

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

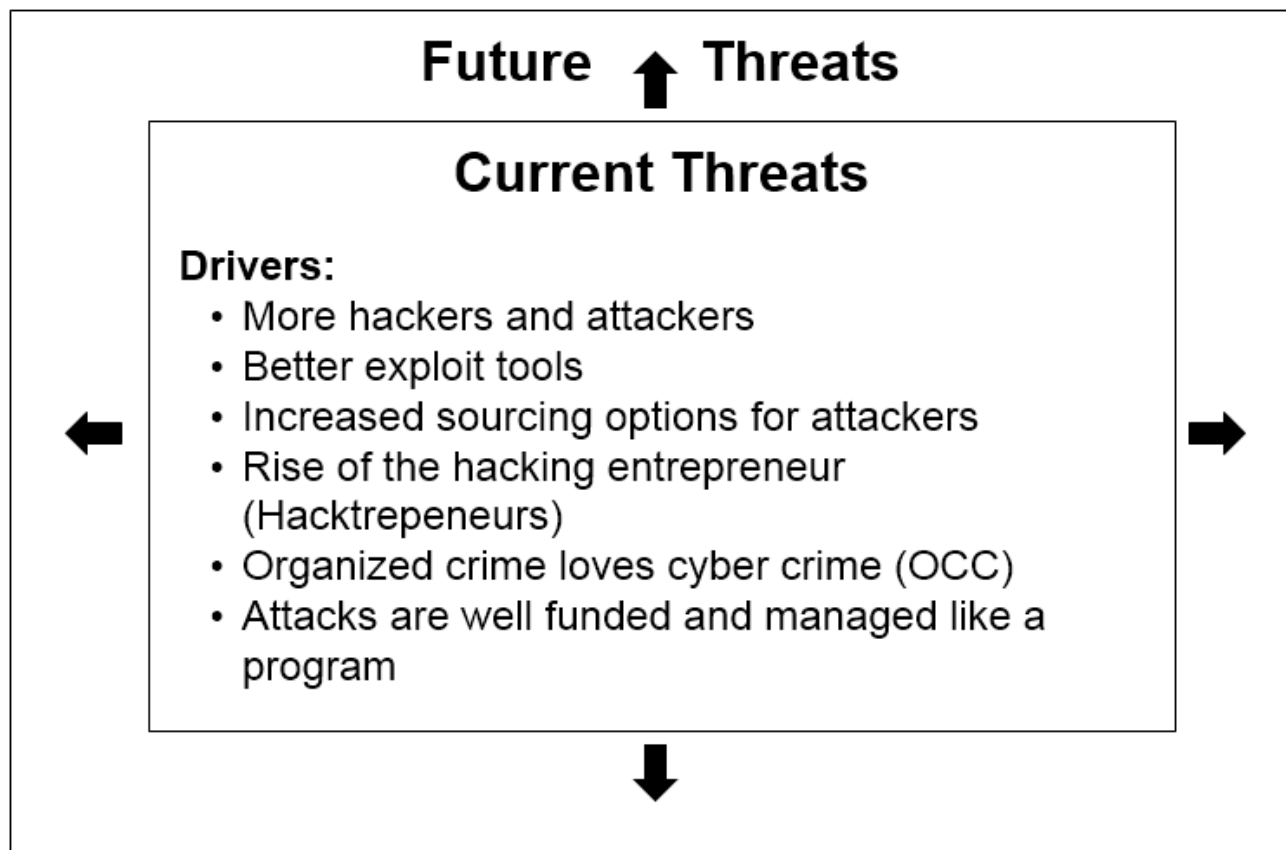
Security Services Architect & Advisor, IBM Italia

