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

Mattia Cinacchi

Security Services Architect & Advisor, IBM Italia

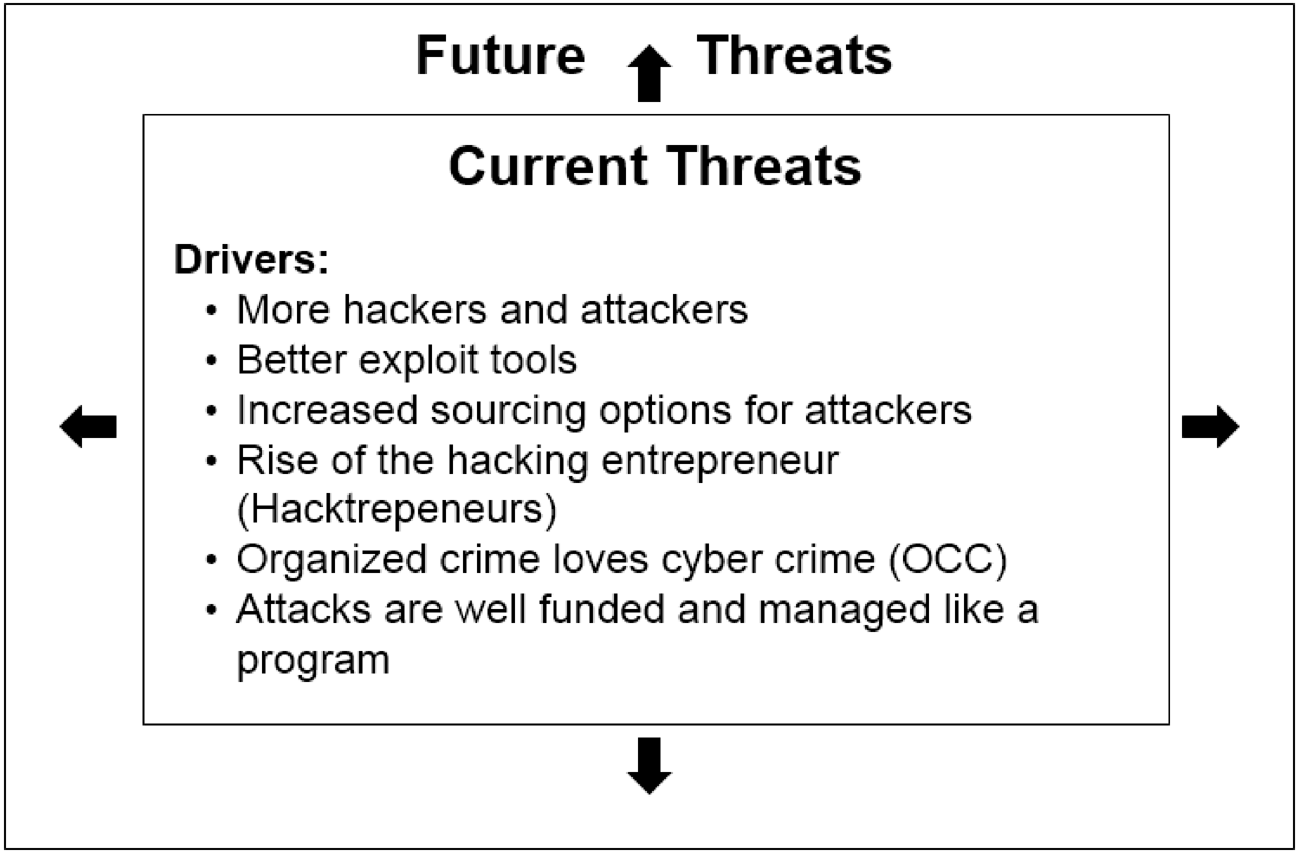
Con l’intervento di:

