

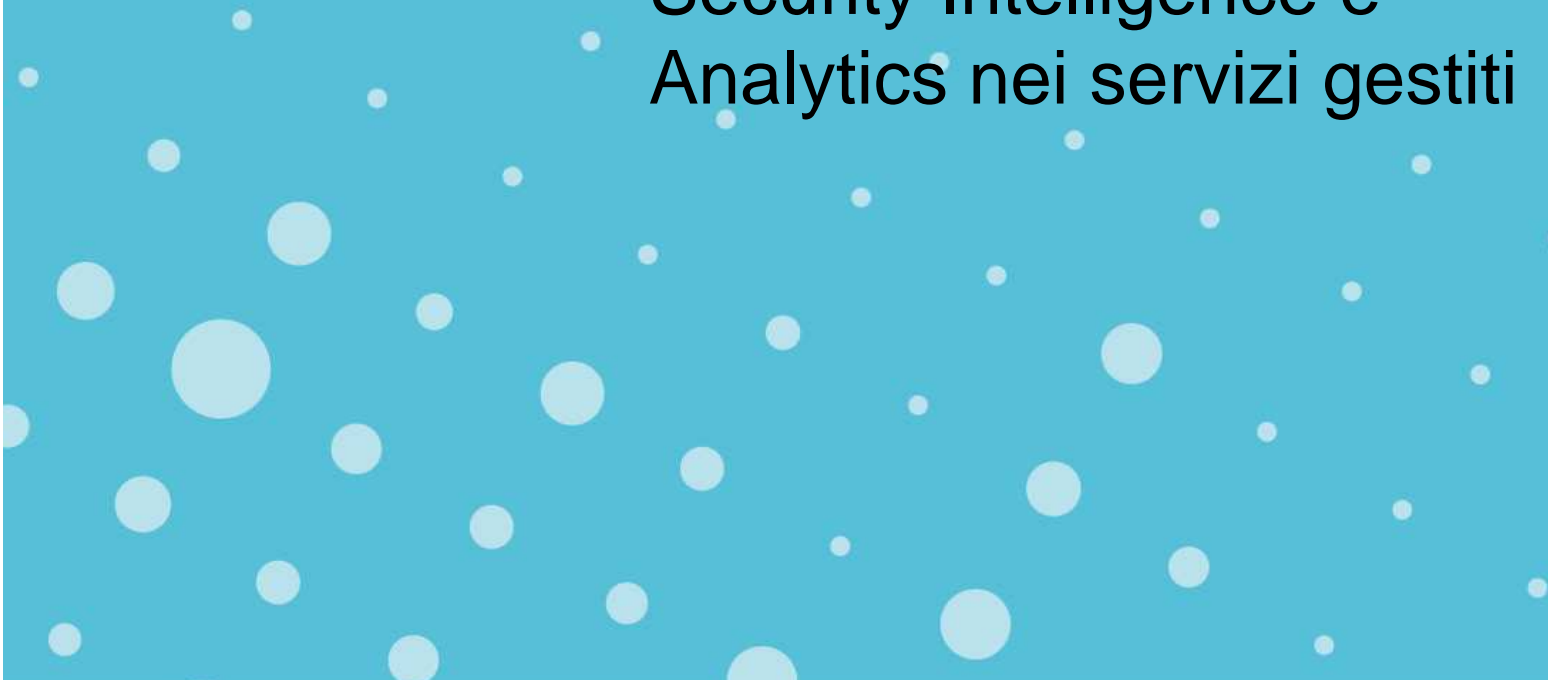
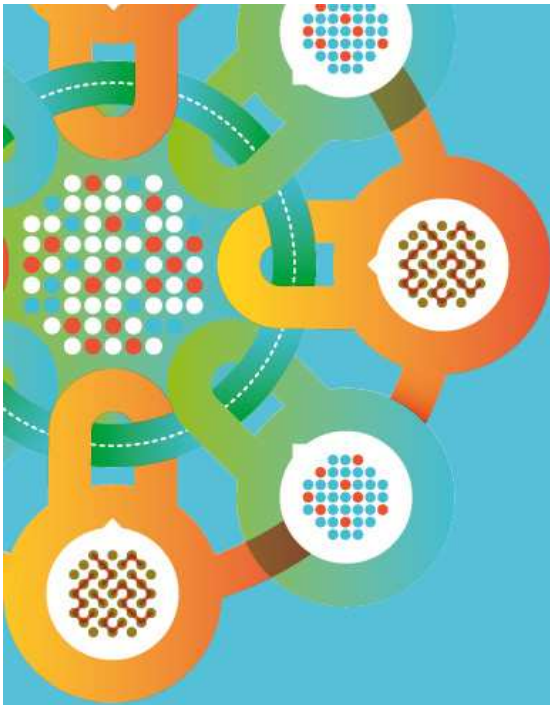
IBM Forum Segrate - Milano