Con l'intervento di

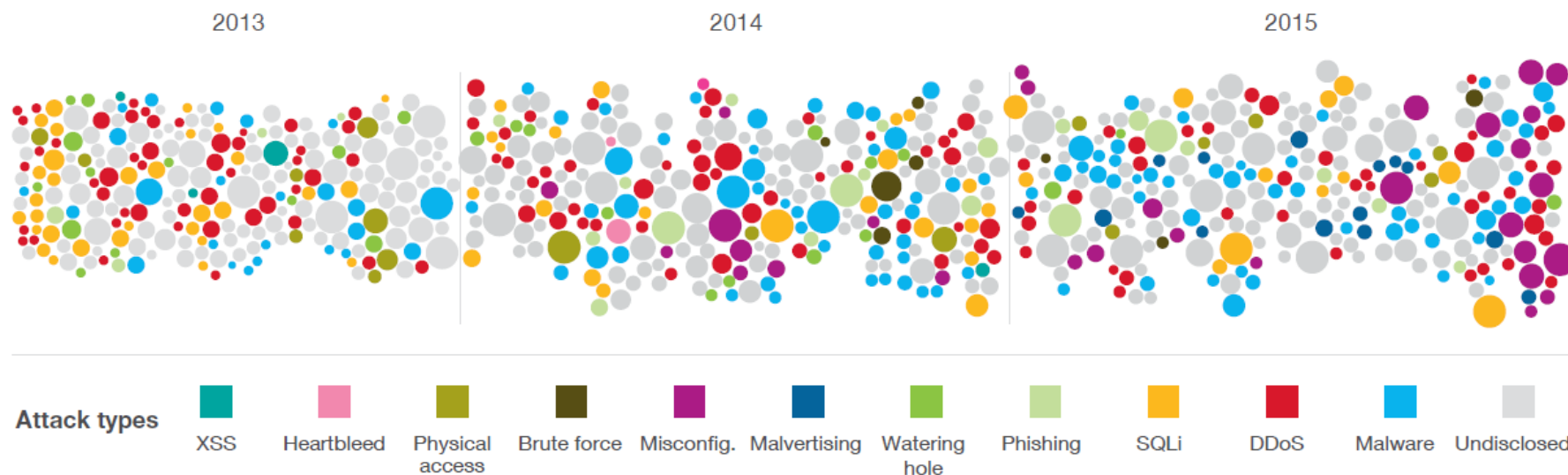
Andrea Zapparoli Manzoni

Docente Clusit

Universe of cyber security threats is constantly expanding



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

Is your security team prepared?

Broad Attacks

Indiscriminate malware, spam and DoS activity

Tactical Approach

Compliance-driven, reactionary

- Build multiple perimeters
- Protect all systems
- Use signature-based methods
- Periodically scan for known threats
- Read the latest news
- Shut down systems

Targeted Attacks

Advanced, persistent, organized, politically or financially motivated

Strategic Approach

Intelligence-driven, continuous

- Assume constant compromise
- Prioritize high-risk assets
- Use behavioral-based methods
- Continuously monitor activity
- Consume real-time threat feeds
- Gather, preserve, retrace evidence

