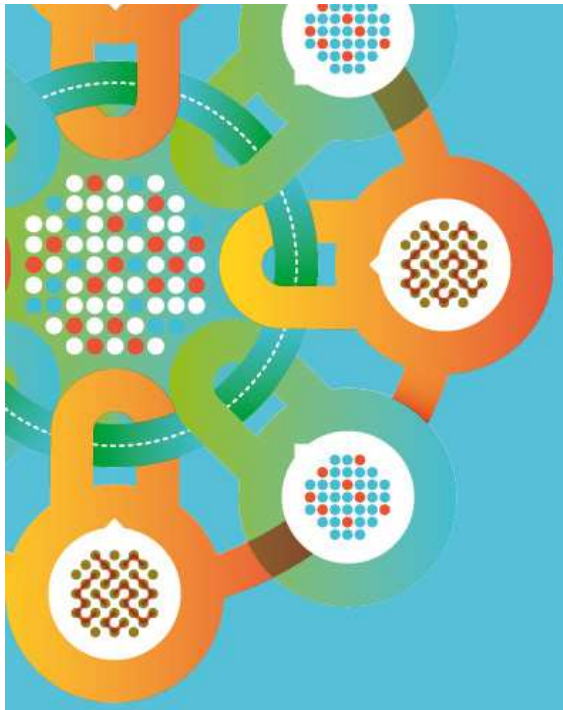


IBM Forum Segrate - Milano

# 18 settembre: Missione Sicurezza

**Identifica e combatti i rischi con la Security Intelligence IBM**

**Samuele Battistoni**

## Security Intelligence e Analytics nei servizi gestiti

# **The Perfect Storm :** Number of vulnerabilities increase radically with emergence of new business models and technologies

**Adopting new business models, and embracing new technologies**


**Years to reach 50M audience**

| | |
|---|---|
| Radio | 38 years |
| TV | 13 years |
| Internet | 4 years |
| iPod | 3 years |
| Facebook | 2 years |

# Unmatched global coverage and security awareness


- Security Operations Centers
- Security Research Centers
- Security Solution Development Centers
- Institute for Advanced Security Branches

## IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration

**10B** analyzed web pages and images
**150M** intrusion attempts daily
**40M** span and phishing attacks
**46K** documented vulnerabilities and millions of unique malware samples

X-FORCE

## Worldwide managed security services coverage

- 20,000-plus devices under contract
- 3,300 GTS[1] service delivery experts
- 3,700-plus MSS[2] clients worldwide
- 15B-plus events managed per day
- 1,000-plus security patents
- 133 monitored countries (MSS)

[1]IBM Global Technology Services (GTS); [2]Managed Security Services (MSS)

# IBM offers a broad managed service portfolio to help address a variety of business requirements

## Managed Security Services (CPE)

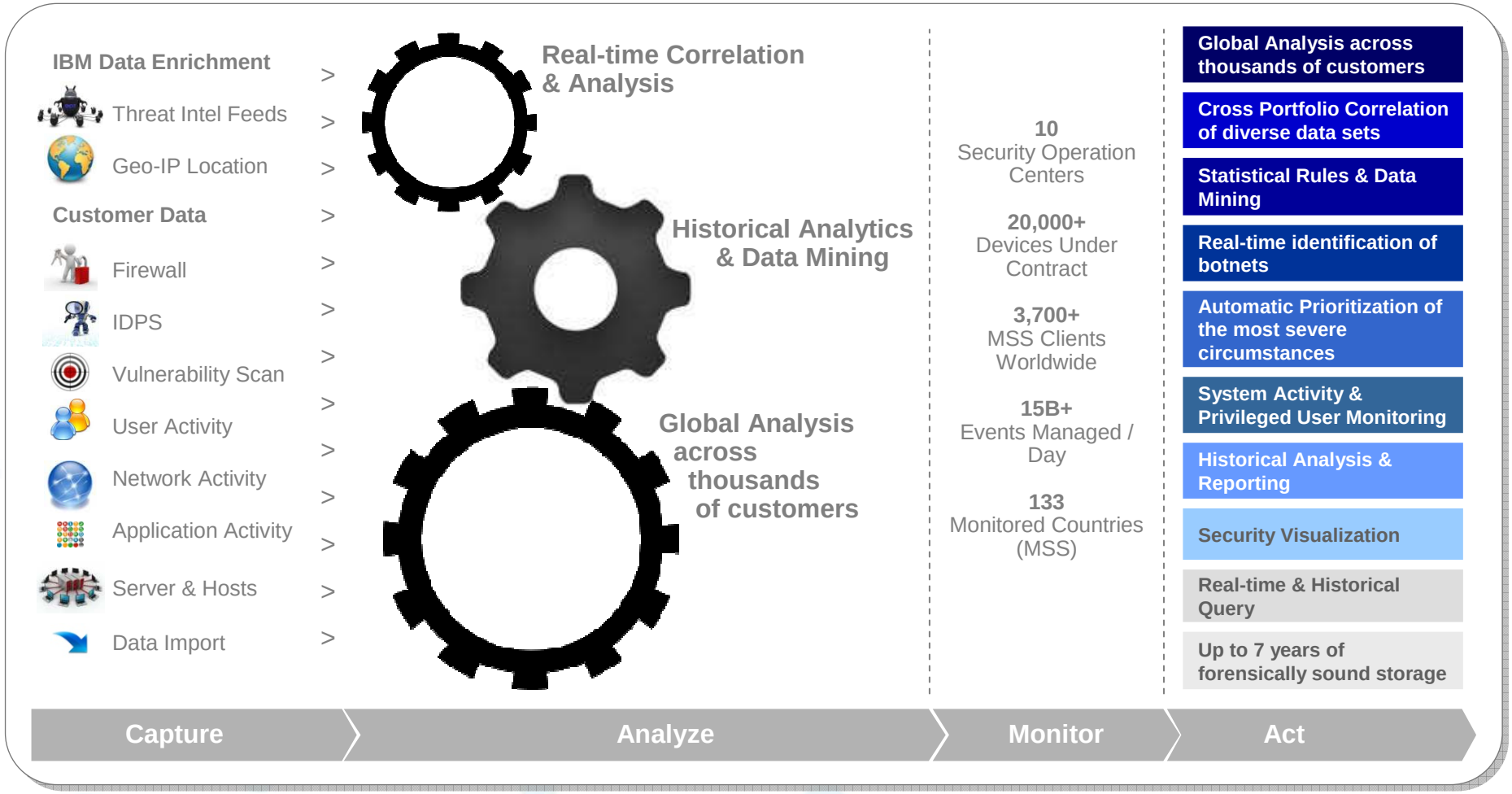
- Managed security incident and event management
- Managed firewall services
- Managed and monitored IPS and IDS services
- Managed UTM services
- Managed protection services for networks, servers and desktops
- Managed identity services