18 settembre: Missione Sicurezza

Identifica e combatti i rischi con la Security Intelligence IBM

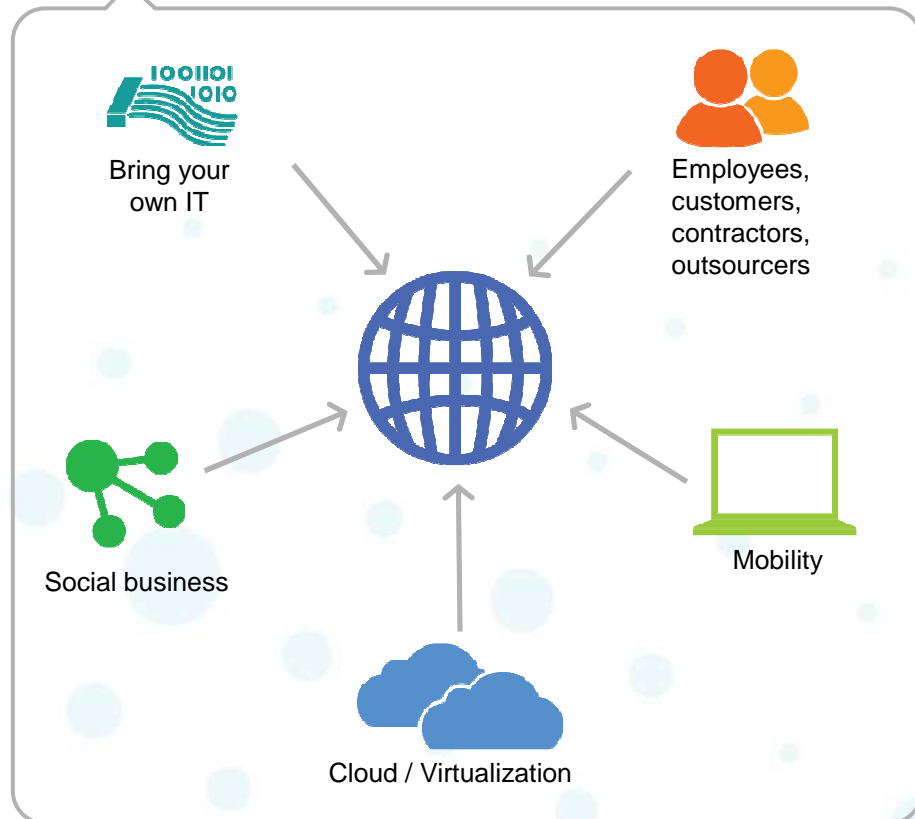
Samuele Battistoni
Security Intelligence e
Analytics nei servizi gestiti



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 spam and phishing attacks
46K documented vulnerabilities and millions of unique malware samples



Worldwide managed security services coverage

- 20,000-plus devices under contract
- 3,300 GTS¹ service delivery experts
- 3,700-plus MSS² clients worldwide
- 15B-plus events managed per day
- 1,000-plus security patents
- 133 monitored countries (MSS)

³ 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)

