNG in the last year?
 - Indicator 01: Adversaries have been observed targeting North American LNG facilities since at least 01 JAN 2021.
 - SIR 01: Hunters have identified adversaries targeting North American LNG at at least Stage 1 of the ICS Cyber Kill Chain.

Planning & Direction – Threat Modeling

The Diamond Model

INFRASTRUCTURE

- C2 nodes
- Domains
- Hosting
- Obfuscation



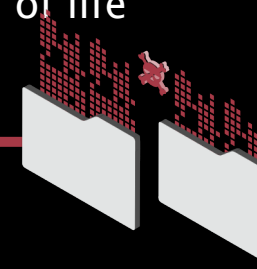
ACTIVITY GROUP

ADVERSARY

- Associations with other groups/activities
- Home base
- Languages/cultural references
- Working hours
- Pattern of life

CAPABILITIES

- Expertise
- Operational discipline
- Malware type: operational, open source, bespoke
- Exploit development
- Tools
- Espionage or disruption or both?



VICTIM

- Target description
- Apparent target objectives
- At Dragos, an AG is only named if the adversary aims for or purposefully affects ICS and/or OT of its target

Planning & Direction – Threat Modeling

Xt

XENOTIME

SINCE 2014

ICS IMPACT: Demonstrated capability to execute disruptive ICS attacks, such as the 2017 TRISIS incident.

INFRASTRUCTURE

- Virtual Private Server and compromised legitimate infrastructure
- European web hosting providers
- Asian shipping company



ACTIVITY GROUP

ADVERSARY

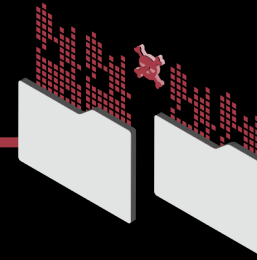
- Unique tool development

VICTIM

- Oil & Gas, Electric Utilities
- Middle East, Europe, North America, Australia

CAPABILITIES

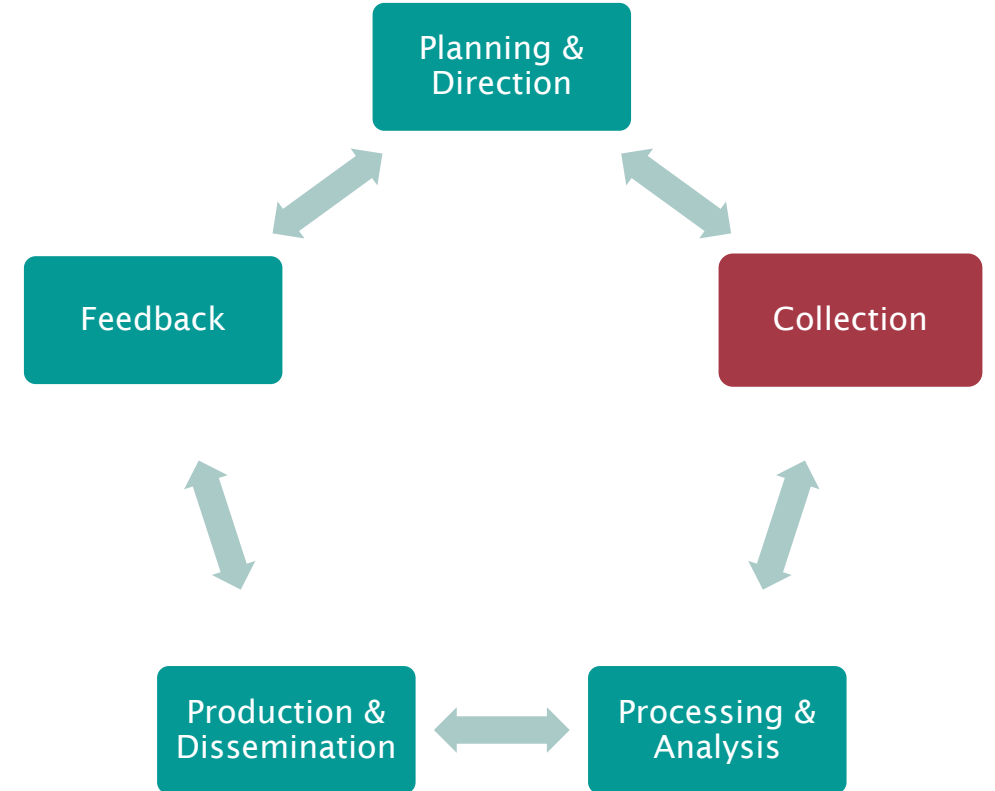
- TRISIS
- Custom credential harvesting
- Off-the-shelf tools



