Prescriptive Risk Solutions, LLC

April 2017

CISO Series on Today's Critical Issues

Cyber Threat Intelligence

By Tari Schreider C|CISO, CHS-III, CRISC, ITIL™ v3, MBCI, MCRP, SSCP

Chief Cybersecurity Strategist & Author

Prescriptive Risk Solutions, LLC.

EC-Council

http://ciso.eccouncil.org/

Cyber Threat Intelligence Overview

Organizations ready to move to the next level of threat management can turn to external intelligence services to aid in their threat decision making process. Actionable intelligence is key to guiding threat management investments. Dedicating personnel to scour the Internet looking for threat intelligence or gleaning threat data from Information Sharing and Analysis Center (ISAC) alerts has proven ineffective. The alternative is to outsource threat intelligence gathering to companies specializing in sourcing threat information.

For over twenty years, companies have offered threat intelligence services to help organizations stay ahead of the threat curve. Early services relied on manually sifting through vendor vulnerability reports. Now, intelligence services are faster, more in-depth and highly targeted toward advanced persistent threats. Today's services have solved the relevance problem that plagued this industry from sometime. This ensures that only threat information aligned to an organization's attack surface or industry makes it to the CISO's desk.

Companies found themselves with multiple threat feeds or services that resulted in various levels of redundancy. Redundancies caused multiple alerts for the same threat costing valuable research time to sort out the overlap. As a user of several of these services over the years, I was disappointed with how many low value alerts where rated as high. I also found much of the reporting run of the mill already known threats.

CYBER THREAT INTELLIGENCE REQUIREMENTS

Requirements guide the gathering of threat intelligence and its analysis to make it actionable. Documenting a proper set of requirements will help you:

- ✓ Track bad actors targeting your organization.
- ✓ Acquire threat information aligned to your attack surface.
- ✓ Know which hacktivist organization targets your industry.
- ✓ Understand the types of techniques adversaries use to exploit vulnerabilities in your enterprise.

THREAT INTELLIGENCE SUBSCRIPTION SERVICES

According to IT-Harvest, the Threat Intelligence Market reached $340 million in 2016 growing at 84% CAGR. The market estimate is set to reach $626 million by 2017. Presently, there are nearly 30 providers of cybersecurity intelligence services of various flavors. Some services focus on providing intelligence on professional hackers and hacktivists, while others focus reporting on emerging threats and vulnerabilities based on your attack surface.

Approaches vary widely from those firms that provide human intelligence harvested from the deep web to others who provide sophisticated platforms that integrate threat intelligence directly as a feed to your security information and event management (SIEM) solution.

The following are the main players in this market:

COMPANY	SERVICE
Accenture	iDefense Security Intelligence Services
ANOMALI	ThreatStream
Centripetal Networks	QuickThreat®
Control Risks Group Holdings Ltd	Cyber Threat Intelligence
CrowdStrike	Falcon Intelligence
Digital Shadows Ltd	Digital Shadows SearchLight™
FireEye, Inc.	iSIGHT Intelligence Subscriptions
Flashpoint	Advisory Services
Intel 471 Inc.	INTEL471
Ixia	Application and Threat Intelligence
Kaspersky Lab	Kaspersky Security Intelligence Services
LookingGlass Cyber Threat Intelligence Group	Threat Intelligence Services
NSFOCUS	NSFOCUS Threat Intelligence Subscription Service
NSS Labs	CAWS Cyber Threat Protection Platform
Proofpoint, Inc.	Proofpoint ET Intelligence
SurfWatch Labs, Inc.	SurfWatch Threat Analyst
Symantec Corporation	DeepSight™ Intelligence
ThreatConnect, Inc.	ThreatConnect
ThreatQuotient, Inc.	ThreatQ

Cyber Threat Intelligence Program Use Cases

If you are still wondering how an intelligence capability would benefit your organization, I have highlighted several tactical use cases:

- Countermeasures Alignment – Countermeasures rely on rules, filters and signatures to be effective. Intelligence provides advanced warning of specific threats that countermeasures can address if properly configured. Using high quality intelligence reduces false positives.

- Incident Response (IR) – The IR team can use threat intelligence to validate indicators that triggered alarms accelerating response time. The intelligence can provide valuable data about a threat's origin, behavior and associated adversaries.

- SecOps – Threat intelligence can assist SecOps personnel to triage SIEM alerts through the attachment of risk score tags. Threat intelligence systems can interface directly with the SIEM to automate alert prioritization.