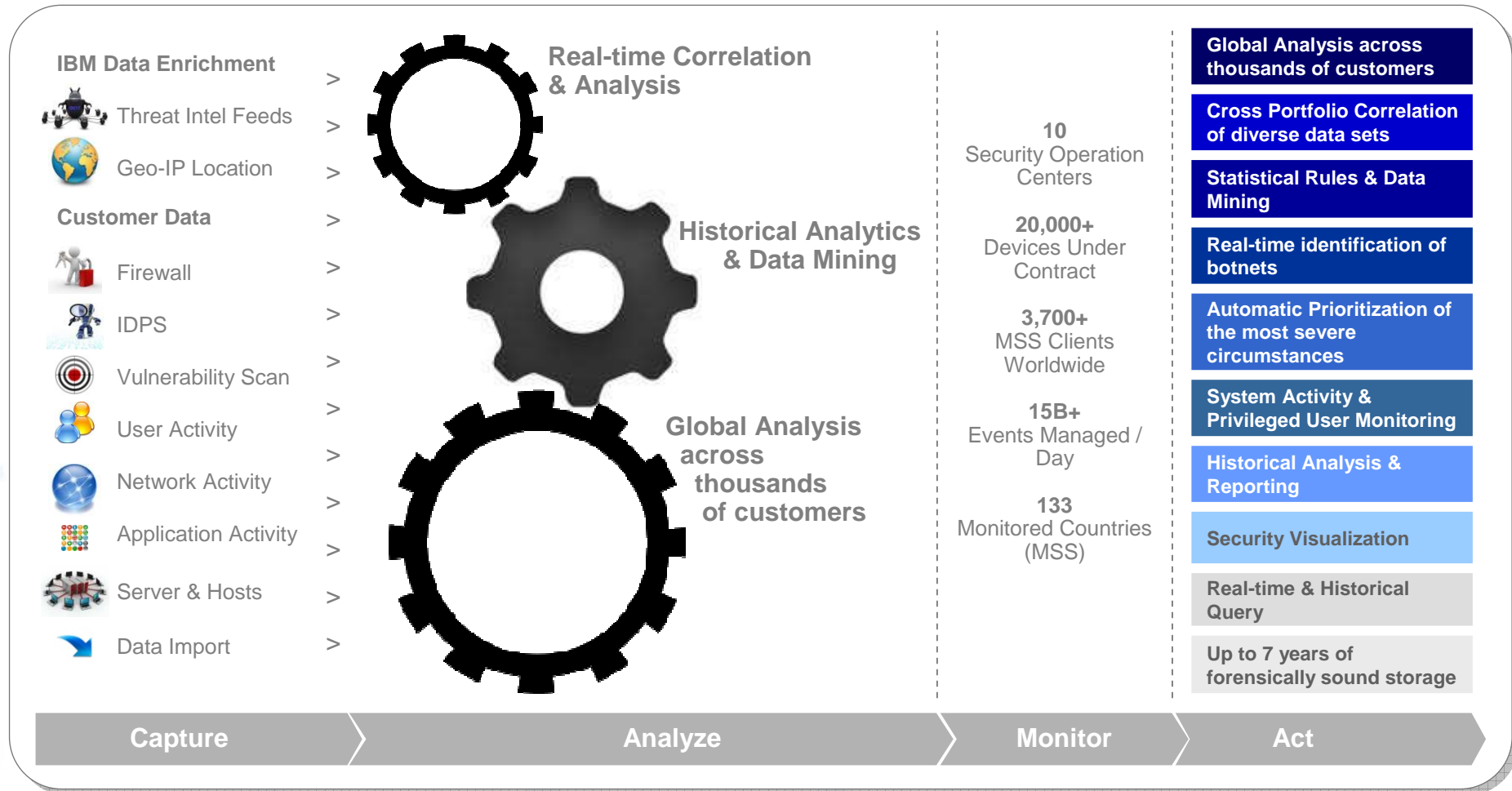
- Hosted security event and log management services
- Hosted vulnerability management services
- Hosted application scanning
- Hosted mobile device security management
- Hosted managed e-mail and web security
- Hosted IBM X-Force threat analysis service



