CONTROLLING YOUR OWN BATTLESPACE

From Threat Response Teams
To Threat Intelligence Teams
Agenda

• Motivations

• The Intelligence Process

• The Cyber Kill Chain Approach

• Indicators of Compromise

• Information Sharing

• Takeaways
Today’s Threat Landscape

- Organized attackers
- Increasing volume
- Sophisticated

Remediation is broken
Limited correlation across disjointed security technologies
Limited security expertise

Must prevent attacks across perimeter, cloud and endpoint

CSO challenges
Information Overload

Detection-focused

Alert Overload

Manual Response Required

Enterprise Network

UTM/Blades

DNS protection for outbound DNS

DNS protection cloud

Internet

Anti-APT for Email APTs

Anti-APT for HTTP APTs

Anti-APT cloud

Network AV

Endpoint AV

DNS Alert

Endpoint Alert

Web Alert

SMTP Alert

DNS Alert

SMTP Alert

SMTP Alert

Web Alert

DNS Alert

SMTP Alert

Web Alert

AV Alert

Web Alert

AV Alert

Web Alert

DNS Alert

SMTP Alert

Vendor 1

Vendor 2

Vendor 3

Vendor 4
Cyber Kill Chain

Relationship of Data, Information, and Intelligence

Operational Environment  
Collection  
Data  
Processing and Exploitation  
Information  
Analysis and Production  
Intelligence
Cyber Kill Chain
The Intelligence Process

The Intelligence Process

Evaluation

Dissemination and Integration

Planning and Direction

Collection

Processing and Exploitation

Analysis and Production

and Feedback

Mission
The Paradox of Warning

Friendly intelligence determines adversary intention.

Friendly intelligence detects indications.

Friendly forces react to adversary activity.

Friendly intelligence provides warning.

Adversary intelligence provides warning.

Adversary intelligence detects indications.

Adversary intelligence determines friendly intention.

Adversary adopts different course of action.
Indicators of Compromise

Figure 1: Indicator life cycle states and transitions
Indicators of Compromise
Information Sharing

Some of the organizations contributing to the STIX conversation:

- Microsoft Interflow
- Financial Services ISAC
- REN-ISAC
- ES ISAC
- ThreatConnect
- US-CERT
Takeaways

• Move onus of security ops from reactionary to proactive
  (Incident Response to Threat Intelligence)

• Place and tune your defensive sensors appropriately
  Use the intelligence feedback loop

• Don’t do it alone