Back to Basics - CTI Cycle

Collection

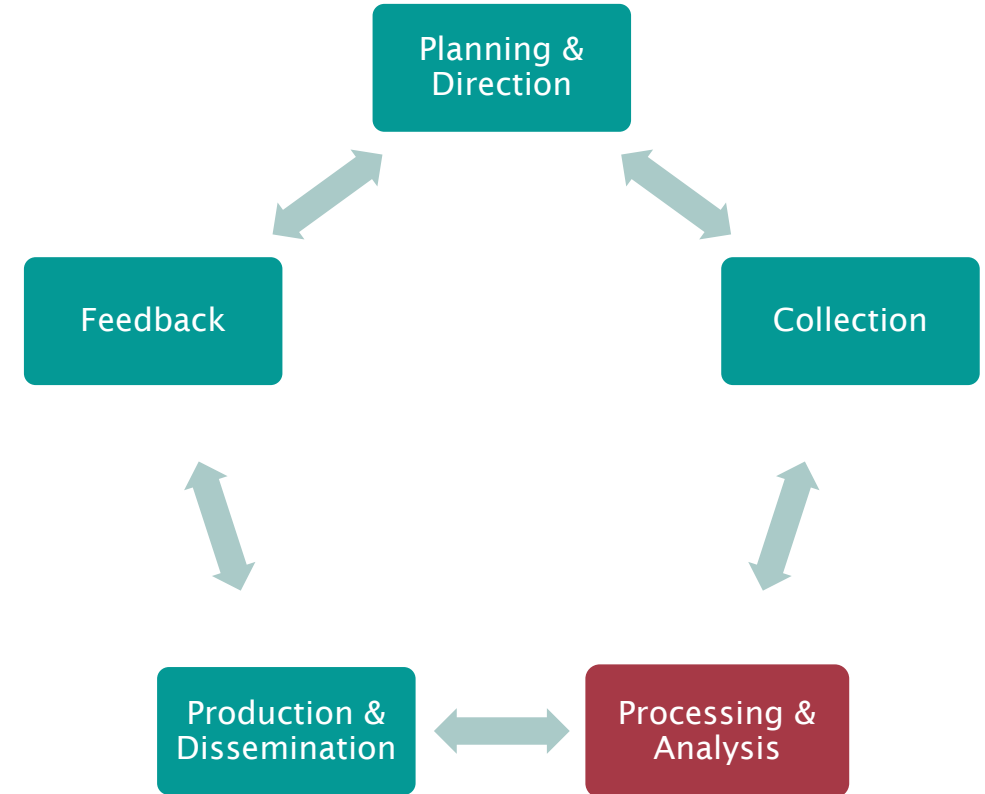
- Begin to build your Collection Management Framework (CMF)
 - What do we have?
 - What do we need?
- Access to internal telemetry
 - Where can we improve visibility into OT?
- Processes and Procedures
 - How do we get this stuff?
 - Who oversees what sources?



Back to Basics - CTI Cycle

Processing & Analysis

- Raw Data → Information
- Refinement based on PIRs
- Relevance and Correlation
 - Does this fit into our tech stack?
 - Do we have telemetry?
- Threat, Impact, Action
- Contextualize and Prioritize
 - Develop a rating system



