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

Mattia Cinacchi
Security Services Architect & Advisor, IBM Italia

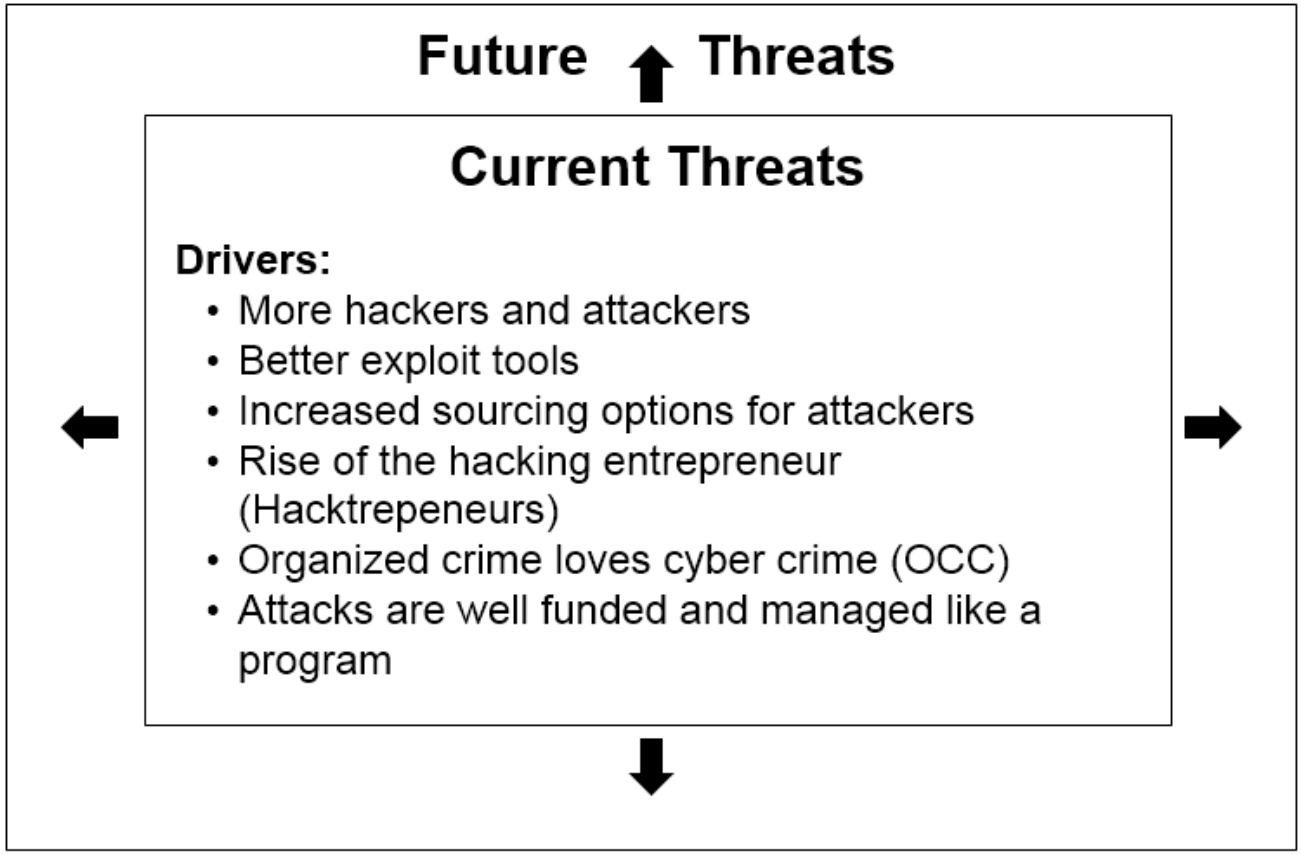
Clusit Education

Intervento al Security Summit Milano 2016 – 15 aprile