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

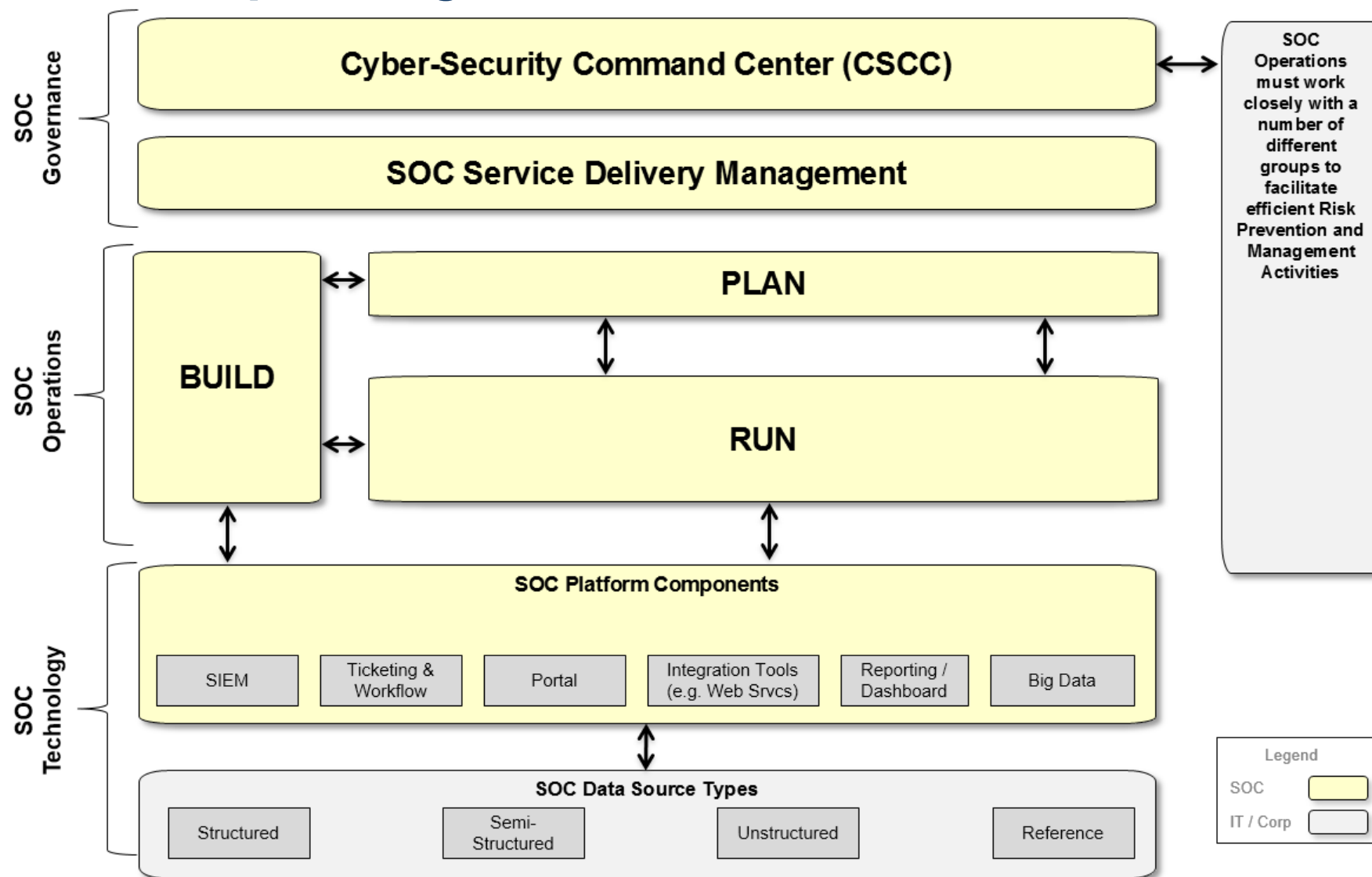


To achieve these objectives, IBM Security looks at the whole span of the threat management lifecycle

Threat management lifecycle



SOC Operating Model



Cybersecurity Incident Response Planning

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.



- **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

CSIRP Review
and
Gap Assessment

CSIRP
Development

Incident Mock Tests
and
Table Top Exercise

¹CSIRP = 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

Cyber Emergency Hotline

Italy	+39 02 99953631
US	1-888-241-9812
Worldwide	1-312-212-8034

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

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

Helps manage incident response across multiple stages including prevention, intelligence gathering, containment, eradication, recovery, and compliance management

Security Strategy, Risk and Compliance	Security Intelligence and Operations	Cyber Security Assessment and Response	Identity and Access Management	Data and Application Security	Infrastructure and Endpoint Security
Security Essentials and Maturity Consulting	Security Operations Consulting	Emergency Response Services	Identity and Access Strategy and Assessment	Critical Data Protection Program	Deployment and Migration
Security Strategy and Planning	SIEM Design and Deploy	Incident Response Planning	Access Management Design and Deploy	Data Discovery and Classification	Staff Augmentation Services
Security Architecture and Program Design	Managed SIEM	Active Threat Assessment	Multifactor Authentication Design and Deploy	Data Security Strategy and Architecture	Firewall Management
Critical Infrastructure Security Services	Security Intelligence Analyst	Penetration Testing	Identity and Access Solution Migration	Data Loss Prevention and Encryption	Unified Threat Management
PCI Compliance Advisory Services	Advanced Cyber Threat Intelligence Services	Smart and Embedded Device Security	Identity Governance and Administration, Design and Deploy	Application Security Assessment	Intrusion Detection and Prevention System Management
Information Security Assessment	Intelligent Log Management	APT ³ Survival Kit		Application Source Code Security Assessment	Managed Protection Services
Security Framework and Risk Assessments	IBM® XForce® Hosted Threat Analysis Service	Executive Protection	Managed Identity	Hosted Application Security Management	Secure Web Gateway Management
Integrated Account Security Management			Cloud Identity		Malware Defense Management
Cloud Security Strategy					Managed Web Defense
					Hosted Email and Web Security
					Hosted Vulnerability Management

Consulting and Systems Integration

Managed Security Services

Cloud Security Services

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

© **Copyright IBM Corporation 2016. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.