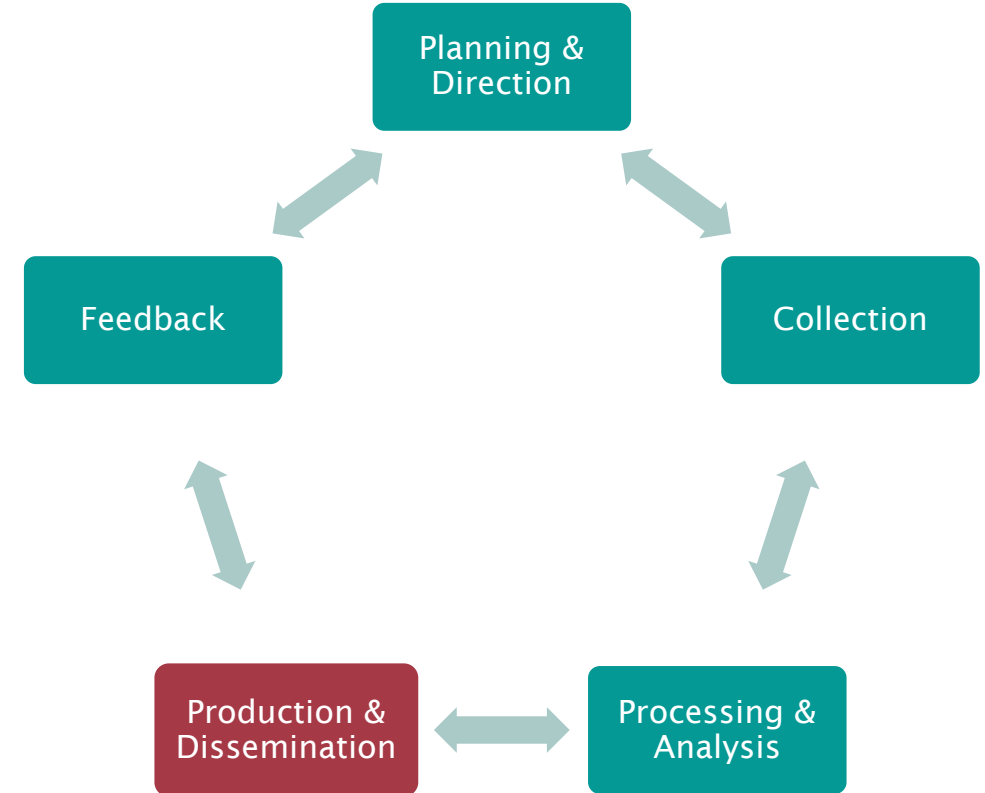
Processing and Analysis – TIA Assessment

Threat	What is the threat? Addressing who, what, where, when, why, and how.
Impact	What is the impact to an organization if the threat were realized?
Action	Which actions mitigate the threat in both the near- and mid-term?

Back to Basics - CTI Cycle

Production & Dissemination

- Processed intelligence for stakeholders
 - Briefs, reports, newsletters, tickets, etc.
- Identify stakeholders and determine relevancy
- Make it actionable!
- Communicate the threat
- Track actions taken



INTERNAL FLASH REPORT

Report Title	BlackMatter Sample -- [ORGANIZATION] Flash Report
Report Classification	Situational Awareness Only
Required Actions	Situational Awareness Only
WorldView Report Type	Advisory Alert
TLP	RED; Do not disseminate to external recipients

Prepared For:
[ORGANIZATION]

Prepared By:
[ANALYST]

-- Situational Awareness Only --

FLASH REPORT 20210930-01

EXECUTIVE SUMMARY

On September 20, 2021, open source and private intelligence source: claimed as victim by BlackMatter ransomware operators on their dairy farmers' feed and grain cooperative that covers 14 of 99 counties in Iowa corn and soybeans in the United States. The corn and soybean harvest time of this reporting, increasing the impact of the attack on operations. moderate confidence that this attack will immediately impact the production and other grain and may have further implications for the food supply.

ANALYST COMMENTS

RELEVANCE TO [ORGANIZATION]

Although the targeted industry in this attack is Food and Agriculture Manufacturing, Processing or Storage, this incident is noteworthy for all industrial verticals, as it highlights the willingness of ransomware operators to continue to target critical industries, despite government warnings and statements to the contrary. BlackMatter ransomware is a suspected rebranding of DarkSide ransomware, the group responsible for targeting the Oil and Gas Industry with their attack on Colonial Pipeline, causing significant disruption to the east coast's oil and gas supply chain. Ransomware operators will continue to seek out high value targets with a need for operational resilience, as this increases the likelihood of ransom payment for quick restoration of services.