## Managed Security Services (Cloud)

- Hosted security event and log management services
- Hosted vulnerability management services
- Hosted application scanning
- Hosted mobile device security management
- Hosted managed e-mail and web security
- Hosted IBM X-Force threat analysis service

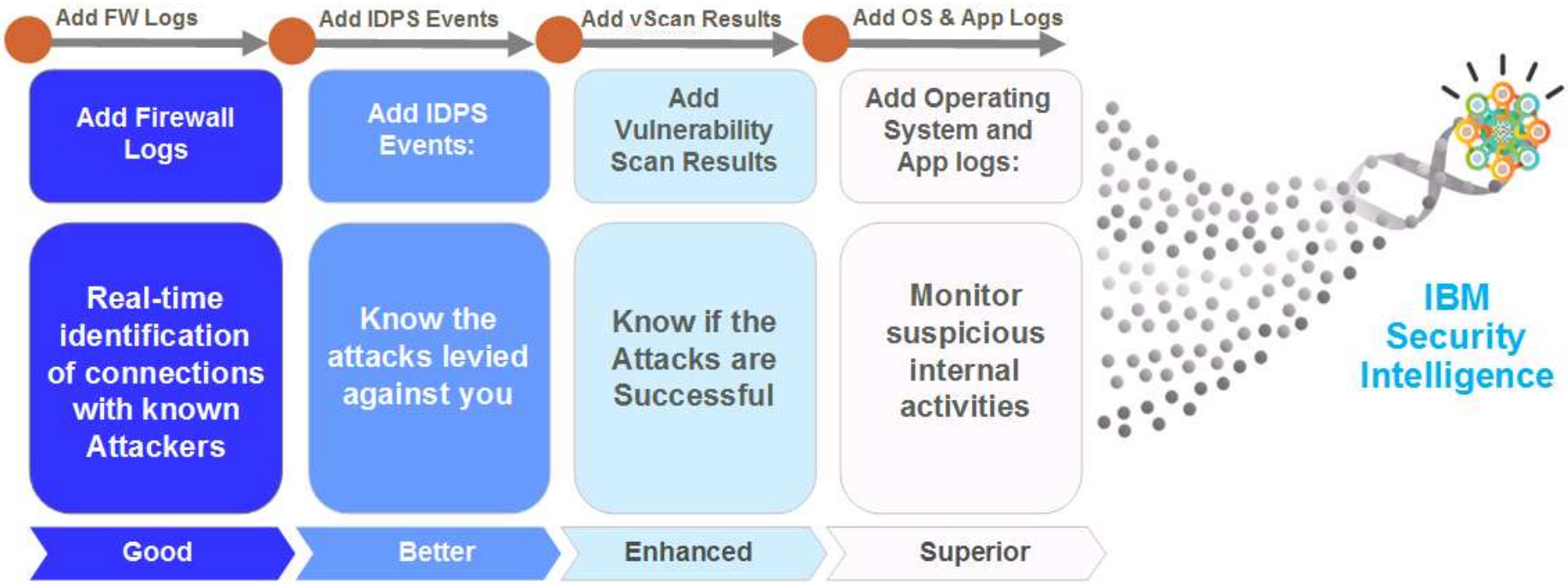
## Multiple device types and vendors supported

# IBM Security Services analytic capabilities




**Enabled by the X-Force Protection System, a multi-tenant environment that collects, aggregates, stores, summarizes, and analyzes data to deliver security intelligence**

