L’evoluzione del Security Operation Center tra Threat Detection e Incident Response & Management

Mattia Cinacchi
Security Services Architect & Advisor, IBM Italia
Intervento al Security Summit Milano 2016 – 15 aprile

Autore e Speaker: Mattia Cinacchi
Security Services Architect & Advisor, IBM Italia

Con l’intervento di Andrea Zapparoli Manzoni
Docente Clusit
Universe of cyber security threats is constantly expanding

Future Threats

Current Threats

Drivers:
- More hackers and attackers
- Better exploit tools
- Increased sourcing options for attackers
- Rise of the hacking entrepreneur (Hacktrepreneurs)
- Organized crime loves cyber crime (OCC)
- Attacks are well funded and managed like a program
Attacks are relentless, aggressive and constantly evolving

Size of circle estimates relative impact of incident in terms of cost to business.

Source: IBM X-Force Threat Intelligence Report 2016
New threats require a new approach to security, but most are defending against yesterday’s attacks, using **siloed, discrete defenses**.
What is a Security Operations Center, or SOC?

A Security Operations Center is a highly skilled team following defined definitions and processes to manage threats and reduce security risk.

Security Operations Centers (SOC) are designed to:

- protect mission-critical data and assets
- prepare for and respond to cyber emergencies
- help provide continuity and efficient recovery
- fortify the business infrastructure

The SOC’s major responsibilities are:

- Monitor, Analyze, Correlate & Escalate Intrusion Events
- Develop Appropriate Responses; Protect, Detect, Respond
- Conduct Incident Management and Forensic Investigation
- Maintain Security Community Relationships
- Assist in Crisis Operations
A Security Operations Center is key to keeping up with a perpetually evolving cyber security environment

**Objectives**

1. Manage risk
2. Meet compliance and regulatory requirements
3. Safeguard critical data
4. Protect business against attacks
5. Increase cyber security visibility
6. Move from reactive response to proactive mitigation
To achieve these objectives, IBM Security looks at the whole span of the threat management lifecycle.

**Threat management lifecycle**

- **Strategize**
  - Assess security posture and capabilities
  - Where can I begin or improve?

- **Collect**
  - Gather and process threat data
  - What threats am I facing?

- **Analyze**
  - Analyze, correlate, score and filter
  - What do they mean to me?

- **Prioritize**
  - Rank, prioritize and measure
  - Which are ‘high value’ threats?

- **Respond**
  - Operationalize and respond
  - How should I respond?

- **Prevent**
  - Track, learn and integrate into the organization
  - How can I prevent it in the future?

**Enterprise risk management data platform**

**Ongoing optimization**
Cybersecurity Incident Response Planning

- An incident response plan is the foundation on which all incident response and recovery activities are based:
  - It provides a framework for effectively responding to any number of potential incidents
  - It specifically defines the organization, roles and responsibilities of the computer security incident response team (CSIRT)
  - It should have criteria to assist an organization determine types and priorities of each security incident
  - It defines escalation and communication procedures to management, executive, legal, law enforcement, and media depending on incident conditions and severity
  - It must be regularly updated and fully tested via dry runs

At least 50 percent of the CSIRPs evaluated by IBM security consultants show no evidence of a formal document lifecycle or a history of continual revisions.

Having an incident response plan in place saved U.S. organizations on average USD1.2 million per data breach in 2013.

CSIRP = Computer Security Incident Response Plan
Incident Response: Prepare proactively and respond instantly

Around-the-clock access to incident response and forensics experts

Combat a significant intrusion, sophisticated attack or other security incident for faster recovery and forensic analysis

- Incident planning
- Proactive preparation
- Periodic reviews

Worldwide, around-the-clock coverage to enable faster recovery and reduce business impact from incidents

- Incident triage
- Containment, eradication and recovery
- Post-incident analysis

Cyber Emergency Hotline

<table>
<thead>
<tr>
<th>Country</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italy</td>
<td>+39 02 99953631</td>
</tr>
<tr>
<td>US</td>
<td>1-888-241-9812</td>
</tr>
<tr>
<td>Worldwide</td>
<td>1-312-212-8034</td>
</tr>
</tbody>
</table>

Helps manage incident response across multiple stages including prevention, intelligence gathering, containment, eradication, recovery, and compliance management
### IBM Security Services Portfolio

<table>
<thead>
<tr>
<th>Security Strategy, Risk and Compliance</th>
<th>Security Intelligence and Operations</th>
<th>Cyber Security Assessment and Response</th>
<th>Identity and Access Management</th>
<th>Data and Application Security</th>
<th>Infrastructure and Endpoint Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Strategy and Planning</td>
<td>SIEM Design and Deploy</td>
<td>Incident Response Planning</td>
<td>Access Management Design and Deploy</td>
<td>Data Discovery and Classification</td>
<td>Staff Augmentation Services</td>
</tr>
<tr>
<td>Security Architecture and Program Design</td>
<td>Managed SIEM</td>
<td>Active Threat Assessment</td>
<td>Multifactor Authentication Design and Deploy</td>
<td>Data Security Strategy and Architecture</td>
<td>Firewall Management</td>
</tr>
<tr>
<td>PCI Compliance Advisory Services</td>
<td>Advanced Cyber Threat Intelligence Services</td>
<td>Smart and Embedded Device Security</td>
<td>Identity Governance and Administration, Design and Deploy</td>
<td>Application Security Assessment</td>
<td>Intrusion Detection and Prevention System Management</td>
</tr>
<tr>
<td>Information Security Assessment</td>
<td>APT³ Survival Kit</td>
<td>Executive Protection</td>
<td>Managed Identity</td>
<td>Application Source Code Security Assessment</td>
<td>Managed Protection Services</td>
</tr>
<tr>
<td>Security Framework and Risk Assessments</td>
<td></td>
<td></td>
<td>Cloud Identity</td>
<td></td>
<td>Secure Web Gateway Management</td>
</tr>
<tr>
<td>Integrated Account Security Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Malware Defense Management</td>
</tr>
<tr>
<td>Cloud Security Strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Managed Web Defense</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Hosted Email and Web Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Hosted Vulnerability Management</td>
</tr>
</tbody>
</table>

**Clusit Education**
Key components for a SOC initiative

Consulting Services
- Security Intelligence & Operations Consulting
- SOC Strategy & Planning
- SOC Maturity Assessment
- SOC Build & Transformation
- SIEM Activation & Tuning
- Integrations

SIEM platform
- QRadar SIEM (software, virtual, appliances, SaaS)
- Security Intelligence feed
- QRadar additional modules (QVM, QFlow)

Managed Security Services
- Managed SIEM service
- Security Monitoring
- Security Service Manager
- Emergency Response Services
- Early Warning (XForce Threat Analysis Services)
Thank You

Mattia Cinacchi
Security Services Architect & Advisor, IBM Italia
mattia.cinacchi@it.ibm.com
+39.334.6004854