Multiple device types and vendors supported

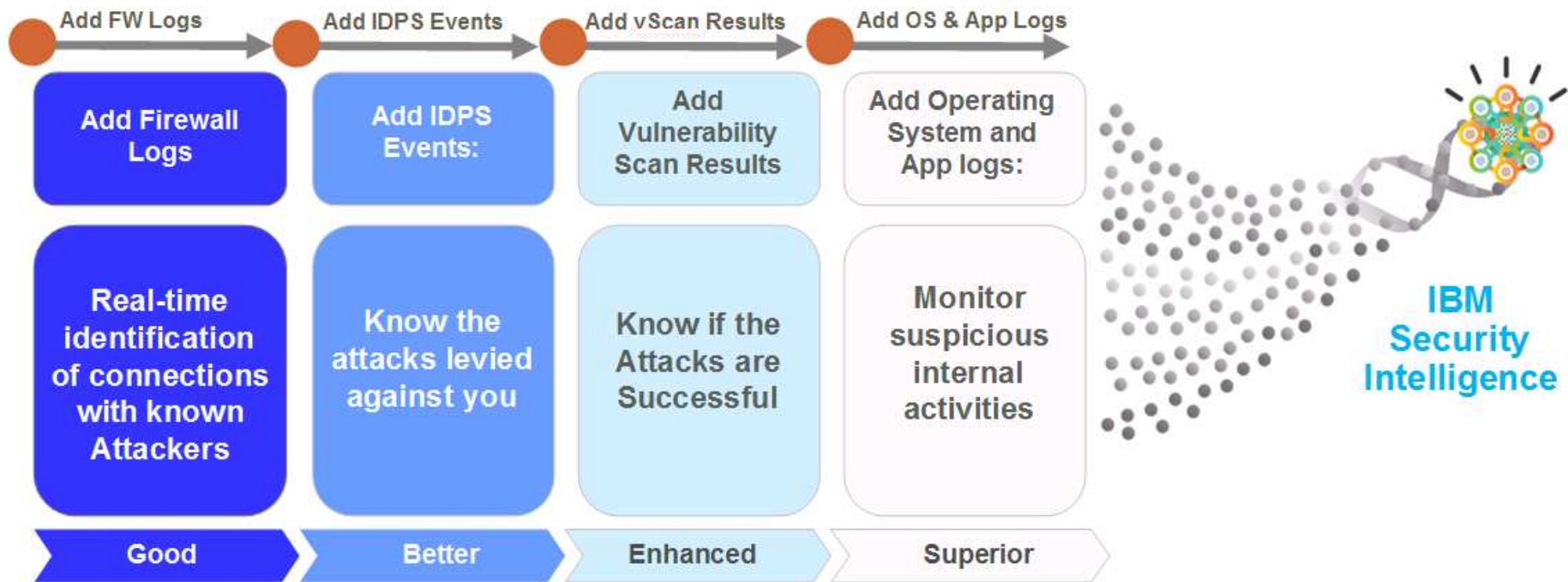


IBM Security Services analytic capabilities



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
 - (2) Managed UTM
 - (3) Hosted SELM
- (1) Managed IDPS
 - (2) Managed UTM
 - (3) MPS
 - (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

Home Tickets Alerts (355) Logs VMS Intelligence Devices Analytics Reports Support John Markott 3 Help IBM

Analytics > Suspicious Hosts Search Portal...

Filters

Devices: All devices Direction: All Firewall action: Accept, Log, Mor Dest Port: Source or Dest IP:

Time Interval: Last 7 days from May 08 2012 to May 15 2012 Apply Reset

% Change	Count	Source IP	Dest IP	Dest Port	Protocol	Device	Site	Action	Last Event (GMT)	IPS Severity (H/M/L)	30d FW Trend	Category
New	73	207.231.140.16	78.129.132.31	3005	TCP	atl-stg-cpfw-01	Atlanta	Accept	May 13 12 08:01	0 / 0 / 0		Botnet
New	16	92.255.106.211	207.231.140.22	80	TCP	atl-stg-cpfw-01	Atlanta	Accept	May 12 12 00:01	3 / 5 / 4		Botnet
New	51	160.45.48.3	atl-stg-cpfw-01	80	TCP	atl-stg-cpfw-01	Atlanta	Accept	May 14 12 08:01	12 / 28 / 17		Botnet