# We can help you optimize security intelligence




**Services recommended to enable these capabilities:**

| | | | |
|---|---|---|---|
| (1) Firewall Mgmt<br>(2) Managed UTM<br>(3) Hosted SELM | (1) Managed IDPS<br>(2) Managed UTM<br>(3) MPS<br>(4) Hosted SELM | (1) VMS 2.0 | (1) Hosted SELM |

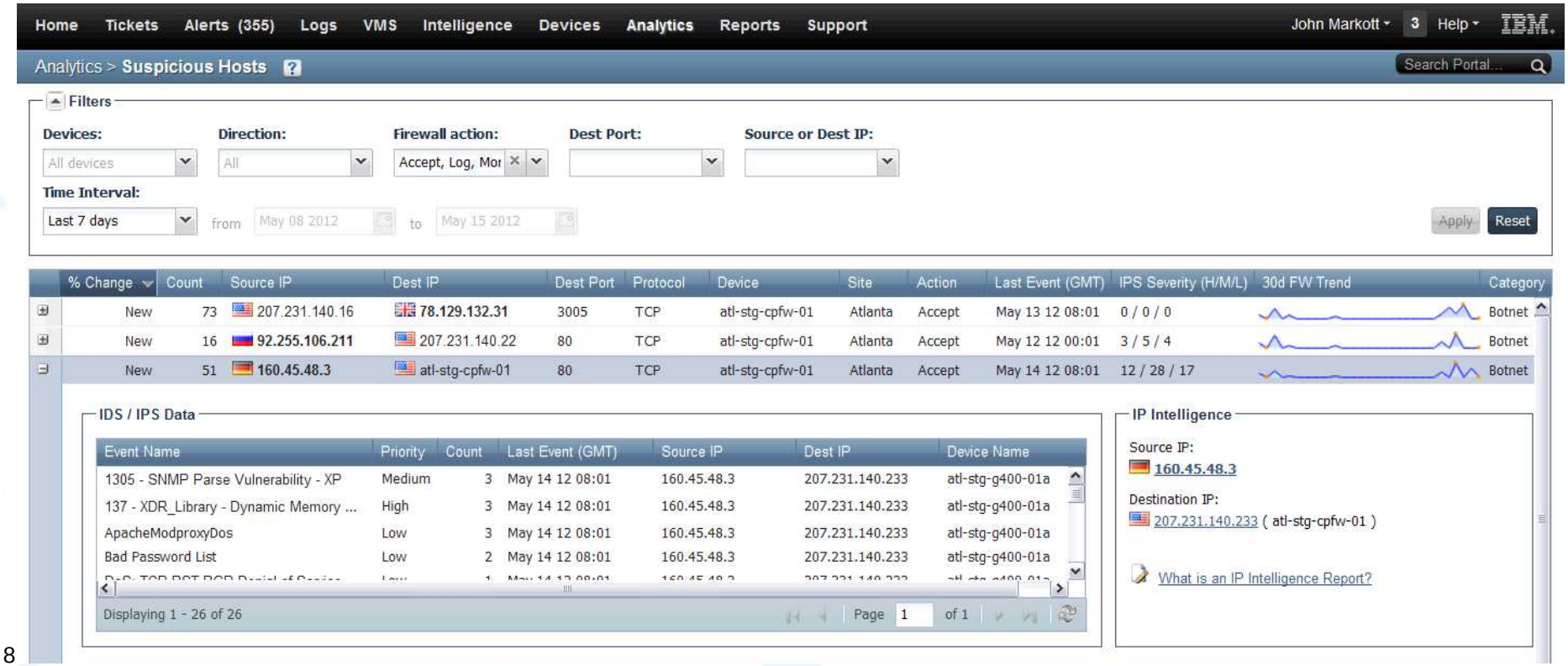
# IBM MSS Security Analytics

# Suspicious Host Dashboard

Identifies connections with botnet command and control, and prioritizes the most active….

Available to all customers who send firewall logs to the Virtual SOC Portal.

Use Case #1 : Identification of reconnaissance (e.g. TCP port 1443 from suspicious host)
Use Case #2 : Gain visibility despite encryption or obfuscation



