IBM approach to Cyber Security
Security has an intrinsic value, how to mitigate risks

Domenico Raguseo
Manager of Europe Technical Sales and Solutions

Follow  @domenicoraguseo
Contact  dom.raguseo@it.ibm.com
Connect  https://www.linkedin.com/in/draguseo

© 2015 IBM Corporation
SQL Injection
Dos or Ddos
Malware or Botnet
Scanning
Spam
Command and Control
Watering Hole
Disenfranchised
Vulnerabilities (i.e. ShellShock ... )

- Central strategic targets
- Takeover social profiles
- Zero day drive by download
- Mobile malware
Security teams are using multiple sources of intelligence

65% of enterprise firms use external threat intelligence to enhance their security decision making.¹

However, security teams lack critical support to make the most of these resources.

- Analysts can’t separate the signal from the noise
- Data is gathered from untrusted sources
- It takes too long to make information actionable

¹ Source: ESG Global
Introducing IBM X-Force Exchange

IBM X-Force Exchange is:

**OPEN**
a robust platform with access to a wealth of threat intelligence data

**ACTIONABLE**
an integrated solution to help quickly stop threats

**SOCIAL**
a collaborative platform for sharing threat intelligence

Backed by the reputation and scale of IBM X-Force
OPEN

A robust platform with access to a wealth of threat intelligence data

Leverage the scale of IBM Security and partner ecosystem

Quickly gain access to threat data from curated sources:

- **Over 700 terabytes** of machine-generated intelligence from crawler robots, honeypots, darknets, and spamtraps
- **Multiple** third party and partner sources of intelligence
- Up to **thousands of malicious indicators** classified every hour

Human intelligence adds context to machine-generated data:

- Insights from **security experts**, including industry peers, IBM X-Force, and IBM Security professionals
- **Collaborative interface** to organize and annotate findings, bringing priority information to the forefront
**ACTIONABLE**
An integrated solution to help quickly stop threats

**IBM Threat Protection System**


IBM Security
- Trusteer Apex
- Network Protection
- XGS
- QRadar
- Security Intelligence

**STIX / TAXII**
(future feature)

**API**

**3rd Party Products**

**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 planned future support for STIX and TAXII, the established standard for automated threat intelligence sharing
- Leverage the API to connect threat intelligence to security products
SOCIAL
A collaborative platform for sharing threat intelligence

Add context to threats via peer collaboration
- **Connect** with industry peers to validate findings
- **Share** a collection of Indicators of Compromise (IOCs) to aid in forensic investigations

**INCIDENT RESPONDE**
- Discovers a new malware domain and marks it as malicious in the X-Force Exchange

**SECURITY ANALYST**
- Finds the domain and applies blocking rules to quickly stop malicious traffic. Shares with his CISO using the Exchange

**CISO**
- Adds the domain to a public collection named “Malicious Traffic Sources Targeting Financial Industry” to share with industry peers

**IBM X-FORCE**
- For the first time, clients can interact with IBM X-Force security researchers and experts directly
IBM Security: Market-changing milestones

- **2013**
  - Trusteer is acquired for mobile and application security, counter-fraud and malware detection.

- **2014**
  - Crossidea is acquired for ID Governance.

**IBM Security Investment**
- 6,000+ IBM Security experts worldwide
- 3,000+ IBM security patents
- 4,000+ IBM managed security services clients worldwide
- 25 IBM Security Labs worldwide
IBM Security Framework

Helping customers to protect from advance fraud, malware, mobile and application attacks

Helping financial institutions to protect customer transactions from advanced frauds

Helping financial institutions to protect customer transactions from advanced frauds

Enterprise-wide solutions for helping secure the privacy and integrity of trusted information in your data center

Reducing the cost of developing more secure applications

Help guard against sophisticated attacks with insight into users, content and applications
Security Intelligence and Analytics

Helping customers to protect from advanced fraud, malware, mobile and application attacks

Portfolio Overview

QRadar SIEM
- Integrated log, threat, compliance management
- Asset profiling and flow analytics
- Offense management and workflow