IDS / IPS Data

Event Name	Priority	Count	Last Event (GMT)	Source IP	Dest IP	Device Name
1305 - SNMP Parse Vulnerability - XP	Medium	3	May 14 12 08:01	160.45.48.3	207.231.140.233	atl-stg-g400-01a
137 - XDR_Library - Dynamic Memory ...	High	3	May 14 12 08:01	160.45.48.3	207.231.140.233	atl-stg-g400-01a
ApacheModproxyDos	Low	3	May 14 12 08:01	160.45.48.3	207.231.140.233	atl-stg-g400-01a
Bad Password List	Low	2	May 14 12 08:01	160.45.48.3	207.231.140.233	atl-stg-g400-01a
Bad TCP RST DOS Denial of Service	Low	1	May 14 12 08:01	160.45.48.3	207.231.140.233	atl-stg-g400-01a

Displaying 1 - 26 of 26 Page 1 of 1

IP Intelligence

Source IP: 160.45.48.3

Destination IP: 207.231.140.233 (atl-stg-cpfw-01)

What is an IP Intelligence Report?



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 is identified: follow your incident response procedure*
6. *If no malware is 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

Asset

Firewall

IDPS

vScan

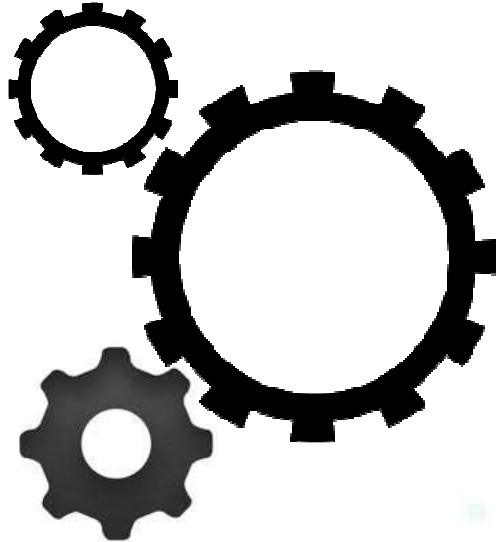
Ticket

The screenshot displays a comprehensive IP Intelligence Report interface with the following sections:

- Asset Intelligence:** Includes a map of Europe and a detailed profile for IP address 207.221.140.233, listing details such as Platform (CPU:1711-1 210), Operating system (SLAT 3.70), Timezone (GMT Greenwich Mean Time (UTC)), Serial number, Machine host name (slatgpfw01), Customer device name (CPU:1711), and Partner device name.
- Suspicious Host Data:** Features a table of suspicious host activity and a line graph showing the count of events from 07 May 12 to 15 May 12.
- IDS/IPS Data:** Contains a table of intrusion detection and prevention events, including event name, priority, count, last seen time, source and destination IP addresses, and device name.
- Vulnerability Data:** Shows a table of identified vulnerabilities with columns for Name, CVE ID, CVE Score, Severity, Asset Name, Last Seen, and Last Resolved.
- Ticket Data:** Includes a table of system tickets and a line graph showing the number of tickets over time.



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

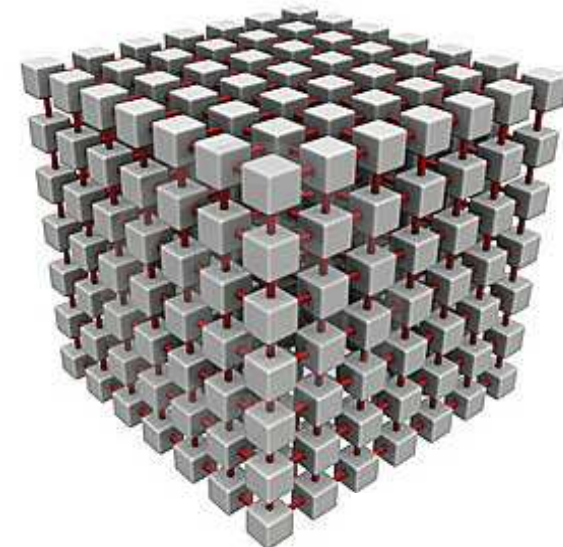
based on the availability of up to 7 years of forensically sound, live data