POTENTIAL IMPACT

This report is for situational awareness only. Security operations maintains the ability to detect and respond to ransomware because of these security controls [INSERT] and offline backups [INSERT]. Security operations will perform an applicability assessment and evaluate incident response plans as warranted, based on emerging ransomware reporting.

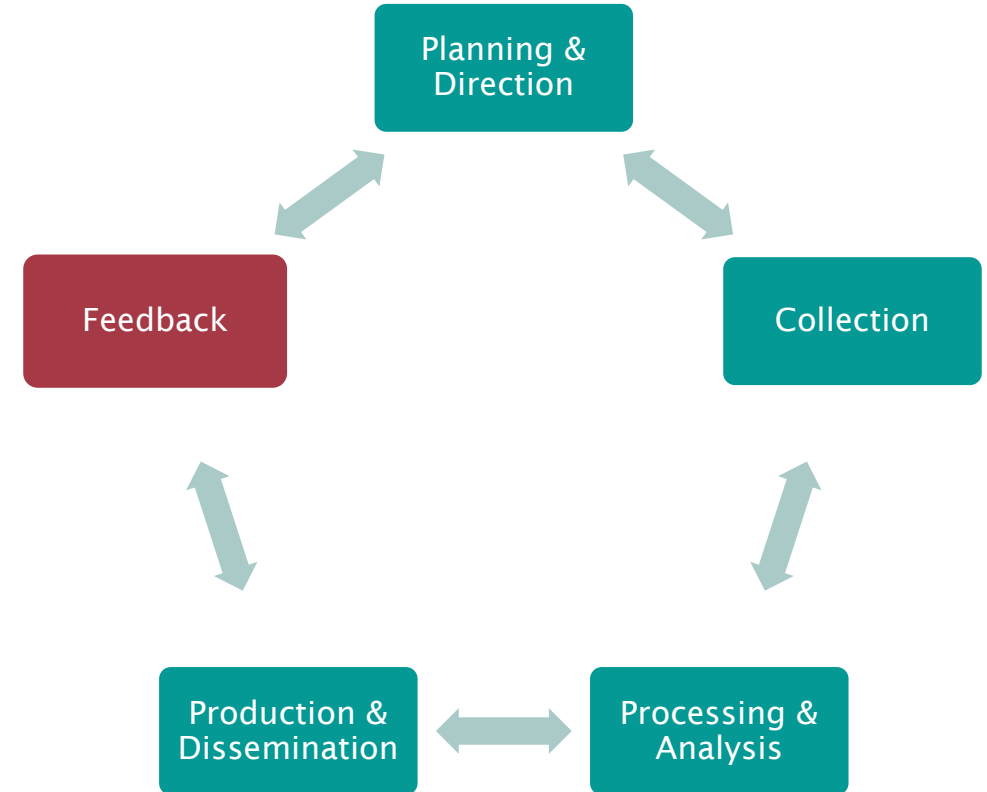
ACTIONABLE FINDINGS

This is for Situational Awareness Only. Security Operations has analyzed internal telemetry for the following indicators of compromise associated with the attack on NEW Cooperative and found no matches.

Back to Basics - CTI Cycle

Feedback

- Critical to Planning & Direction
 - Always be refining
 - Identify new priorities
- Allows for adjustments throughout the cycle
- Again, start small
 - Deliver value with one true OT action item on a monthly team sync



The background of the slide features a dark, moody image of a Ferris wheel, likely the London Eye, with its intricate metal framework visible. Overlaid on this are faint, light-colored technical diagrams, including circular patterns with dots and various geometric shapes, suggesting a theme of engineering or technology.

Use Cases for Operationalization

USE CASE – THREAT DETECTION

PROBLEM:

OT Defenders often do not know what detections to prioritize, or what they should be detecting on in general



ICS Threat Intelligence

Threat Hunters, Researchers, and Analysts aggregate known and suspected malicious technical elements into various private and public data feeds.



Defender Action

Ingest new IOCs into internal defense systems (SIEM, EDR, etc.) to hunt and monitor for communication with known or suspected bad infrastructure or anomalous activity within internal telemetry. Tune alerting to fit security monitoring goals and directives.