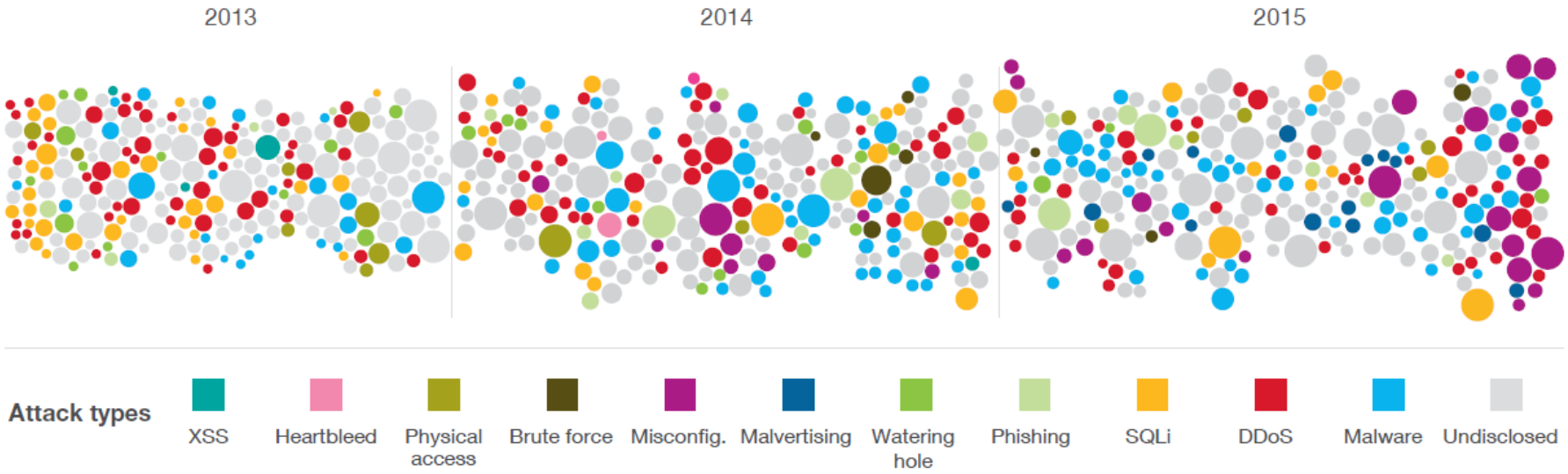
Autore e Speaker:
Mattia Cinacchi
Security Services Architect & Advisor, IBM Italia

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:

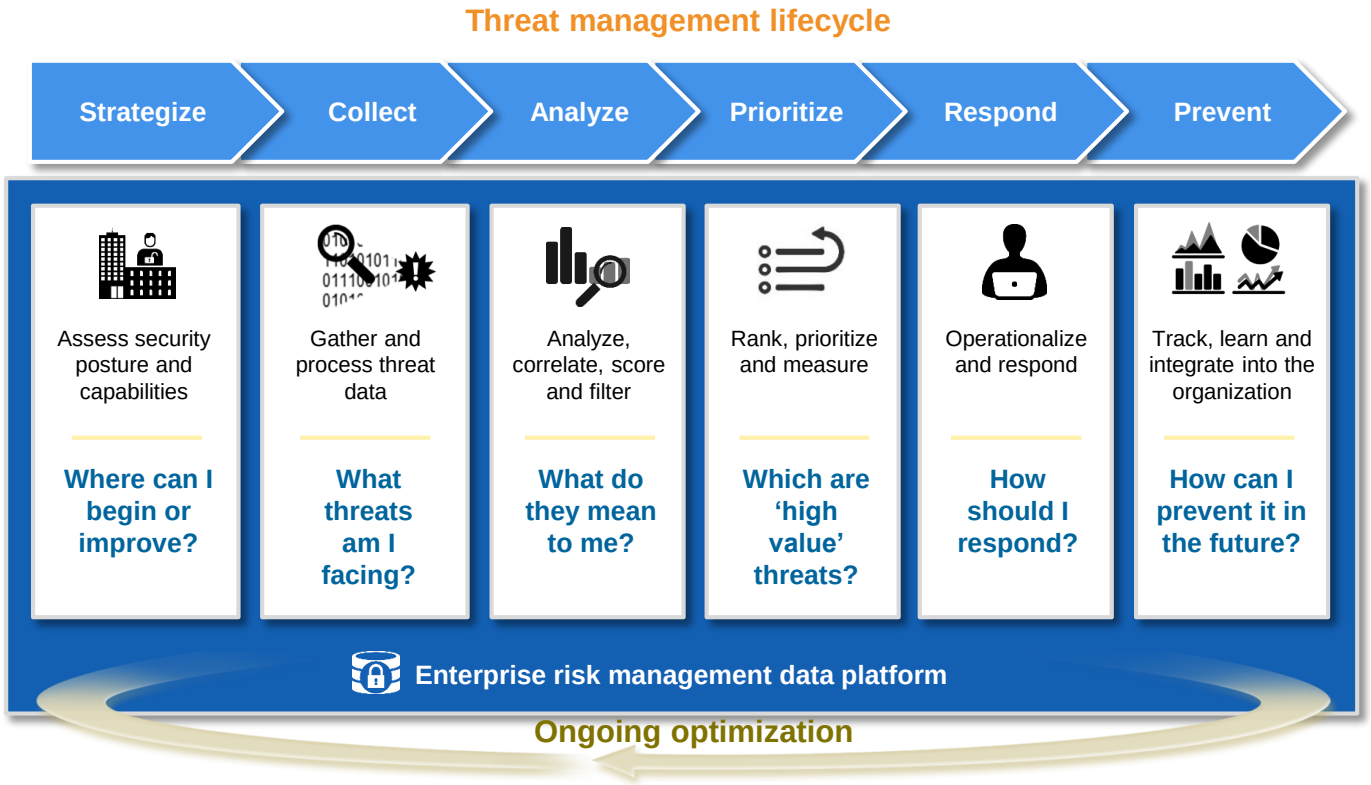
- Monitor, Analyze, Correlate & Escalate Intrusion Events
- Develop Appropriate Responses; Protect, Detect, Respond
- Conduct Incident Management and Forensic Investigation
- Maintain Security Community Relationships
- Assist in Crisis Operations