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



- ### Notifications
- [Notification Archive](#)
- IBM Content Update XPU 32.090 (Sep 11 2012)
 - VMS Content Release: 2012-09-12 (Sep 11 2012)
 - IBM Content Update XPU 32.082 (Aug 30 2012)
 - Portal Webcast: Save the Dates (Aug 30 2012)
 - IBM Content Update XPU 32.081 (Aug 26 2012)

Active Security Incidents (126)

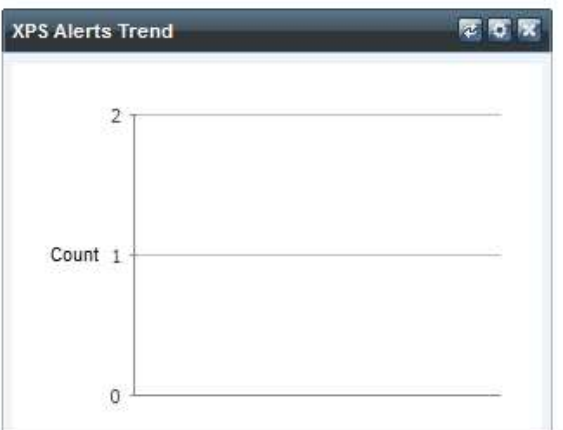
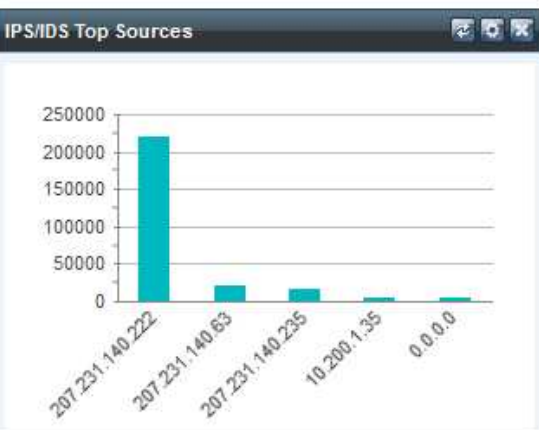
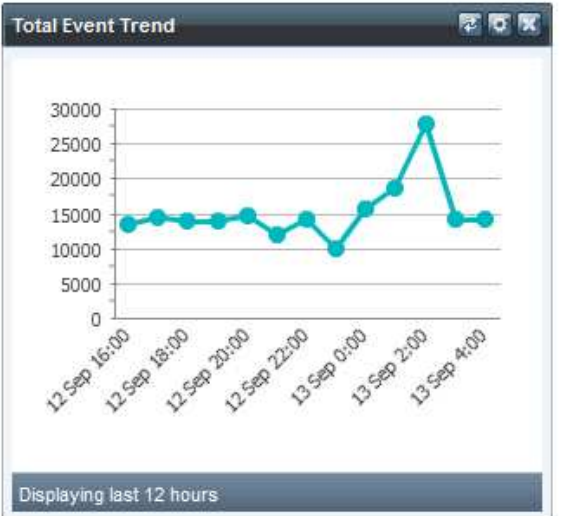
[View All](#)

Ticket ID	Type	Priority	Status	Created	Last Upd
0701144710				Aug 11 12	Sep 12 1:
0701144839				Aug 11 12	Sep 12 1:
0701189438				Sep 12 12	Sep 12 1:
0701187581				Sep 11 12	Sep 11 1:
0701187580				Sep 11 12	Sep 11 1:

Recent XPS Alerts

[View All](#)