# Best Practice usage of Suspicious Host Results available in the vSOC Portal

1. *Validate the threat*

2. *Adjust FW/IPS Policy*

3. *Quarantine the machine*

4. *Scan the machine*

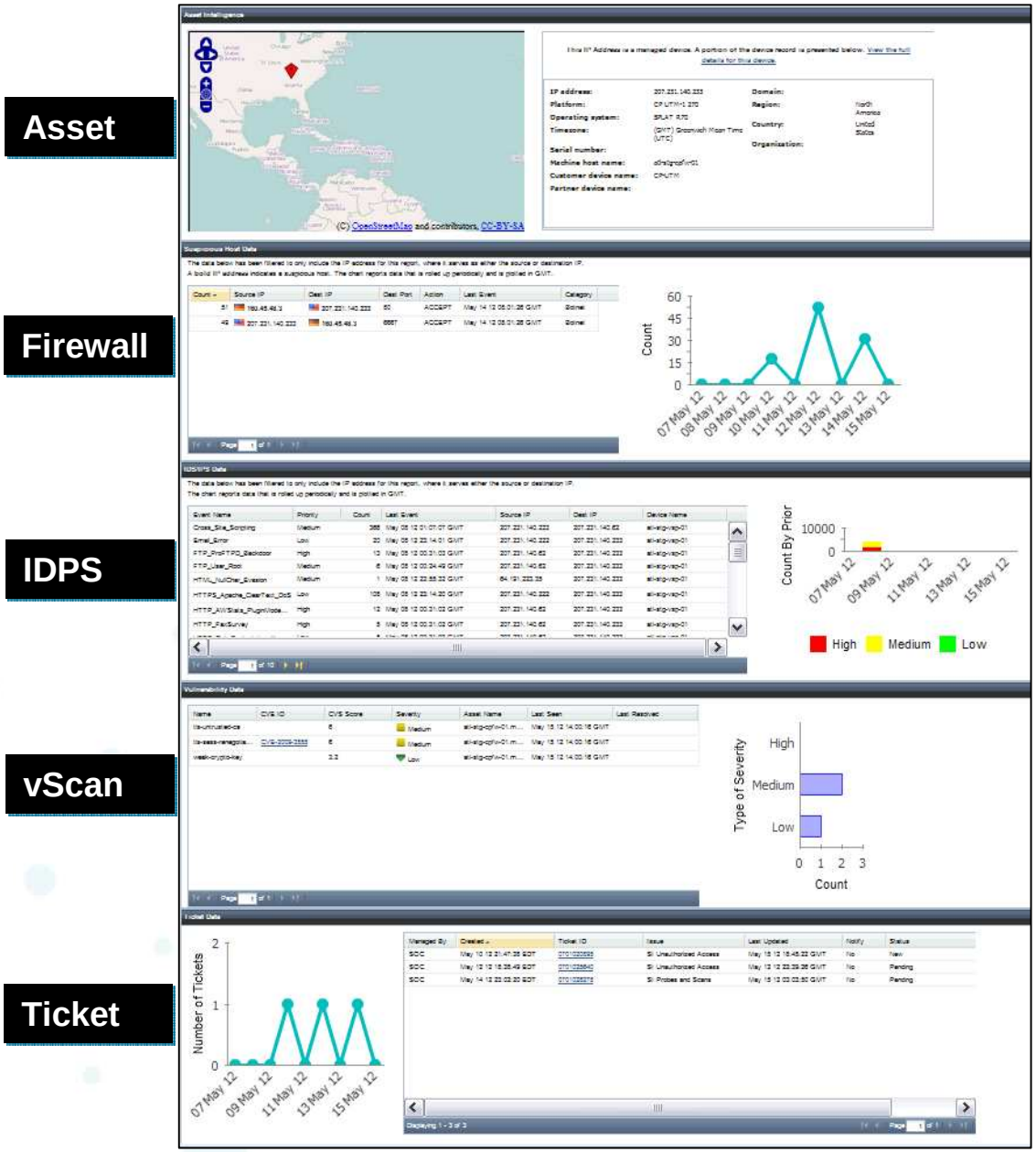
5. *If malware if identified: follow your incident response procedure*

6. *If no malware if found: consider to reimage the OS and application and monitor Suspicious Host Dashboard for additional indication*

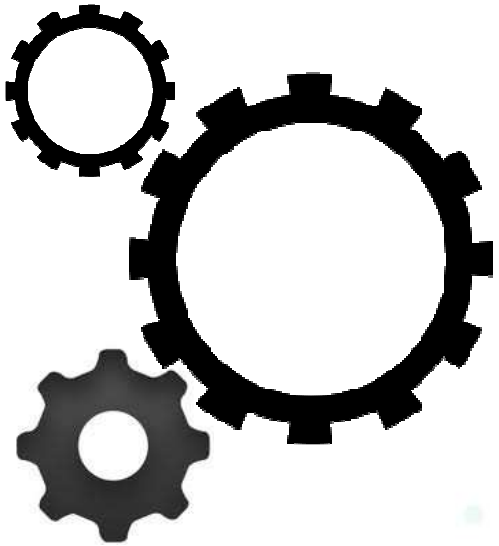
7. *Record all mitigation activities*

# IP Intelligence Report

- On demand IP Reputation and Profiling of attacker or victim addresses.
- Saves customers time and complexity by consolidating multiple summary views into a single pane.
- Available in the Virtual SOC Portal to all customers who subscribe to one or more of the following services:
  1. Managed FW
  2. Managed IDPS
  3. Managed UTM
  4. Managed Protection Services
  5. Hosted Vuln Mgmt Service
  6. Hosted SELM
- Accessible from most places where an IP address is displayed