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

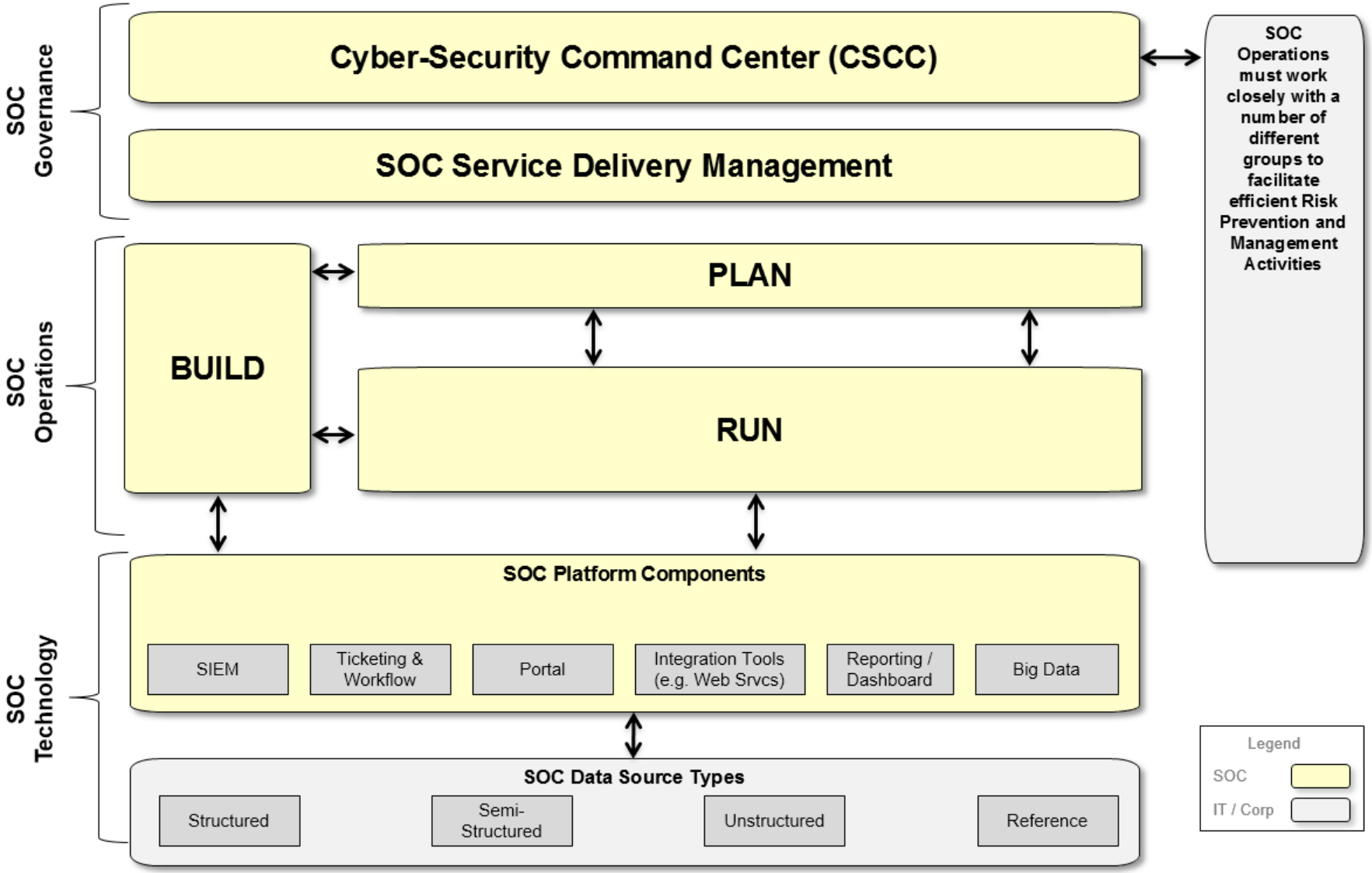
Objectives

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

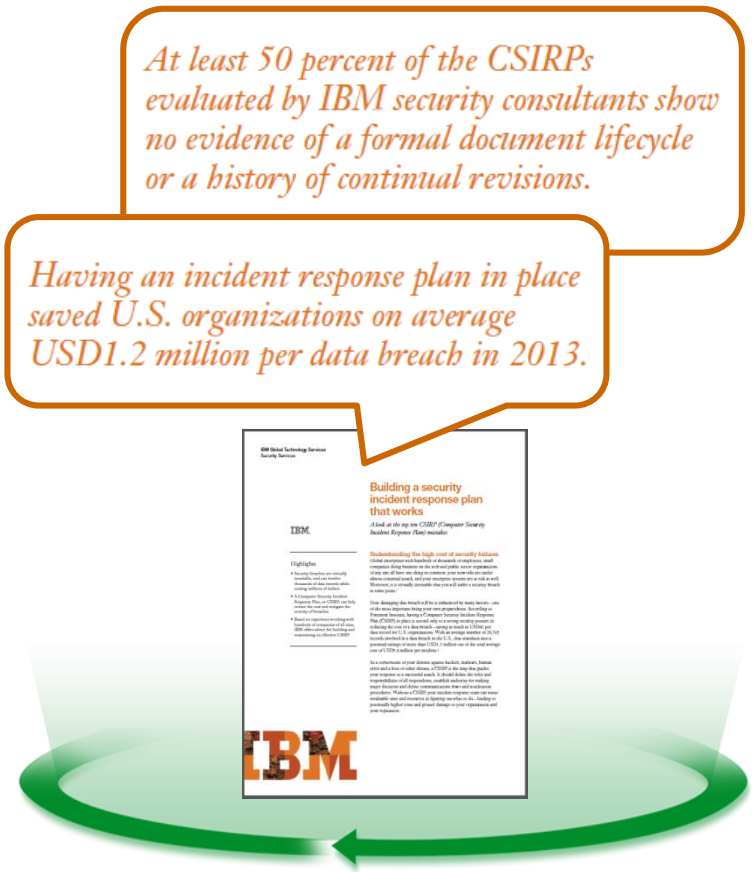
To achieve these objectives, IBM Security looks at the whole span of the threat management lifecycle



SOC Operating Model



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 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