Alert ID	Created (EST)	Event Names
----------	---------------	-------------





Filters

Devices: ▾
Direction: ▾
Firewall action: ▾
Dest Port: ▾
Source or Dest IP: ▾

Time Interval: ▾
from to

Apply Reset

% Change ▾	Count	Source IP	Dest IP	Dest Port	Protocol	Device	Site	Action	Last Event (EST)	IPS Severity (H/M/L)
2500 ↑	26	160.45.48.3	atl-stg-cpfw-01	80	TCP	atl-stg-cpfw-01	Atlanta	Accept	Sep 09 12 19:02	9 / 23 / 14
133 ↑	63	141.8.224.25	207.231.140.93	80	TCP	atl-stg-cpfw-01	Atlanta	Accept	Sep 11 12 19:04	11 / 25 / 16
69 ↑	27	61.159.167.11	atl-stg-oademo-01	1433	TCP	atl-stg-cpfw-01	Atlanta	Accept	Sep 11 12 19:01	1 / 1 / 1
69 ↑	27	atl-stg-oademo-01	61.159.167.11	6667	TCP	atl-stg-cpfw-01	Atlanta	Accept	Sep 11 12 19:01	0 / 0 / 0
68 ↑	42	207.231.140.70	64.74.223.46	6667	TCP	atl-stg-cpfw-01	Atlanta	Accept	Sep 09 12 11:01	0 / 0 / 0
63 ↑	44	64.74.223.46	207.231.140.70	80	TCP	atl-stg-cpfw-01	Atlanta	Accept	Sep 09 12 11:01	8 / 19 / 14

IDS / IPS Data

Event No	Priority	Count	Last Event (EST)	Source IP	Dest IP	Device Name
1305 ...	Medium	2	Sep 09 12 11:01	64.74.223.46	207.231.140.70	atl-stg-g400-01a
137 ...	High	2	Sep 09 12 11:01	64.74.223.46	207.231.140.70	atl-stg-g400-01a
Apac...	Low	2	Sep 09 12 11:01	64.74.223.46	207.231.140.70	atl-stg-g400-01a
Bad P...	Low	2	Sep 09 12 11:01	64.74.223.46	207.231.140.70	atl-stg-g400-01a
DoS: ...	Low	1	Sep 09 12 11:01	64.74.223.46	207.231.140.70	atl-stg-o400-01a

Displaying 1 - 27 of 27

IP Intelligence

Source IP:
[64.74.223.46](#)

Destination IP:
[207.231.140.70](#)

[What is an IP Intelligence Report?](#)



Filters

Devices: All | **Issue Types:** All | **Statuses:** New, Assigned, Work In Pr | **Priorities:** All | **Ticket ID:** Enter part or all...

Last Updated: Last 7 days from Sep 06 2012 to Sep 13 2012 | **Event Names:** All | **Source IP:** | **Destination IP:** | Apply | Reset

Ticket ID	Managed By	Created (EST)	Issue Type	Issue	Last Updated (EST)	Latest Worklog	Contact Name	Status	Priority	Report	Rating
0701180145	SOC	Sep 06 12 16:12	Outage	Device Down	Sep 12 12 08:09	Customer contact not required for this issue - confirmed at 6/9/2012 22:07:48 S...	Mister Anderson	Resolved, P...	High		★★★★★
0701189438	SOC	Sep 12 12 04:34	Security Incident	Unauthorized Access	Sep 12 12 04:35	Portal Notification send to AU991034@jp.ibm.com,hinoue@jp.ibm.com,bjmurray...		Pending	Medium		★★★★★
<div style="border: 2px solid red; padding: 5px;"><p>Device(s): atl-stg-ysp-01 Source IP(s): 207.231.140.63, 207.231.140.222 Destination IP(s): 207.231.140.233</p><p>Description: Several attempts to connect to a single FTP server have been made within a short time frame. This may indicate the use of a script or other malicious attempts at guessing or "brute forcing" a login and password. A password guessing attack or a (authorized) vulnerability scan may be under...</p><p>Event Name(s): BackOffice_Ping, DNS_NULL_Query, DNS_Version_Request</p><p>Source Port(s): Destination Port(s): Assigned To: AI</p><p>Latest Worklog: Sep 12 12 04:35:41 GMT Submitted by atl-prd-aicont-01a-ai_alert_co Portal Notification send to AU991034@jp.ibm.com,hinoue@jp.ibm.com,bjmurray@us.ibm.com at...</p></div>											
0701187582	Customer	Sep 11 12 07:47	Commented Security Inves...	External Activity	Sep 11 12 07:47	Device atl-stg-win-ula-01 had 5 or more occurrences of userName "TempTestUse...		Resolved, P...	Low		★★★★★
0701187581	Customer	Sep 11 12 07:47	Security Incident	Denial of Service	Sep 11 12 07:47	Ticket submitted via MSS Portal by user Christina DiCarlo [dicarlo]	Christina DiCarlo	New	Low		★★★★★
0701187580	SOC	Sep 11 12 07:46	Security Incident	Unauthorized Access	Sep 11 12 07:46		Mr. Anderson	New	Medium		★★★★★
0701187579	SOC	Sep 11 12 07:46	Security Incident	Unauthorized Access	Sep 11 12 07:46		Mr. Anderson	Assigned	High		★★★★★
0701187577	SOC	Sep 11 12 07:45	Security Incident	Unauthorized Access	Sep 11 12 07:45		Mr. Anderson	New	Medium		★★★★★

