A New Security Dimension:
Industry Experience Using Open Standards to Accelerate Threat Response

Jason Corbin
VP Product Management and Strategy
IBM Security
Cyber Threat Intelligence Refresher

- STIX: Payload
- TAXII: Protocols
- CybOX: Transport
Why IBM is interested

Source: IBM MSS, “What surfaces from the deep, dark web”
Facilitate collaborative defense with actionable intelligence

**IBM Threat Protection System**


- **Endpoint Protection**
- **Network Protection**
- **Security Intelligence**

Push intelligence to enforcement points for timely protection

- Integration between IBM Security products and X-Force Exchange-sourced **actionable intelligence**
- Designed for **third-party integration** with support for STIX and TAXII, the established standard for automated threat intelligence sharing
- Leverage the **API** to connect threat intelligence to security products
IBM Threat Ecosystem

Share/Curate IOC Data
X-Force Exchange Collections

Publish IOC Data
CRE Response
Offense Sharing
Manual Reference Data Sharing

Consume IOC Data
Threat Engine Reference Data
A New Security Dimension: Industry Experience Using Open Standards to Accelerate Threat Response

Paul Kurtz
CEO, TruSTAR
Why Is Incident Sharing Important

The median number of days that threat groups were present on a victim's network prior to detection now stands at 205 - that’s 4920 hours! Damages can be done in minutes with 295,200 minutes to go.

Based on attacks observed by RiskAnalytics during 2014, 75% of attacks spread from Victim 0 to Victim 1 within one day (24 hours). Over 40% hit the second organization in less than an hour....” – 2015 Verizon Data Breach Investigations Report
Current State of Info Sharing

– **Ad hoc:** It works in some places for some organizations, but most are left on their own

– **Perishable:** By the time we exchange the really valuable information, our attackers have already moved on to the next attack

– **Unproductive:** We are not seeing the results we want to see from the efforts we do have in place
Why are we fighting back alone?

Legal
Concerns over disclosing personally identifiable information, IP and discovery.

Market
Concerns over brand reputation and financial implications of disclosing a breach.

Government
Concerns over anti-trust violations and/or being seen as in bed with government.
Enabling “Connective Defense”

- Ability to quickly sanitize a report of attributable data or personally identifiable information
- Ability to share incidents anonymously with vetted businesses
- Real time correlation of incidents giving value back to the sharer and early warning to others
- Secure collaboration among businesses to solve problems
- Real time alerting to information of interest based on a user’s role
- Trend reporting that enables businesses to understand the how attacks are morphing and migrating across networks
A New Security Dimension:
*Industry Experience Using Open Standards to Accelerate Threat Response*

Ted Julian
CoFounder & VP Product Management
Resilient Systems
Pioneers in incident response

- Founded in 2010, created the first Incident Response Platform (IRP)
- Winning awards for innovation — and so are our customers
- World leader in incident response management bringing together people, process and technology
- Bruce Schneier, CTO — the leading security industry guru
- Headquartered in Cambridge, MA and London, UK
Resilient’s approach to IR

Brings together people, process and technology to transform, orchestrate and empower your incident response.
How Resilient Relates To TI

AUTOMATED ESCALATION
- SIEM
- EMAIL
- ENTRY WIZARD
- WEB FORM
- TROUBLE TICKETING

RESILIENT IRP MODULES
- PRIVACY
- SECURITY
- ACTION

INFRASTRUCTURE INTEGRATION
- Directory
- Endpoint forensics
- Threat Intelligence
- Endpoint controls
- Network controls

DASHBOARDS & REPORTING
- TEAM UTILIZATION
- CSO DASHBOARD
- INCIDENT TIMELINE STATUS
- INCIDENTS BY TYPE OVER TIME
- CUSTOM DASHBOARDS & REPORTS
How Resilient Operationalizes TI

- Multiple threat feeds
- Automatic lookup across all feeds as IOCs are added

Relevant intel, automatically presented, with context to unfolding events
- Orchestrated response
- Further enrichment
- Mitigation

Structured and streamlined, potentially automated response
Barriers to info sharing

• Uh, people have to share it ;-)
• Once shared, it must be valuable
  – It has to be relevant
    • Few can hunt, so how do the rest find out?
  – It has to be actionable
    • Now that I know, what specifically should I do?
    • Can I act?: people, process, technology
How To Break Down the Barriers

• Incident driven, threat specific, vertical market agnostic
• The more you give, the more you get
Vision For A Shared Future

• Quick and decisive response
  – Emerging events automatically alerted and enriched by the community
  – Targeted, proven, orchestrated remediation

• Peer benchmarking and improvement
  – Here’s where you are at and here’s how to get better

• Turn the tables on the bad guys
  – Collective response, not by one by one
#BorderlessCyber

Questions ?