[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**

- Incident planning
- Proactive preparation
- Periodic reviews

Cyber Emergency Hotline

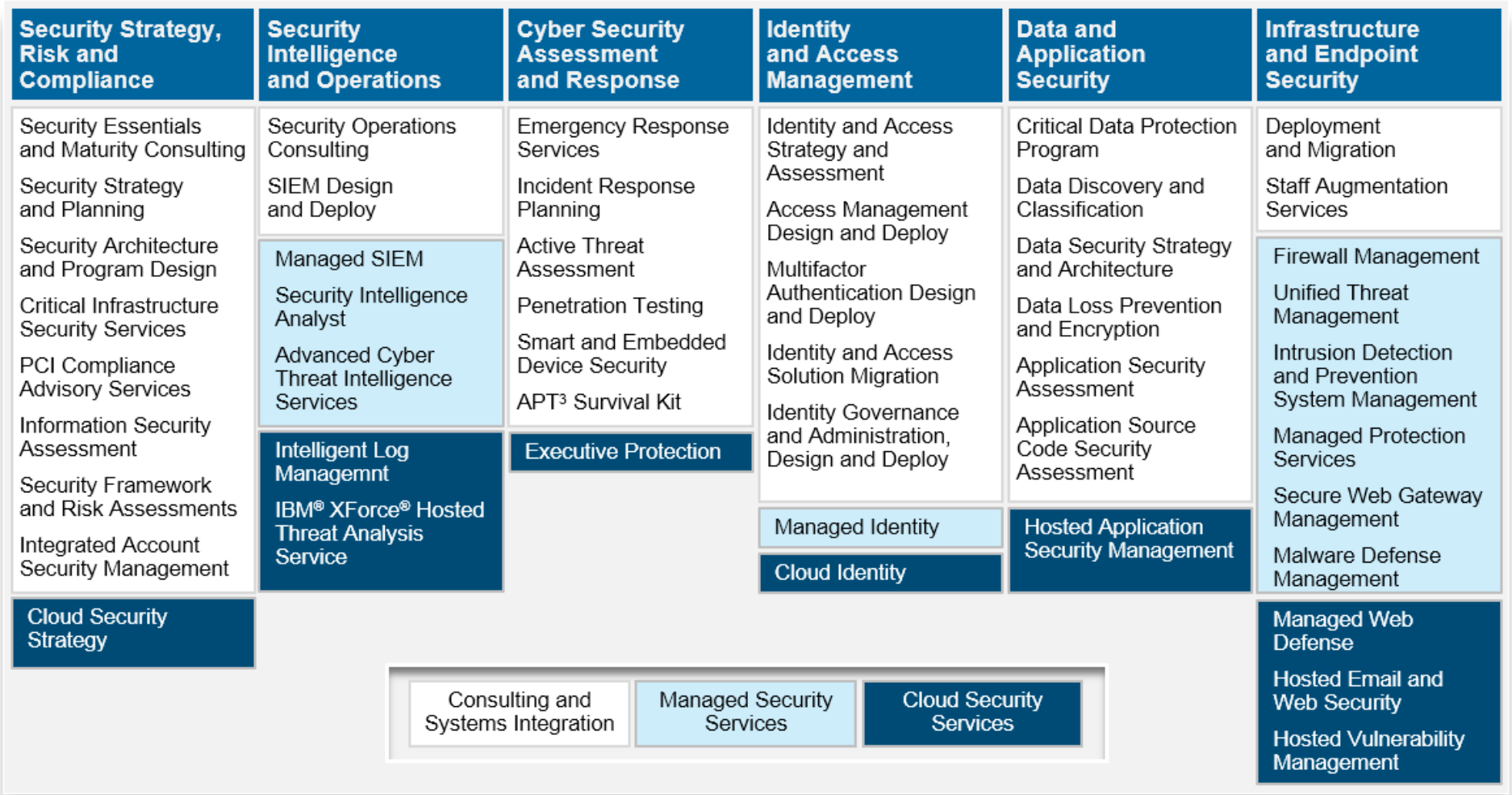
Italy	+39 02 99953631
US	1-888-241-9812
Worldwide	1-312-212-8034

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

IBM Security Services Portfolio



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