Corrado Giustozzi

Cybersecurity Evangelist and Strategic Information Security Consultant

Clusit
Education

Universe of cyber security threats is constantly expanding



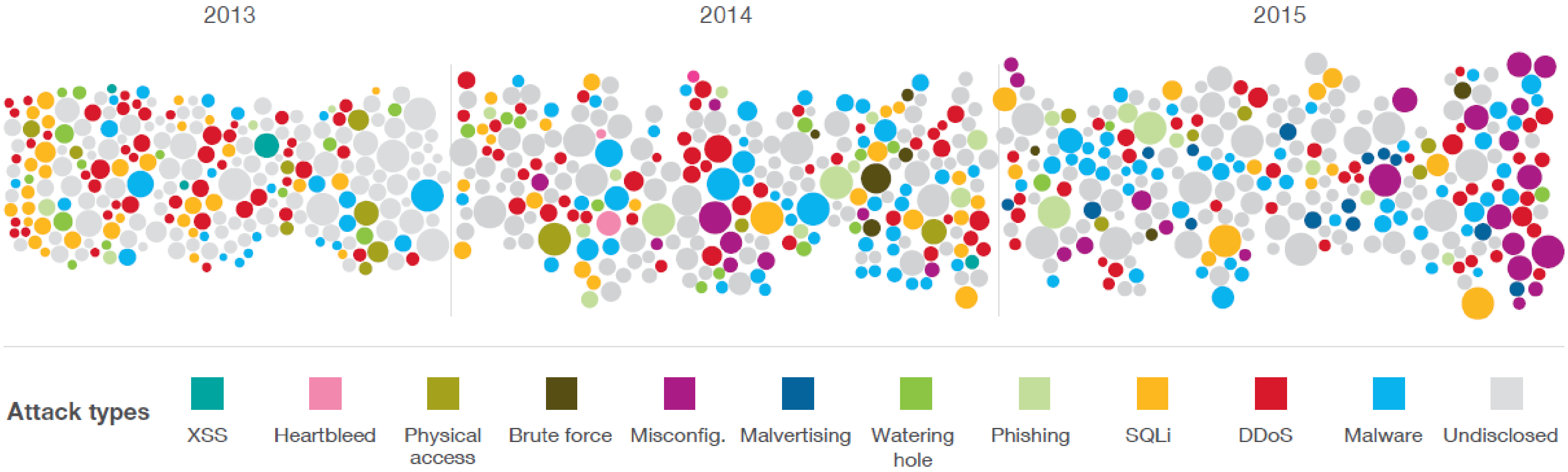
Future Threats

Current Threats

Drivers:

- More hackers and attackers
- Better exploit tools
- Increased sourcing options for attackers
- Rise of the hacking entrepreneur (Hacktrepeneurs)
- 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

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

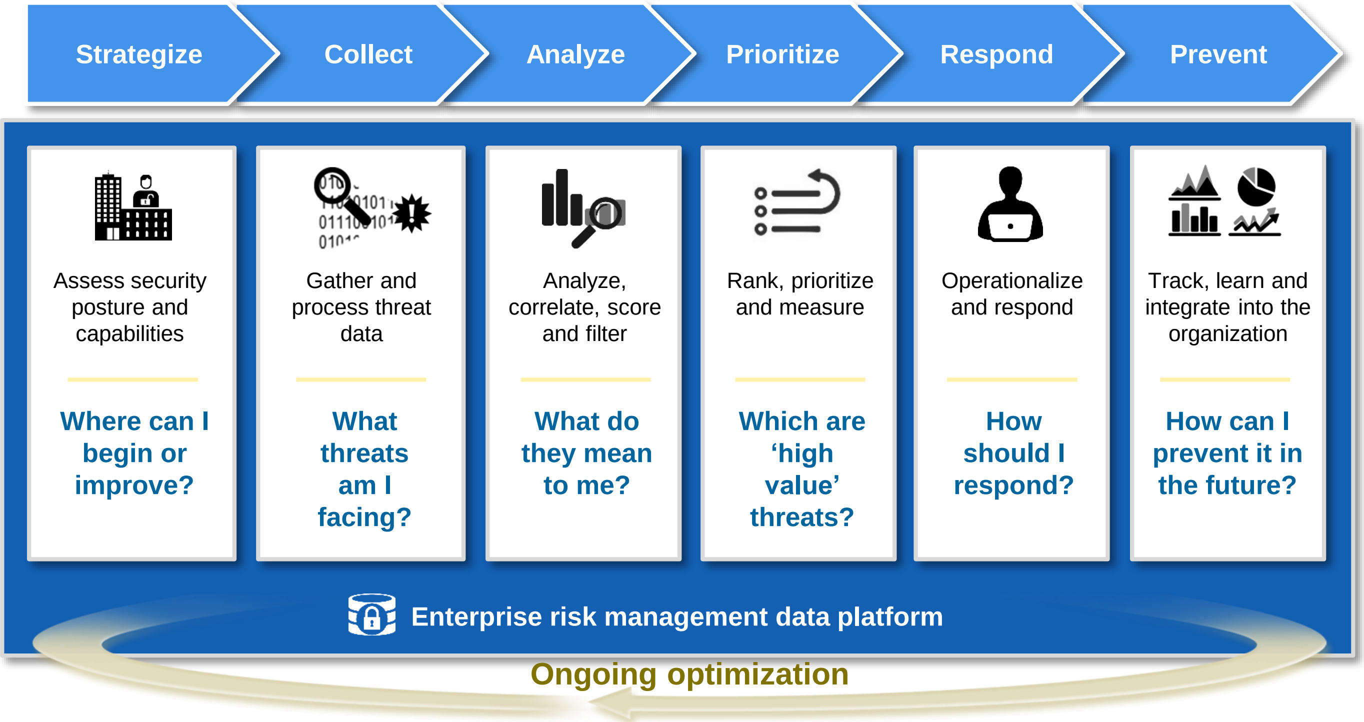
A Security Operations Center is key to keeping up with a perpetually evolving cyber security environment

