Advancing Cyber Intelligence Practices Through the SEI’s Consortium

SEI Emerging Technology Center

Jay McAllister
Melissa Kasan Ludwick
Agenda

The Cyber Intelligence Research Consortium
  • Purpose
  • Origins
  • Offerings

Demonstrations
  • Evaluating Intelligence
  • Evaluating Analysts

Future Work
  • How-To Guides
  • Cyber Threat Baseline
  • Crisis Simulation
Advancing Cyber Intelligence Practices
Through the SEI’s Consortium

The Cyber Intelligence Research Consortium
Purpose

The Consortium is a member-funded initiative that researches and develops technical solutions and analytical practices to advance the art and science of cyber intelligence

Cyber intelligence: The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making

It was formed because government, industry, and academia were looking for…

• Access to cost-effective resources for cyber intelligence workforce development and technology scouting
• Awareness of analytical practices from all organizations, regardless of size and economic sector
• Insight into SEI and Carnegie Mellon skills and capabilities
Origins

Cyber Intelligence Tradecraft Project

- [www.sei.cmu.edu/etc/cyber-intelligence/citp](http://www.sei.cmu.edu/etc/cyber-intelligence/citp)
- Studied how 30 organizations from government, industry, and academia performed cyber intelligence

Overall finding

- Effective organizations balance the need to protect their network perimeters with the need to look beyond them for strategic insights

Deliverables

- Summary of Key Findings: Best practices and lessons learned
- Implementation Frameworks: How-to-guides for analysis
- White Paper: Practitioner core competencies and skills
## Offerings

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steering Committee</td>
<td>Guide Consortium activities and plan for future success</td>
</tr>
<tr>
<td>Cyber Threat Baseline</td>
<td>Anonymized research of members’ cyber threat environments to identify common challenges and associated best practices</td>
</tr>
<tr>
<td>Tradecraft Labs</td>
<td>Workshops to advance cyber intelligence capabilities and showcase relevant technologies</td>
</tr>
<tr>
<td>Implementation Frameworks</td>
<td>How-to guides for navigating key analytical practices and technologies</td>
</tr>
<tr>
<td>Crisis Simulation</td>
<td>Capture-the-flag exercise to apply analytical techniques and technologies to a simulated cyber attack</td>
</tr>
<tr>
<td>Intelligence Insights</td>
<td>Biweekly emails and bimonthly newsletters on topics relevant to the practice of cyber intelligence</td>
</tr>
</tbody>
</table>
Advancing Cyber Intelligence Practices Through the SEI’s Consortium

Offering Demonstrations
Evaluating Intelligence

Challenge

• Cyber intelligence is a phrase often used, but interpreted in many different ways, leading to a diverse output of threat analysis categorized as cyber intelligence

• Such output is difficult to evaluate and compare, stifling an organization’s ability to establish guidelines and goals

Solution

• An evaluation template based on standards observed during our research and set forth in U.S. Intelligence Community Directive Number 203

Template – Evaluating Intelligence

Assess the quality and thoroughness of an intelligence analyst’s work using a grading system based on points accumulated for criteria the analyst satisfies in an intelligence product.

Grading system

A: 17-16, B: 15-14, C: 13-12, D: 11-10, F: 9 and below

Criteria

- Objective
- Independent of political considerations
- Timely
- Based on all available sources
- Exhibiting proper standards of analytic tradecraft
Criteria - Objective

Worth 4 points

• Functions from an unbiased perspective
• Gives due regard to alternative perspectives
• Gives due regard to contrary reporting
• Acknowledges developments that necessitate adjustments to analytic judgments
Criteria – Independent of Political Considerations

Worth 2 points

• Provides objective assessments informed by available information

• Is not distorted or altered with the intent of supporting or advocating a particular policy, political viewpoint, or audience
Criteria - Timely

Worth 1 point
• Is actionable
Criteria – Based on All Available Sources

Worth 3 points

• Is informed by all relevant information that is available, including open source information
• Addresses where critical intelligence gaps exist
• Identifies appropriate collection, dissemination, and access strategies to fill the gaps
Criteria – Exhibiting Proper Standards of Analytic Tradecraft

Worth 7 points

• Properly describes the quality and reliability of the underlying sources
• Caveats and expresses confidence in analytic judgments
• Distinguishes between assumptions and judgments
• Demonstrates relevance to the stakeholder(s)
• Uses logical argumentation
• Exhibits consistency of analysis over time
• Makes judgments and assessments that are justified with supporting information
Evaluating Analysts

Challenge

• No analyst produces intelligence the same way, making it difficult to evaluate critical thinking and problem solving skills

Solution

• An evaluation template based on how analysts assess fictitious, ill-structured, and complex cyber threats presented through scenario-based exercises
Template – Evaluating Analysts