QRadar Risk Manager
- Predictive threat modeling and simulation
- Scalable configuration monitoring and audit
- Advanced threat and impact analysis

QRadar Log Manager
- Turnkey log management
- Upgradeable to enterprise SIEM

Vulnerability Manager

Forensic
**Advanced Fraud Protection**

**Area of Focus**

Helping financial institutions to protect customer transactions from advanced frauds

- **Security Intelligence and Analytics**
- **Advanced Fraud Protection**
- **Advanced Security and Threat Research**

**Portfolio Overview**

**Trusteer Pinpoint Malware**
- 100% accurate clientless detection of active MitB malware on users’ devices
- Minimum impact on existing infrastructure

**Trusteer Pinpoint ATO**
- Detect and protect from Account Take Over frauds
- Conclusive criminal access detection by correlating device fingerprint and account compromise history
- Minimum impact on existing infrastructure

**Trusteer Rapport**
- Compact software agent that prevents malware and Phishing attacks

**Trusteer Mobile**
- Endpoint solutions for detecting malware, jailbreak, and other mobile risk factors
- Out-of-Band Authentication

© 2015 IBM Corporation
Manage and extend enterprise identity context across security domains with comprehensive Identity Intelligence

Portfolio Overview

IBM Security Identity Manager *
- Automate the creation, modification, and termination of users throughout the lifecycle
- Identity control including role management and auditing

IBM Security Access Manager Family *
- Automates sign-on and authentication to enterprise web applications and services
- Entitlement management for fine-grained access enforcement

IBM Security zSecure suite *
- User friendly layer over RACF to improve administration and reporting
- Monitor, audit and report on security events and exposures on mainframes

IBM Security Identity Governance
Portfolio Overview

IBM InfoSphere Guardium Product Family

- Database Activity Monitoring – continuously monitor and block unauthorized access to databases
- Privileged User Monitoring – detect or block malicious or unapproved activity by DBAs, developers and outsourced personnel
- Database Leak Prevention – help detect and block leakage in the data center
- Database Vulnerability Assessment – scan databases to detect vulnerabilities and take action
- Audit and Validate Compliance – simplify SOX, PCI-DSS, and Data Privacy processes with pre-configured reports and automated workflows

IBM Security Key Lifecycle Manager

- Centralize and automate the encryption key management process
- Simplify administration with an intuitive user interface for configuration and management
Applications

Area of Focus

Reducing the cost of developing more secure applications

<table>
<thead>
<tr>
<th>Portfolio Overview</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AppScan Enterprise Edition</strong></td>
<td></td>
</tr>
<tr>
<td>• Enterprise-class solution for application security testing and risk management with governance and collaboration</td>
<td></td>
</tr>
<tr>
<td>• Multi-user solution providing simultaneous security scanning and centralized reporting</td>
<td></td>
</tr>
<tr>
<td><strong>AppScan Standard Edition</strong></td>
<td></td>
</tr>
<tr>
<td>• Desktop solution to automate web application security testing for IT Security, auditors, and penetration testers</td>
<td></td>
</tr>
<tr>
<td><strong>AppScan Source Edition</strong></td>
<td></td>
</tr>
<tr>
<td>• Adds source code analysis to AppScan Enterprise with static application security testing</td>
<td></td>
</tr>
</tbody>
</table>
Help guard against sophisticated attacks with insight into users, content and applications

IBM Security
Network Intrusion Prevention (IPS)
• Delivers Advanced Threat Detection and Prevention to help stop targeted attacks against high value assets
• Proactively improves protection with IBM Virtual Patch® technology
• Helps protect web applications from threats such as SQL Injection and Cross-site Scripting attacks
• Integrated Data Loss Prevention (DLP) monitors data security risks throughout your network
• Provides Ahead of the Threat® protection backed by world renowned IBM X-Force Research

IBM Security SiteProtector
• Provides central management of security devices to control policies, events, analysis and reporting for your business

Endpoint Management & Fiberlink