Cyber Threat Intelligence: Integrating the Intelligence Cycle

Elias Fox and Michael Norkus, Cyber Threat Intelligence Analysts

January 2017
The internet offers global connectivity to all the good things contained therein…and to all the bad things, as well.
Risk and opportunity management is a core function of every organization. Situational awareness is key to improved business decisions.
The Value of Cyber Threat Intelligence

Proper CTI should extend our vision and allow us to take steps that normally we would not.
Noblis Definition and Vision

Requirements-Driven Methodology

Traditional and Non-Traditional Intelligence Techniques

Holistic Cyber Threat Picture

Proactively Diminish Threats

Tactical Operational Strategic

Technical Expertise Analytic Tradecraft

Timely Accurate

Our vision incorporates network defense data and all-source intelligence to provide a holistic cyber threat picture.
The Three Levels of Threat Intelligence

“tactics are concerned with ‘doing the job right,’ and higher levels of strategy are concerned with ‘doing the right job’.” (Drew and Snow, 2006)
Cyber Threat Intelligence: A Holistic Picture

- Tactical
- Operational
- Strategic

Reactive

- Focused on Today/Tomorrow Feeds and IoCs
- Focused on Next Week/Month Adversary TTP
- Focused on Years Ahead Planning and Risk
Man in the Middle
DDoS
Social Engineering

Proactive Defense Measures!
Risk Mitigation:
What do we have that they want?
How do we protect our data?
Incorporating the traditional Intelligence Cycle into analysts’ workflow will expand the precision with which we can identify, defend against, and prevent cyber threats.
Integrating CTI, network operations and security, and business operations enables more effective decisions to balance risk, response, and allocation of resources.
Incorporating the Traditional Intelligence Cycle into analysts’ workflow allows the company to proactively identify threats and intelligence gaps.
Incorporating the Intelligence Cycle into analysts’ workflow allows the company to proactively identify threats and intelligence gaps.
A Monitoring and Response framework links the organization’s intelligence support with its network operations division – and drives information flow.
Cyber Threat Intelligence: A Holistic Picture

- Tactical
- Operational
- Strategic

Proactive

- Focused on Today/Tomorrow Feeds and IoCs
- Focused on Next Week/Month Adversary TTP
- Focused on Years Ahead Planning and Risk
Benefits of Integrating People and Tools

- Dissemination
- Dissemination Management
- Collection Management
- Collection
- Cyber All-Source Analysis
- Cyber Threat Triage
- Analysis and Production
- Processing and Exploitation
- Requirements and Planning
Knowledge, Skills, and Abilities: Integrating People

Just as people and tools are behind these threats, people and tools are required to resolve these threats – automation and machine learning provide only half of the solution.
Knowledge, Skills, and Abilities: Integrating People

Just as people and tools are behind these threats, people and tools are required to resolve these threats – automation and machine learning provide only half of the solution.
Now remember, Proactive Man says: