Security Intelligence – an effective response to evolving cyber-attacks

Cliff Wilson – Associate Partner, IBM Security UKI

cliff.Wilson@uk.ibm.com

ISACA Event, Salford - February 2016

IBM is a member of both of these schemes:
- CSIR – CESG/CPNI scheme (Networks of national significance)
- CREST – CIR (Industry, academia and private or public sector)

For further details on these services, or if you have an incident, contact IBM’s Cyber Incident Response team on:
01475-898-201 Email: ukcir@uk.ibm.com
Organizations today face a growing range of cyber adversaries...

- The number and variety of new adversaries and threats continues to grow.
- Old threats don’t always disappear – while new threats continue to add to the total landscape.

£1.46m - £3.14m Avg.
2015 Attack Targets (Sept)

Source Hackmageddon 2015

Source IBM X-Force 2015
Attacker motivation and sophistication are evolving rapidly

- Attackers have more resources – and, crucially, TIME
- Effective off-the-shelf tools are available for sale
- Many breaches go un-noticed for increasingly long periods
- They will keep trying until they get in…
SHODAN Realtime attacks demo (2015) – This tool can be used to your advantage in a Security Intelligence context.
A perfect security storm is brewing...

73% of security executives have cloud and mobile concerns

614% Mobile malware growth in just one year

83% of enterprises have difficulty finding the security skills they need

85 security tools from 45 vendors

COMPLIANCE
Growing need to address a steadily increasing number of mandates

- National regulations
- Industry standards
- Local mandates
- Internal standards
- Geography Standards (EU)

2015 IBM CISO Survey

2015 Juniper Mobile Threat Report

2015 ESG Research
Compliance – major changes lie ahead!

GDPR – General Data Protection Regulation (protecting “Data Subjects and Personal Data”)

**Impact of the General Data Protection Regulation at a Glance**

- **Expanded scope**: Any organisation that processes data of EU citizens must comply, no matter where they are located or data is stored.
- **Personal data**: The definition of sensitive personal data has been expanded to include genetic and biometric data, as well as online identifiers such as IP addresses or cookie identifiers, as well as other identifiers such as RFID tags.
- **Breach notification**: Data protection authorities must be notified of a breach within 72 hours of its discovery unless the breach is unlikely to result in a risk for the rights and freedoms of individuals. Records must be kept of all breaches that the authorities are not notified about.
- **Where the breach is likely to impact the rights and freedoms of individuals, data subjects must be notified without undue delay.**
- **Sanctions**: Data protection authorities can impose fines for non-compliance of up to 4% of an organisation’s global revenue or 20 million euros, whichever is higher. A 2% fine or 10 million euros, whichever is higher, is applicable for more minor breaches.
- **Data protection officer**: A data protection officer must be appointed by organisations with more than 250 employees or that holds 5,000 records or more. SMEs for which data processing is not a core activity are exempt from this requirement.
- **Data protection impact assessments**: Where processing is deemed to be high risk for the rights of individuals, organisations must conduct a data protection assessment prior to processing. The assessment must detail the safeguards, security measures and mechanisms put in place to address risk and ensure compliance with the regulation.

Source: Bloor White Paper Jan 2016

- GDPR and NIS are coming! Get a good understanding of these ASAP
- Both will have major impact on our customers
- IBM are well placed to help customers prepare...
- Note the sanctions/penalties! This WILL get the attention of the C-suite – it may even drive some players/investors out of the market!

NIS – Network and Information Security Directive (everything else?)
A staggering, and growing, amount of security event data has to be collected and analysed, real-time

Security events

- **Annual**: 91,765,453
- **Monthly**: 7,647,121
- **Weekly**: 1,764,121

Security attacks

- **Annual**: 16,857
- **Monthly**: 1,405
- **Weekly**: 324

Security incidents

- **Annual**: 109.37
- **Monthly**: 9.11
- **Weekly**: 2.10

Security Intelligence

- Correlation and analytics tools
- Human security analysts

**Events: up 12% year on year to 91m**

Observable occurrences in a system or network

**Attacks: Increased efficiencies achieved**

More efficiency in security processing to help clients focus on identified malicious events

**Incidents: up 22% year on year**

Attacks deemed worthy of deeper investigation
The old tools just don’t cut it anymore
- It takes around 4.4 days of effort, on average, to investigate a Security breach

First-generation SIEM products are now *obsolete*:

- Little or no network activity monitoring
- Not architected to scale
- No pre-exploit security awareness
- Reliance on signature-based detection
- Too slow to deploy, too expensive to staff

Time for a new approach…
What is Security Intelligence – and why is it important?

“Security Intelligence is the real-time collection, normalisation, and analysis of the data generated by users, applications and infrastructure and information ingested from external sources - that impacts the IT security and risk posture of an enterprise.

The goal of Security Intelligence is to provide actionable and comprehensive insight that reduces risk and operational effort for any size organization.”

SI is important because it demonstrably helps to reduce risk and operational costs and significantly reduces the time taken to detect, analyse and deal with complex security attacks….

Source: IBM X-Force
Where did SI come from?

Security Intelligence solutions have evolved from a number of technologies you may be familiar with:

- SI builds on the data collection capabilities and compliance benefits of log management.

- The correlation, normalisation and analysis capabilities of SIEM (security information and event management) - across the organisation.

- The network visibility and advanced threat detection of NBAD (network behaviour anomaly detection).

- The ability to reduce breaches and ensure compliance provided by risk management, and

- The network traffic and application content insight afforded by network forensics.

AND

The ingestion, correlation and analysis of a broad range of security-related information from outside the organisation (Sector, Agency, Vendor, CUG, OS?)
What are the SI benefits?

Security intelligence reduces risk, facilitates compliance, shows demonstrable return on investment (ROI) and maximises investments in existing security technologies by:

• Distilling large amounts of information into an efficient decision-making process, reducing a billion pieces of data to a handful of action items

• “Operationalising” data collection and analysis through automation

• Delivering enterprise network visibility and clarity that enable organisations to understand and control risk, detect problems and prioritise remediation

• Validating that the organization has the right policies in place to comply with industry standards and governmental regulations

• Assuring that controls are in place to effectively enforce defined policies
The amount of internal and external threat intelligence data available can be overwhelming to decipher and operationalise without the right people, processes and technology. Advanced analytics and human intelligence must be applied and integrated into the organization to leverage the value of all the data/information collected.
No single participant can detect and contextualise all relevant information

- Join a community that shares Security Intelligence
- But, what to share? Should you trust what you receive?
- Standards (OS) are key:
  - **TAXII** – Trusted Automated Exchange of Indicator Information
    - A set of specs. For exchanging CT information
  - **CybOX** – Cyber Observable Expression
    - A common structure for representing cyber observables
  - **STIX** – Structured Threat Information Expression
    - A communications language for the representation of CT information
    - STIX VIZ gives you a nice visual representation of CTI as an XM
The intelligence has to be processed somewhere.
IBM security operations operating model: Hybrid
Incident postmortem scorecards

The incident postmortem scorecards provide visibility over security controls and the cost of service quality.

**Security Incident Post Mortem**

<table>
<thead>
<tr>
<th>Incident</th>
<th>Description</th>
<th>Phase 1 Recon</th>
<th>Phase 2 Weaponize</th>
<th>Phase 3 Delivery</th>
<th>Phase 4 Exploit</th>
<th>Phase 5 Install</th>
<th>Phase 6 C2</th>
<th>Phase 7 Actions</th>
<th>Actions &amp; Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC-001234</td>
<td>CRITICAL - exec laptop/mobile compromise</td>
<td>$1,500</td>
<td>$5,500</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10/12- Laptop was reimaged.</td>
</tr>
<tr>
<td>SOC-001388</td>
<td>HIGH - AP middleware servers exploit</td>
<td>$1,200</td>
<td>$2,500</td>
<td>$13,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10/17- patches scheduled for deployment during next maintenance window (10/24)</td>
</tr>
<tr>
<td>SOC-001412</td>
<td>CRITICAL - crown-jewel application server, unauthorized access</td>
<td>$5,000</td>
<td>$11,500</td>
<td>$17,000</td>
<td></td>
<td></td>
<td>$25,000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Kill Chain Legend**

- **Phase 1 - Reconnaissance**: research, identification and target selection
- **Phase 2 - Weaponization**: attack vector selected, tool kit
- **Phase 3 - Delivery**: transmission of attack to targeted environment
- **Phase 4 - Exploitation**: attack exploits target vulnerability
- **Phase 5 - Installation**: embedding attack/tool-kit into target environment
- **Phase 6 - Command & Control (C2)**: compromised targets are under control of attacker
- **Phase 7 - Actions on Intent**: attacker takes planned actions (i.e. data exfiltration)

Utilizing a kill-chain view of security incidents allows for complete understanding of the effectiveness of your controls, such as, which control processes can be improved, which control processes are ineffective, and then prioritize which controls should be implemented.
The security intelligence function

The security intelligence function must incorporate all elements of internal or external factors to drive enterprise awareness and response.

Features of this function include:

- Support to internal business stakeholders by collecting and publishing threat intelligence via email, briefings, and recurring publications
- Review and analysis of intelligence feeds
- Evaluation of emerging threats
  - Internal proactive analysis of events, offenses, and exploits
  - External analysis of Security Intelligence
- Proactive risk mitigation, analysis of emerging threats, and relevance to organization
- Operationalization of threat detection and threat response based on intelligence feeds
- Research, creation, and modification of use cases or rules
  - Align use cases and rules to corporate security policies
  - Align use cases and rules with industry standard controls (for example, ISO, COBITT, ISA, NERC, and NIST)
The security operations governance model

Establishing the security operations governance model early will provide the leadership and decision making framework used to monitor and manage the entire program.

This is a complete governance program that includes all stakeholders and defines the required communications, reporting, and escalation procedures.
Intel. sources – IBM X-Force Global Threat Intelligence - draw upon human and machine-generated information

Global Threat Intelligence

- Combines the renowned expertise of X-Force with Trusteer malware research
- Catalog of 70K+ vulnerabilities, 22B+ web pages, and data from 100M+ endpoints
- Intelligence databases dynamically updated on a minute-by-minute basis

New

Trusteer
Real-time sharing of Trusteer intelligence

Zero-day Research
Malware Analysis
Exploit Triage

IP/Domain Reputation
URL/Web Filtering
Web App Control

X-Force Intelligence Network

DYNAMIC PROTECTION AND ANALYTICS PLATFORM
NETWORK | ENDPOINT
PHYSICAL | VIRTUAL | CLOUD

SECURITY PARTNER ECOSYSTEM
Intel. sources – Indicators of Compromise Sources and Tools

**IOC sharing and detection tools** Rapid communication of threat data makes it possible to quickly identify IOCs and defend against attacks:

- IBM X-Force Exchange
- OpenIOC
- IOC Bucket
- MISP
- Mandiant’s IOC Finder
- ESET IOC Repository
- TAXII
- Splunk SA-SPLICE
- CybOX
- GitHub (google/grr Rapid Response for remote live forensics)

Leveraging the power of IOCs, you can find the footprints attackers leave behind when they breach enterprise security defences. It’s one of the most effective ways to put advanced tactics to work to help protect against advanced threats.
Intel. Sources - Humint

External Intelligence sources are essential in the prevention and detection of insider attacks and adding context to external activities

- World-check
- Passport-check
- People Finder sites
- Email Finder sites
- Insurance Fraud Register (UK IFB)
- Lexis-Nexis
- uk-osint.net
- DueDil
- DataLocator 2202
- Jane’s Strategic Advisory Services
- Economic League (CAPRIM) - compromised Labour Govt capability
- Infosphere AB Sweden
- Equifax
- Experian
- tracesmart.co.uk for electoral roll information,
- creepy for twitter
- Acxiom
- Choicepoint
- Companies House
- Land registry
- Bloomberg
- andstone AB Luxembourg
- above 2 joined to make Naked Intelligence
- The University of Southern Denmark, has established an institute for applied mathematics in counter terrorism, the “Counterterrorism Research Lab” (CTR Lab), which conducts research and development around: advanced mathematical models, novel techniques and algorithms, and useful software tools to assist analysts in harvesting, filtering, storing, managing, analysing, structuring, mining, interpreting, and visualizing terrorist information
- Internal Systems of Record – HR/Payroll Systems
- Social Media Scrapers/Bots
- DIY with ELP analysis (i2ANB)

A number of Intel. Aggregator services are emerging – like EUROSINT and VIRTUOSO
IBM’s key intelligence partner: CrowdStrike

1. **Sophisticated insight into threat actors**, tools, tactics and practices, combining advanced technology with an all-source model.

2. **Detailed technical and strategic analysis** of adversary capabilities, indicators and tradecraft, attribution and intentions.

3. **Customizable feeds and API** for indicators of compromise provide real-time attribution to known actor tactics, techniques, and procedures.

4. **Tailored Intelligence** feature provides visibility into breaking events that matter to an organization’s brand, infrastructure, and customers.
IBM’s latest SI source – this is free of charge

The IBM X-Force Exchange holds 700 terabytes of up-to-the-minute threat intelligence, or the equivalent of all the data flowing through the internet every day.


xforce.ibmcloud.com
Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security