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



Strategize	Collect	Analyze	Prioritize	Respond	Prevent
Assess security posture and capabilities	Gather and process threat data	Analyze, correlate, score and filter	Rank, prioritize and measure	Operationalize and respond	Track, learn and integrate into the organization
Where can I begin or improve?	**What threats am I facing?**	**What do they mean to me?**	**Which are 'high value' threats?**	**How should I respond?**	**How can I prevent it in the future?**

Enterprise risk management data platform

Ongoing optimization

SOC Operating Model

Il contenuto di questa slide è stato utilizzato
durante l’evento Security Summit 2016 di Roma.

Per informazioni:

Claudio D’Arconte
CDArcon@uk.ibm.com

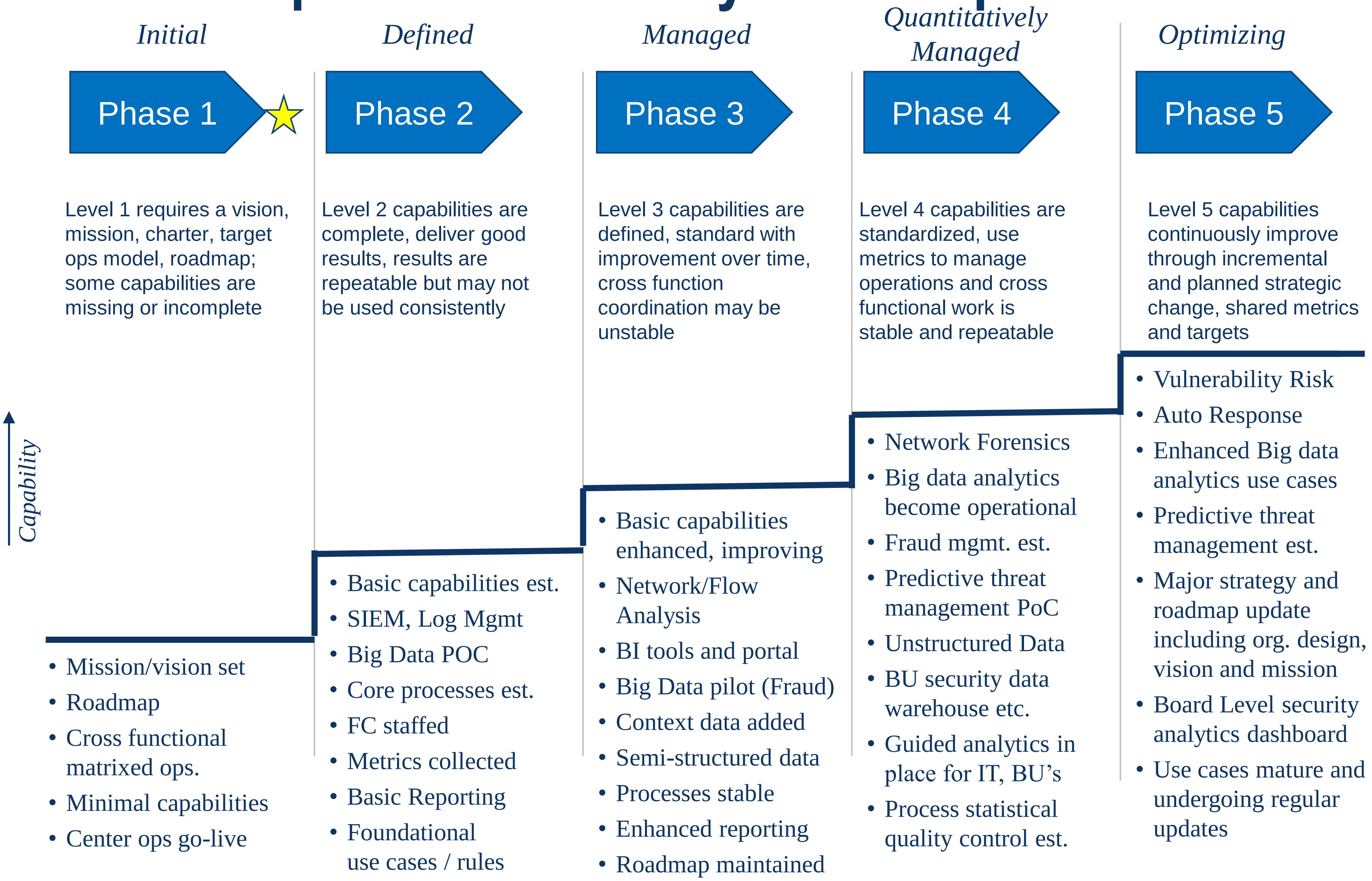
SOC Operating Model

Il contenuto di questa slide è stato utilizzato
durante l'evento Security Summit 2016 di Roma.

Per informazioni:

Claudio D'Arconte
CDArcon@uk.ibm.com

SOC Capabilities Maturity Roadmap



Capability

Initial

Phase 1

Level 1 requires a vision, mission, charter, target ops model, roadmap; some capabilities are missing or incomplete

- Mission/vision set
- Roadmap
- Cross functional matrixed ops.
- Minimal capabilities
- Center ops go-live

Defined

Phase 2

Level 2 capabilities are complete, deliver good results, results are repeatable but may not be used consistently

- Basic capabilities est.
- SIEM, Log Mgmt
- Big Data POC
- Core processes est.
- FC staffed
- Metrics collected
- Basic Reporting
- Foundational use cases / rules

Managed

Phase 3

Level 3 capabilities are defined, standard with improvement over time, cross function coordination may be unstable

- Basic capabilities enhanced, improving
- Network/Flow Analysis
- BI tools and portal
- Big Data pilot (Fraud)
- Context data added
- Semi-structured data
- Processes stable
- Enhanced reporting
- Roadmap maintained

Quantitatively Managed

Phase 4

Level 4 capabilities are standardized, use metrics to manage operations and cross functional work is stable and repeatable

- Network Forensics
- Big data analytics become operational
- Fraud mgmt. est.
- Predictive threat management PoC
- Unstructured Data
- BU security data warehouse etc.
- Guided analytics in place for IT, BU's
- Process statistical quality control est.

Optimizing

Phase 5

Level 5 capabilities continuously improve through incremental and planned strategic change, shared metrics and targets

- Vulnerability Risk