- System Hygiene – Patching systems is a significant effort for any organization and knowing what and when to patch can save precious resources, time and budget. Most organizations operate on a patching backlog and prioritizing patching efforts allows you to focus on your most at risk systems.

THREAT INTELLIGENCE STANDARDIZATION

A long-standing problem with the threat intelligence community was competing threat reporting formats. This changed in 2016 when providers of cyber threat intelligence agreed to support a single standard. The OASIS Cyber Threat Intelligence (CTI) Technical Committee's was subsequently formed with the charter to define a set of protocols to address the need to share cyber threat intelligence. The first step was to transition specifications maintained by US Department of Homeland Security (DHS) for development and standardization under the OASIS open standards process. These included STIX (Structured Threat Information Expression), TAXII (Trusted Automated Exchange of Indicator Information) and CybOX (Cyber Observable Expression).

INDICATOR OF COMPROMISE VS. INDICATOR OF ATTACK

Indicators of attack are what we are most familiar as many of our legacy countermeasures such as end-point detection systems use this approach. They alert on evidence that a compromise has occurred before they begin to protect. Here the focus is on IP addresses, malware, vulnerabilities, etc. This approach can be too late in many cases.

Indicators of attack however, focus on the intent of an attacker. For example are they probing our network, is the IP address associated with a known aggressor, have we seen an uptick in suspicious emails, is this happening with some regularity, etc. Here we are concerned with code execution, external communication with command and controls systems, lateral movement, etc.

There is a need for both today and you will need to ensure your intelligence program accommodates threat gathering for indicators of compromise as well as compromises of attack.

THREAT INTELLIGENCE SOURCES

There are four main sources of threat intelligence to feed your program. They range from internally produced to open source.

- Internal – Produced from access and security event logs, firewall and IDS/IPS logs and scan reports correlated and aggregated by your SIEM.
- Commercial – Subscription service provided as an appliance, cloud application or platform to provide customized threat intelligence.
- Open Source – Free sources of threat intelligence from US CERT, Internet Storm Center, Zeus Tracker, etc.
- Information Sharing and Analyses Centers (ISAC) – Industry focused threat intelligence sharing provided on a subscription basis. Over 20 ISACs are available covering all designated critical infrastructure industries.

Cyber Threat Intelligence Resources

If you are serious about creating an intelligence capability within your organization you may wish to access a curated list of cyber threat intelligence resources maintained on GitHub organized in the following manner:

- ✓ Sources
- ✓ Formats
- ✓ Frameworks
- ✓ Tools
- ✓ Research, Standards & Books

Conclusion

As the CISO for your organization, you have a responsibility to understand the near-term and long-term threat landscape. Understanding begins with a strategy to address today's threats as well as the threats of tomorrow. The insight you will require comes from a cyber threat intelligence capability, which should be an integral part of your threat management program.

CISOs will find it difficult to gather the intelligence necessary to protect their information and assets from in house efforts alone. Subscribing to a threat intelligence service is almost an operational imperative today. Choosing the right one is the trick, with nearly 30 to choose, which one will give you the most actionable intelligence. Trialing several based on specific use cases will prove invaluable to the selection process.

ABOUT THE AUTHOR

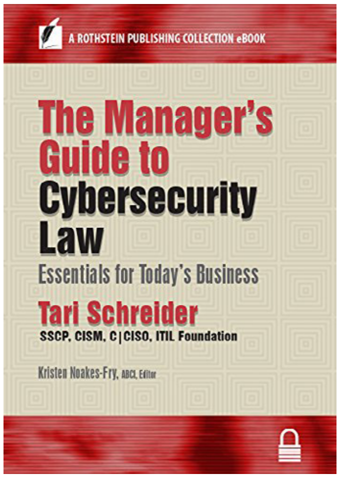
TARI SCHREIDER

C|CISO, CHS-III, CRISC, ITIL™ v3, MBCI, MCRP, SSCP

Chief Cybersecurity Strategist & Author
Prescriptive Risk Solutions, LLC.
Atlanta, GA - Cheyenne, WY

www.prescriptiverisksolutions.com
tari@prescriptiverisksolutions.com

M: Atlanta – 678.595.2818
M: Cheyenne – 307.215.1330



A ROTHSTEIN PUBLISHING COLLECTION eBOOK

The Manager's Guide to Cybersecurity Law

Essentials for Today's Business

Tari Schreider

SSCP, CISM, C|CISO, ITIL Foundation

Kristen Noakes-Fry, ABCI, Editor

The Manager's Guide
to Cybersecurity Law

Qualifies for Five (5) EC-Council ECUs.