STANDARD INFORMATION SHARING FORMATS

Will Semple
Head of Threat and Vulnerability Management
New York Stock Exchange

NYSE EURONEXT

AGENDA

- Information Sharing from the Practitioner's view
- Changing the focus from Risk to Threat
- Why Share? Lead with Intelligence
- Threat vs Privacy


Threat
Information
Sharing
observable
maec
confirmed
behavior
consumable
effort
Threat Actor
Privacy
language
specific
Indicator
vulnerabilities
Community
Cyber
Intelligence
Structure
Expression
cve
source
Security
Target
Common
potential
data
cybox
oval
takii
intent
appropriate
stix
legal
exchange
audit
regulator
patterns
enumeration
collaboration
implementation
standardised
management
incident
context
communication
weaknesses
motivation
operations
attack
malware
adversary
response
Campaign
public relations

THE CHALLANGE…

How to Effectively utilize Cyber Threat Intelligence Information to identify Threat or the intent to compromise an organisation and communicate the Threat to the organisation and community.

- **Consume Cyber Security Intelligence Information**
  - Information in which Cyber Threat teams have access to as part of Cyber Threat Operations
- **Standardize & Normalize Cyber Threat Intelligence**
  - Information which can be used in a repeatable, reliable and weighted fashion
- **Community & Partner Information Exchange**
  - Ability to share and communicate Cyber Threat Information in a standardized and efficient manner
- **Apply Integrity & Fidelity Rating**
  - Verify & Validate Cyber Threat Intelligence Information
- **Understand Motivation and Intent of Threat Actors**
  - Apply situational context to campaign of attack

MAKING USE OF THE INFORMATION

- **Information Exchange**
  - Ability to share threat information with the community via the STIX framework & associated TAXII protocols.
- **Use of Threat Information**
  - Intelligence led Cyber Threat Operations that can effectively detect and mitigate malicious actors and/or campaigns.
  - 'Threat Summery' or 'Brief' to assist with identification, mitigation and remediation of malicious acts
- **Threat Actor Motivation**
  - Ability to determine the ***'How?'*** And ***'Why?'*** motivation indicators relating to specific malicious activity.
  - Understand Intent of the Threat Actor
- **Greater Threat Awareness**
  - Enable Cyber Threat Operations to determine the threat landscape more efficiently and effectively
- **Metrics**
  - Ability to evaluate effectiveness of intelligence sources .
  - Threat Visualizations
  - Threat Summary
  - Making Cyber Threat Measurable

CHANGING FOCUS FROM RISK TO THREAT

ITS ABOUT PERSPECTIVE

- This conversation is not about Risk, its about Threat
- Risk Assessments are the hidden weapon of the Attacker
- Threats are operational
- Risks can be easy to mitigate, Threats not so much

ITS ABOUT CHOICE

"With Risk you have a choice to accept it. With Threat it is thrust upon you regardless if you want it or not!"

Risk is the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome). The notion implies that a choice having an influence on the outcome sometimes exists

ISO27005: **Threat** is a potential cause of an incident, that may result in harm of systems and organization

A **threat** is an act of coercion wherein an act is proposed to elicit a negative response.

WHY SHARE?

LEAD WITH INTELLIGENCE

"An Intelligence led response to Cyber Threat will provide a mechanism to allow both the public and private sectors to formulate predictive and pro-active plans to mitigate the intent of groups that wish to undermine our Critical National Infrastructure and damage our economy."

REDUCE CAPABILITY

Sharing cyber threat information within a community will reduce the ability of a bad actor to successfully execute a campaign

PREVENTION – THE OPPORTUNITY

One members Threat detection becomes
a communities Threat prevention

THREAT VS PRIVACY

CONSIDERING PRIVACY

Privacy Concern Barriers for Private Sector

Disclosure Transparency Trust Brand Damage

Competitive Advantage Intellectual Property

Service Privacy Assurance

- Privacy protection measures
- Data confidentiality markings
- No regulator recourse

Potential Consequence

Selective Sharing Delayed Adoption Increased Threat

Reduced Effectiveness Financial Impact

THREAT INFORMATION SHARING

- Privacy is a valid concern
- The opportunity is to create policy controls to allow privacy
- Make it attractive to join the community, not an overhead

Enabling organizations to collaborate and communicate Cyber Threat Information in a standard format with appreciation for the wider implications of what the data can mean to their business if it is misused will open the door for a successful service

Thank You

wsemple@nyx.com
Linkedin/willsemple
@willsemple