The template conveys a holistic approach to assessing cyber threats

- It consists of three components
  - Threat actor potential to execute the cyber threat
  - Organizational impact of the cyber threat on the target
  - Target exposure to the cyber threat because of potential vulnerabilities
Threat Actor Potential
(to execute the cyber threat)

### Capability

**Attack Methods**
- **Infrastructure**
  - Operational structures needed for success—hardware, software, or command and control
- **Technology**
  - Whether used or manipulated
- **Coding**
  - Nuances and personal preferences
- **Maturity**
  - According to the planning process and pre/post-threat activities
- **Targets**
  - General or specific—mass phishing data or exploiting a specific vulnerability
- **Timing**
  - Minutes, days, or years to act on the cyber threat

### Intent

**Resources**
- **Money**
  - For personnel, tools, training, or access
- **People**
  - Number and type of people involved—collaborators, teachers, mentors, or sponsors
- **Tools**
  - Open source and/or custom, and why
- **Training**
  - Type and quality

**Motive**
- **Intrinsic**
  - Personal rewards to act on the threat—bragging rights, knowledge, justify skills, satisfy boredom, patriotism, or hacktivist allegiance
- **Extrinsic**
  - External rewards to act on the threat—fame, money—or to avoid punishment

**Targeted Data**
- **Personally Identifiable Information (PII)**
  - Payment card data, social security numbers, or biometrics
- **Organizational Data**
  - Research and development information, business processes, or industrial control systems
Organizational Impact
(of the cyber threat on the target)

Operations

Direct Costs
- Incident Response
  Costs to perform an investigation, remediation, and forensics
- Downtime
  Business costs of a network-reliant service being unavailable—missed financial transactions or loss of potential product/services revenue
- Mitigation and/or Prevention
  Costs of additional hardware/software to stop current and future threats

Business Operations
- Supply Chain
  Costs associated with the inability to meet demand, delay to operations, and supplementing or replacing suppliers
- Logistics
  Cost of continuing business operations during and after an attack—rerouting communications, securing intellectual property, or upgrading processes
- Future Earnings
  How the threat affects R&D, product releases, acquisitions, or competitive advantage

Strategic Interests

Organizational Interests
- Strategic Planning
  How the threat affects the strategic vision—annual reports, operational policies, or mergers
- Stakeholders
  Threat impact on shareholders, board of directors, or employees
- Culture
  How the threat affects legal/regulatory requirements, network access, or work-from-home policies

External Interests
- Market/Industry
  Threat impact on target’s competitors and industry, both domestic and foreign
- Geopolitical
  How the threat affects political relationships and local/national/global economies
- Partnerships
  Threat impact on target’s third party providers, information sharing agreements, or other business relationships
- Brand Reputation
  How the threat affects the target’s brand and its implications on public opinion
Target Exposure
(to the cyber threat because of potential vulnerabilities)

People

Relevance

Internet Presence
Susceptible witting and unwitting information

target-related individuals put online and their popularity on blogs/social media

Extracurricular Activities
Vulnerabilities from these individuals roles with non-target entities—non-profits, activist groups, or local/national politics

Motive
The reasons for why such individuals are susceptible to the cyber threat—ignorance, financial trouble, disgruntlement, or boredom

Access

Physical
Vulnerabilities from target-related individuals ability to access the target’s tangible aspects—office space, transportation, or equipment

Network
Susceptible administrative privileges or sensitive data access provided to such individuals

Position
How threat actors exploit the different roles these individuals play for the target—network administrator, senior leader, or rank-and-file employee

Abnormal Activities
Deviations from normal physical, network, or position-based activities of key target-related individuals can signify potential vulnerabilities

Cyber Footprint

Infrastructure

Hardware
Risks emanating from where network appliances, workstations, and third party equipment connect to the target’s network

Software
Risks associated with the target relying on particular software for day-to-day operations, providing access to high-risk software, and detecting software vulnerability exploitation

Supply Chain
How the cyber threat affects the target’s acquisition, implementation, maintenance, and discontinuation of hardware and software

Internet Presence

Website
How the threat actor can leverage the target’s website—compromise content, collect data, or deny access

Social Media
Risks associated with the target’s use of it for organizational activities—marketing, customer service, or product placement

Additional Services
Risks emanating from the target’s use of FTP, Telnet, VPN, webmail, remote desktop, and other web-based services
Advancing Cyber Intelligence Practices Through the SEI’s Consortium

Future Work
Future Work

Automation of templates for evaluating intelligence and analysts

Implementation frameworks

- Predictive analytics
- Red teaming
- Intelligence collection management

Interactive platform for learning how to build a cyber intelligence capability

Crisis simulation
Contact Information

Presenter / Point of Contact
Jay McAllister
Senior Analyst
Telephone: +1 412.268.9193
Email: jjmcallister@sei.cmu.edu
Twitter: @sei_etc

Customer Relations
Email: info@sei.cmu.edu
Telephone: +1 412.268.5800
SEI Phone: +1 412.268.5800
SEI Fax: +1 412.268.6257