Impact

- Improved detection scope
- Security automation
- Early indication of malicious activity

USE CASE – THREAT HUNTING

PROBLEM:

OT Defenders often do not know what to look for in proactive threat hunting in their environments



ICS Threat Intelligence

Threat Hunters, Researchers, and Analysts discover and report on observed adversary behavior for analysis by OT defenders



Defender Action

Review context of threat behaviors in relevant industry, regional, or adversarial reporting to develop a hypothesis on where the adversary might be or what they might be doing in OT environments. Test this hypothesis by searching for similar activity.



Impact

- More informed hypothesis development
- Fruitful hunts with less time burned
- Better understanding of real adversary behaviors

USE CASE – INCIDENT RESPONSE

PROBLEM:

OT Responders have a hard time defining a scope during an investigation



ICS Threat Intelligence

Threat Hunters, Researchers, and Analysts report on previous compromises to provide a comprehensive look into historic adversary activity



Defender Action

Educate incident responders on previous cyber events. Work with the incident response team during engagements to determine ties to previous activity groups and effectively scope the mitigation efforts based on past activity.



Impact

- Reduced adversary dwell time
- Reduced time to recover
- Increased probability of full eradication

USE CASE – VULN MANAGEMENT

PROBLEM:

OT Defenders and asset owners have a more difficult time prioritizing and mitigating OT vulnerabilities than their IT colleagues



ICS Threat Intelligence

ICS Vendors, Hunters, and Vulnerability Researchers analyze and assess known vulnerabilities to provide a true threat score, and research and report on previously unknown zero-day vulnerabilities within OT products



Defender Action

Work with vulnerability management teams and asset owners to review and assess vulnerability relevance to technology stack to prioritize outages and implement mitigations where a patch is not available. Identify and implement mitigations to critical vulnerabilities.



Impact

- Risk reduction, even with no patch available
- Potential permanent improvement to architecture based on vulnerability mitigations

USE CASE – SOCIALIZATION OF THREATS

PROBLEM:

OT Defenders have a hard time prioritizing education of business stakeholders on threats



ICS Threat Intelligence

ICS threat intelligence provides deep technical insight into the threat to OT verticals, helping organizations understand the threat landscape



Defender Action

Inform key stakeholders and leadership on relevant threats and their potential impact through a structure cadence of internal reporting and briefing



Impact

- Improved security awareness
- OT stakeholder engagement
- Quantifiable justification for policy improvements

USE CASE – JUSTIFICATION OF INVESTMENT IN OT CYBERSECURITY

PROBLEM:

OT Defenders struggle to illustrate the entirety of potential and identified cyberthreats affecting their environment and articulate the investments required to close any associated gaps



ICS Threat Intelligence

ICS threat intelligence provides deep technical insight into the threat to OT verticals, helping organizations understand the threat landscape



Defender Action

Educate decision makers on what relevant threats cannot be handled by the organization without additional resources through reporting and briefing. Highlight the real or potential impact of these threats to operations.



Impact

- Improved security awareness
- Quantifiable justification for increased security resources

USE CASE – RESPOND TO RFIs

PROBLEM:

OT Defenders are often queried by organizational leadership regarding preparedness against newsworthy threats



ICS Threat Intelligence

ICS threat intelligence providers produce timely summaries and assessments of recent cyber security incidents impacting industrial control systems and operational technology



Defender Action

Review intelligence sources relevant to newly reported cyber security incidents to guide assessment of defensive practices, enabling an educated response to executive leadership



Impact

- Timely assessment of breaking threats
- Informed support of leadership decision making
- Improved security awareness

USE CASE – ASSESSMENT OF DEFENSES AND RED TEAMING

PROBLEM:

OT Defenders and penetration testers need to know how to emulate OT threats to assess the integrity of defense systems



ICS Threat Intelligence

ICS threat intelligence provides insight into behaviors and toolsets deployed by adversaries in real-world compromises



Defender Action

Assess security posture against adversary toolsets reported in intelligence sources. Educate penetration testers and red teamers on toolsets deployed for emulation in engagements to determine efficacy of defense practices.



Impact

- Appropriately scoped red-team engagements
- Defender insight into adversary toolsets
- Improved security awareness

Thank you so much!



Michael Gardner
Senior Intel TAM, Dragos
mgardner@dragos.com
[linkedin.com/in/michgard](https://www.linkedin.com/in/michgard)