- Auto Response
- Enhanced Big data analytics use cases
- Predictive threat management est.
- Major strategy and roadmap update including org. design, vision and mission
- Board Level security analytics dashboard
- Use cases mature and undergoing regular updates

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.

IBM Global Technology Services
Security Services

IBM.

Building a security incident response plan that works

A look at the top ten CSIRP (Computer Security Incident Response Plan) mistakes

Highlights

- Security breaches are virtually inevitable, and can involve thousands of data records while costing millions of dollars
- A Computer Security Incident Response Plan, or CSIRP, can help reduce the cost and mitigate the severity of breaches
- Based on experience working with hundreds of companies of all sizes, IBM offers advice for building and maintaining an effective CSIRP

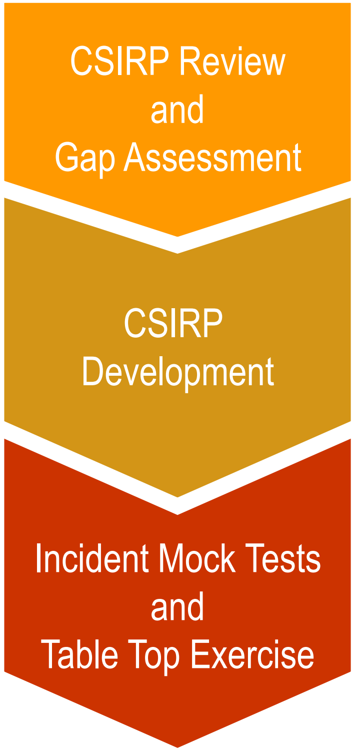
Understanding the high cost of security failures

Global enterprises with hundreds of thousands of employees, small companies doing business on the web and public sector organizations of any size all have one thing in common: your networks are under almost constant attack, and your enterprise systems are at risk as well. Moreover, it is virtually inevitable that you will suffer a security breach at some point.[1]

How damaging that breach will be is influenced by many factors—one of the most important being your own preparedness. According to Ponemon Institute, having a Computer Security Incident Response Plan (CSIRP) in place is second only to a strong security posture in reducing the cost of a data breach—saving as much as USD42 per data record for U.S. organizations. With an average number of 28,765 records involved in a data breach in the U.S., that translates into a potential savings of more than USD1.2 million out of the total average cost of USD5.4 million per incident.[2]

As a cornerstone of your defense against hackers, malware, human error and a host of other threats, a CSIRP is the map that guides your response to a successful attack. It should define the roles and responsibilities of all responders, establish authority for making major decisions and define communications flows and notification procedures. Without a CSIRP, your incident response team can waste invaluable time and resources in figuring out what to do—leading to potentially higher costs and greater damage to your organization and your reputation.