# Automated Intelligence (AI) and Type of Correlations provided



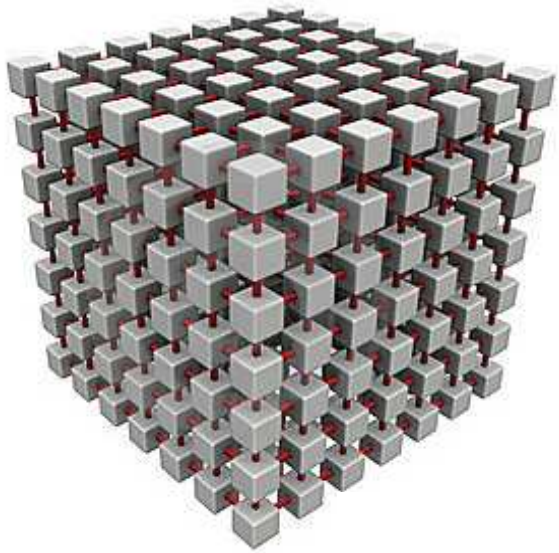
## Statistical and Comparative Analysis
based on individual alerts or frequency and volume of alerts

## Behavioral correlation
based on sequence of alerts

## Historical cross-platform correlation
based on the availability of up to 7 years of forensically sound, live data

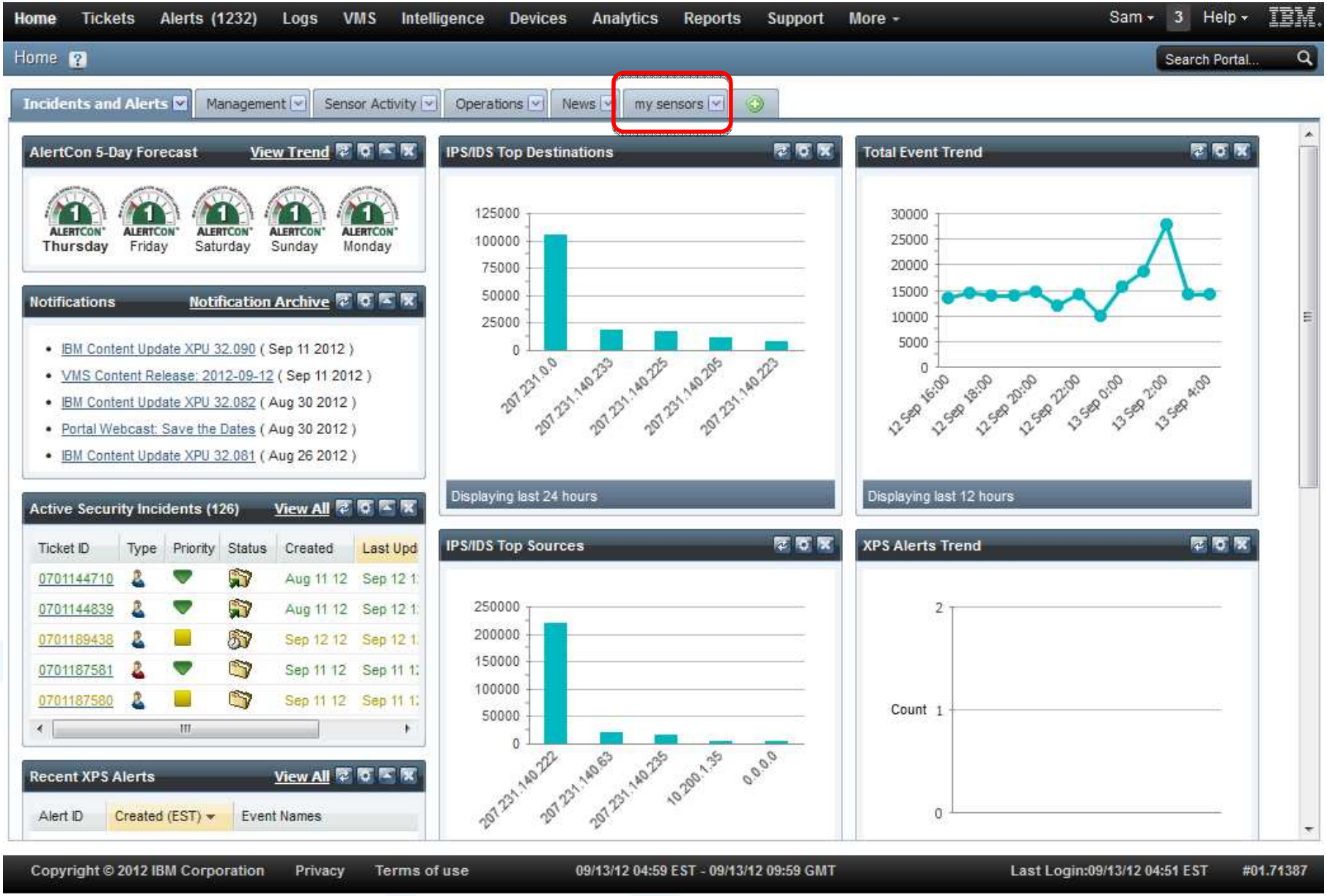
## Vulnerability correlation
based on vulnerable and critical hosts information

## Global Intelligence correlation
number of customer targeted
industries affected
attack sequence and tools used
vulnerability exploited

