SANS FOR578: Cyber Threat Intelligence

The Cycle of Cyber Threat Intelligence

Summary

Course Video
SANS Course

Intelligence

Intelligence is the collecting and processing of information about a competitive entity and its agents, needed by an organization or group for its security and well-being. Intelligence is both a product and a process.

Cyber Threat Intelligence is defined as analyzed information about the hostile intent, capability, and opportunity of an adversary that satisfies a requirement. The focus is on the human threat.

The Intelligence Cycle

Dissemination --> Planning and Direction ---> Collection --> Processing and Exploitation --> Analysis and Production --> Return to Dissemination

Structuring Your Team to Generate Intelligence

Intelligence Team:

- Security Operations Center
- Incident Response
- System Engineering & IT
- Business Operations
- Vulnerability Management

Planning and Direction Fundamentals

- **Intelligence Requirements** - request to satisfy a knowledge gap about the threat or operational environment. Objectives that analysts seek to satisfy through the intelligence process. **Example**:

Strategic: What business units are at most risk to cyber crime?

Operational: What activity groups are currently active in our industry?

Tactical: What adversary behaviors should security focus on to identify threats that are the most likely to breach our organization?

- **Threat Modeling**

  Your Organization

  - Financial Data --> (Activity Group A)
  - Intellectual Property --> (Activity Group A/B)
  - System Availability --> (Activity Group C)
- **Collection Management Framework**
  - Analysts must understand where they are getting data, how it is processed and delivered to them, and what questions can they reasonably ask of the data.
  - A **Collection Management Framework** is a view of sources of data, what is available in the data, and how that data is processed and exploited

Collection

Key Collection Sources

- **Intrusion Analysis**
  - Look to your own internal information
  - Describes stages of a single intrusion
  - Seven stages to defend
- **Malware Collection**
  - Historically, public threat intelligence reports have been malware reports.
    - Strong focus on malware analysis in the community.
    - Can be misleading as a sole source of collection, but can be highly valuable.
  - Leveraged by organizations as a free malware sandbox.
    - Makes the data available to others, including adversaries
  - Some popular sites:
    - VirusTotal
    - Hybrid-Analysis
    - Joe Sandbox
  - Can create your own
  - Useful as a CTI collection source
- **Domains**
  - **Identify** all relevant indicators
  - **Start** with single indicator

- **Pivot** through each data source and add relevant data points
  - C2 Domain
  - Registrant Data
  - IP Resolution
  - Samples calling back to it
- **Validate** ensure links contain context and are meaningful

- **External Datasets**
  - Usually exist in the form of IP addresses, digital hashes, filenames, and other Atomic and Computed threat indicators
  - Key Aspects:
    - Where is the data coming from?
    - Is the data applicable to the type of threats your organization cares about?
    - How is the data going to be used?
  - Highly trusted sources' threat data can be plugged directly into many organization's security architecture to actively identify or block validated threats, but **be cautious**
  - **Measuring Threat Feeds**
    - Plus:
      - Pivots into higher-order context
      - Is focused on your industry threats
      - Has well-articulated understanding of the Collection Management Framework feeding it
      - Openly values quality and accuracy over quantity and speed
    - Minus:
      - Ever contains RFC 1918 addresses or public trusted domains like Microsoft.com
      - No context behind info
      - Expectation is plug and play
- **TLS Certificates**
  - A digital certificate used in secure host-to-host network communications (previously SSL)
  - Collection of TLS certificates (free/paid)
  - Can be used to find C2 infrastructure

Processing & Exploitation

Structured Models: Data into Buckets

- Structured models are useful to analysts for many reasons, but a chief reason is simple: **data into buckets**
    - Allows for the abstraction of the analyst and identification of patterns
    - Kill Chain, Diamond Model, MITRE ATT&CK, VERIS
        - **Diamond Model**
            - Infrastructure
            - Adversary
            - Capability/TTP
            - Victim
        - **MITRE ATT&CK** is a documentation of tactics and techniques
            - A useful framework for expressing and documenting tactics and techniques
            - Supported by MITRE and contributed to through many in the community
            - Focuses on tactics and techniques that have been observed in the real world
    - **Storing Collected Intel**
        - Often discussed in the context of threat intelligence platform
        - The focus is on storing information in a quickly accessible and useful format
        - Pros and Cons to each--consider your requirements!
    - **Storing Platforms**
        - Open Source
            - CRITS
            - MISP
            - Threat_Note
            - YETI
        - Pros: Free, ample storage, open source sharing communities
        - Cons: Difficult to implement and maintain

Analysis and Production

Identifying and Defeating Bias

- All analysts have bias
- Cognitive biases are constraints on how we as analysts think that influence incorrect decisions, assessments, or rationale
- They allow analysts to create their own version of reality where inaccurate judgements and illogical interpretations occur

Confirmation Bias

- Selectively Supporting One Hypothesis
- Evidence Inclusion
    - Seek supporting evidence
    - Reject refuting evidence
- Significance Biasing
    - Greater significance to supporting data
    - Lesser significance to contradicting data

Structured Analytic Techniques

- Structured Analytic Techniques (SATs) are analyst approaches to better evaluate information while reducing the impact of bias
    - Analysts leverage models to abstract data as much as possible from ourselves
    - Sample SATs:
        - Analysis of Competing Hypotheses
        - Devil's Advocacy
        - Team A/Team B
        - Brainstorming
        - Red Team Analysis

Analysis: Correlating Clusters

- Many terms for clusters:
    - threat actors
    - **activity groups** are unique clusters of intrusions mathematically defined by the analyst/team's analytical weighting (confidence scoring)
    - campaigns,
    - intrusion sets
- Different methodologies to do this

Dissemination

Assessment = confidence + analysis + evidence + sources

- **Know your Audience!**
- **Intended Audience**
    - Intended audience and their goals determine the type of threat intelligence generated and how it is used (strategic, operational, tactical)
- **Constructing Assessments**

- Can be viewed as an equation
- **Assessment = confidence + analysis + evidence + sources**
- **We assess with that because of**
  - High Confidence:
    - Supported by preponderance of evidence
    - No evidence against
    - All but certain
  - Moderate Confidence
    - Significant evidence missing
    - New evidence could invalidate
  - Low Confidence
    - Other equally likely hypotheses exist
    - Little evidence available to support