- **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 ream (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

[1] 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**

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

- Incident planning
- Proactive preparation
- Periodic reviews

Cyber Emergency Hotline

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

- 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

Incident Response Platform (IRP) from Resilient Systems

- Automate and orchestrate the many processes needed when dealing with cyber incidents, from breaches to lost devices.
- Enable to respond and mitigate cyber incidents more quickly and effectively, reducing the impact to the organization

SECURITY MODULE

- Industry standard workflows (NIST, SANS)
- Threat intelligence feeds
- Organizational SOPs
- Community best practices

ACTION MODULE

- Automate processes
- Enrich incident details
- Gather forensics
- Enact mitigation

PRIVACY MODULE

- Global breach regulations
- Contractual obligations
- 3rd party requirements
- Organizational SOPs
- Privacy best practices

IBM Security Services Portfolio

- Risk Management Operations
- Consulting & Systems Integration
- Managed Security Services
- Cloud Security Services

SSRC
Security Strategy, Risk and Compliance

- Ten Essential Practices Assessment
- Security Strategy and Planning
- Security Architecture and Program Design
- Critical Infrastructure Security Services
- PCI Compliance Advisory Services
- Information Security Assessment (ISA)
- Security Framework and Risk Assessments
- Automated IT Risk Mgmt.
- SAP Security
- Data Privacy

- Cloud Security Strategy

- Regulatory Program Mgmt.
- Security Management
- Security Policy, Audit and Compliance Mgmt.

SIOC
Security Intelligence and Operations Consulting

- Security Operations Consulting
- SIEM Design and Deploy
- Security Use Case Library

- Managed SIEM
- Security Intelligence Analyst
- Advanced Cyber Threat Intelligence Services

- Hosted Security Event and Log Management
- Intelligent Log Management
- X-Force Hosted Threat Analysis Service

CSAR
Cyber Security Assessment & Response

- Emergency Response Services
- Incident Response Planning
- Active Threat Assessment
- Penetration Testing
- Smart and Embedded Device Security
- APT Survival Kit

- Continuous Remote Threat Response

- Cybersecurity Awareness Training

IAM
Identity and Access Management

- Identity and Access Strategy and Assessment
- Access Management Design and Deploy
- Multi-factor Authentication Design and Deploy
- Identity and Access Solution Migration
- Identity Governance and Administration, Design and Deploy

- Managed Identity

- Cloud Identity

DAS
Data and Application Security

- Critical Data Protection Program
- Data Discovery and Classification
- Data Security Strategy and Architecture
- Data Loss Prevention and Encryption
- Application Security Assessment
- Application Source Code Security Assessment
- Data Security Assessment

- Managed Data Protection Services for Guardium

- Hosted Application Security Management

IES
Infrastructure and Endpoint Security

- Deployment and Migration
- Staff Augmentation Services

- Firewall Management
- Unified Threat Management
- Intrusion Detection and Prevention System Management
- Managed Protection Services (MPS)
- Secure Web Gateway Management
- Endpoint Protection Service

- Managed Web Defense
- Hosted E-mail and Web Security
- Hosted Vulnerability Management

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)

A review of ~300 SOC throughout the world

Best practices in building and operating a SOC:

- Cross-functional governance
- Industrialize your SOC
- SIEMs are development environments - SDLC
- Digital library
- Response-based use case design
- What gets measured gets done
- Automate analysis
- Program not a project
- SNOCs make bad SOCs

Emerging trends in Security Operations Centers

- SOC is **evolving** into the **enterprise threat management center**
- Migration from low-value to **high-value use cases**
- **Dimensional data** increases the **resolution** of security incidents
- **Convergence** of risk data (integrated enterprise risk management platform)
- **Leverage operations management** techniques to manage SOC
- **Measure** and **communicate** the **value** of security services (dashboards)
- **Predictive** security analytics pilot is now underway
- **Active defense** – SOCs will automate threat response and prevention activities
- Add a **Security Integration function** to minimize preventable security incidents

Thank You

Mattia Cinacchi

Security Services Architect & Advisor, IBM Italia

mattia.cinacchi@it.ibm.com

+39.334.6004854

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.