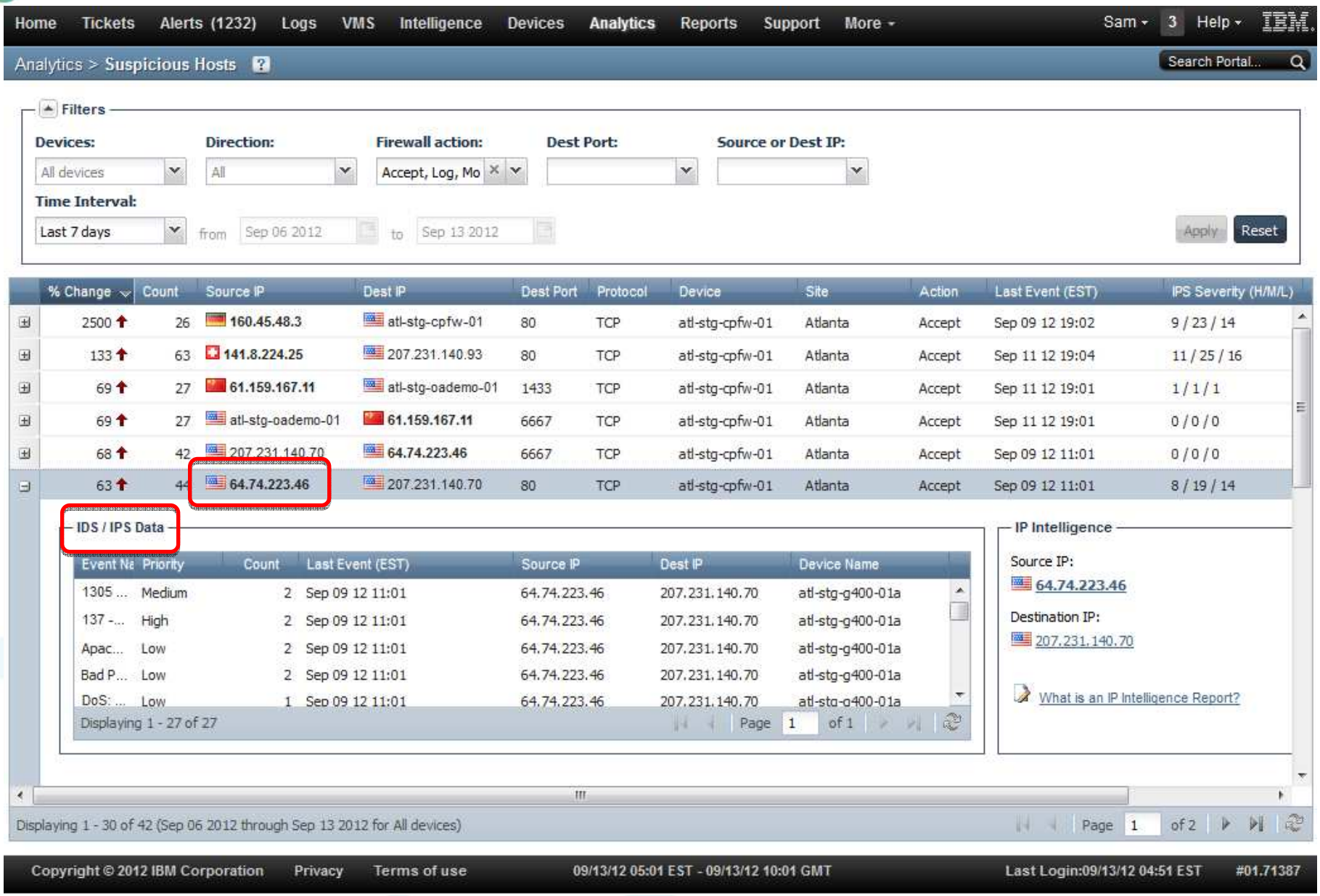


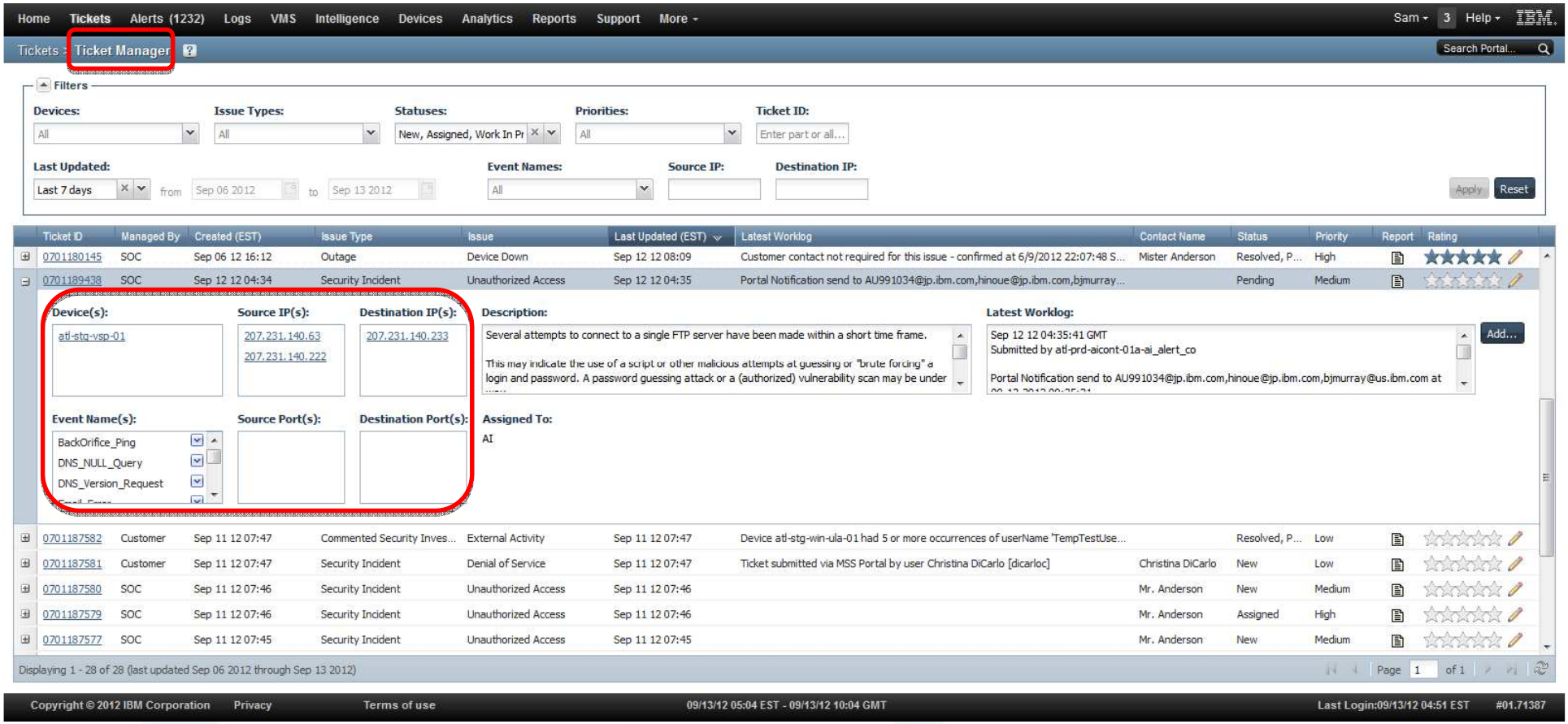
# vSOC Portal Overview

# 18 settembre: Missione Sicurezza

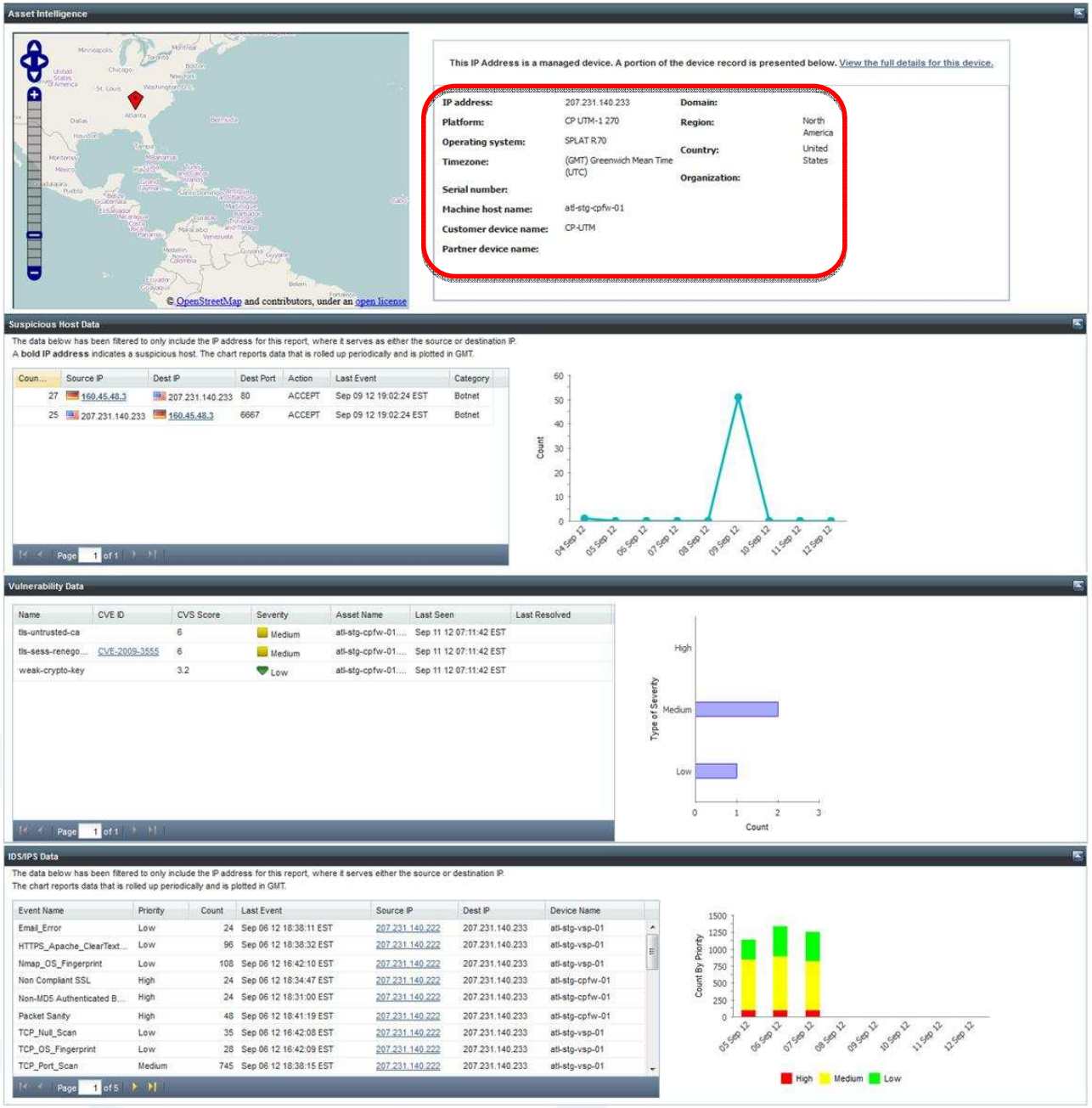


# 18 settembre: Missione Sicurezza

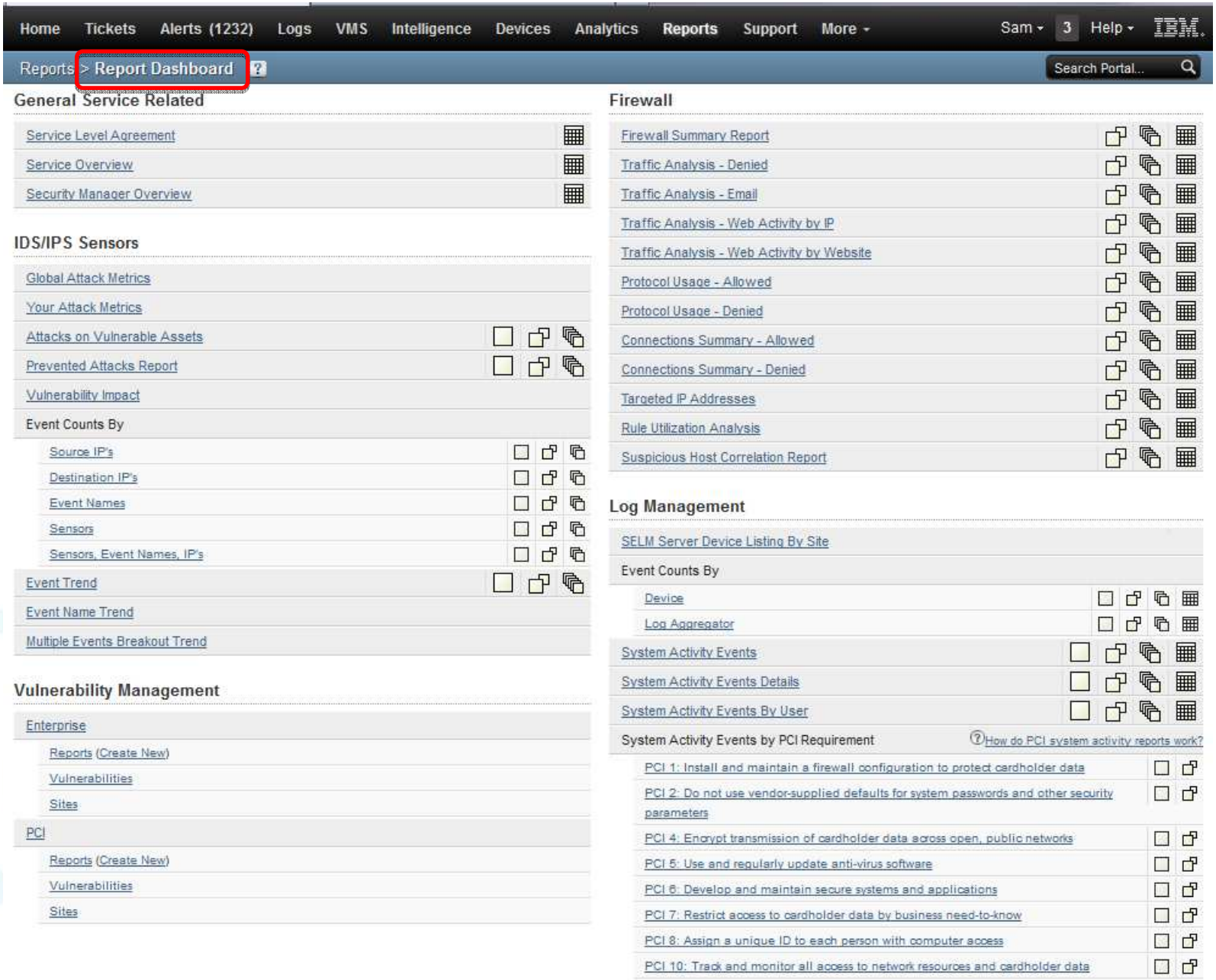




# 18 settembre: Missione Sicurezza



# 18 settembre: Missione Sicurezza



# *Thank you !*