Displaying 1 - 28 of 28 (last updated Sep 06 2012 through Sep 13 2012) Page 1 of 1



Asset Intelligence

© OpenStreetMap and contributors, under an open license

This IP Address is a managed device. A portion of the device record is presented below. [View the full details for this device.](#)

IP address:	207.231.140.233	Domain:	
Platform:	CP-UTM-1.270	Region:	North America
Operating system:	SPLAT.R70	Country:	United States
Timezone:	(GMT) Greenwich Mean Time (UTC)	Organization:	
Serial number:			
Machine host name:	at-stg-cpfw-01		
Customer device name:	CP-UTM		
Partner device name:			

Suspicious Host Data

The data below has been filtered to only include the IP address for this report, where it serves as either the source or destination IP. A bold IP address indicates a suspicious host. The chart reports data that is rolled up periodically and is plotted in GMT.

Count	Source IP	Dest IP	Dest Port	Action	Last Event	Category
27	160.45.48.3	207.231.140.233	80	ACCEPT	Sep 09 12 19:02:24 EST	Botnet
25	207.231.140.233	160.45.48.3	6667	ACCEPT	Sep 09 12 19:02:24 EST	Botnet

Vulnerability Data

Name	CVE ID	CVSS Score	Severity	Asset Name	Last Seen	Last Resolved
its-untrusted-ca		6	Medium	at-stg-cpfw-01...	Sep 11 12 07:11:42 EST	
its-sess-renego...	CVE-2009-3555	6	Medium	at-stg-cpfw-01...	Sep 11 12 07:11:42 EST	
weak-crypto-key		3.2	Low	at-stg-cpfw-01...	Sep 11 12 07:11:42 EST	

IDS/IPS Data

The data below has been filtered to only include the IP address for this report, where it serves either the source or destination IP. The chart reports data that is rolled up periodically and is plotted in GMT.

Event Name	Priority	Count	Last Event	Source IP	Dest IP	Device Name
Email_Error	Low	24	Sep 06 12 18:38:11 EST	207.231.140.222	207.231.140.233	at-stg-vsp-01
HTTPS_Apache_ClearText...	Low	96	Sep 06 12 18:38:32 EST	207.231.140.222	207.231.140.233	at-stg-vsp-01
Nmap_OS_Fingerprint	Low	108	Sep 06 12 16:42:10 EST	207.231.140.222	207.231.140.233	at-stg-vsp-01
Non-Compliant SSL	High	24	Sep 06 12 18:34:47 EST	207.231.140.222	207.231.140.233	at-stg-cpfw-01
Non-MDS Authenticated B...	High	24	Sep 06 12 18:31:00 EST	207.231.140.222	207.231.140.233	at-stg-cpfw-01
Packet Sanity	High	48	Sep 06 12 18:41:19 EST	207.231.140.222	207.231.140.233	at-stg-cpfw-01
TCP_Null_Scan	Low	35	Sep 06 12 16:42:06 EST	207.231.140.222	207.231.140.233	at-stg-vsp-01
TCP_OS_Fingerprint	Low	28	Sep 06 12 16:42:09 EST	207.231.140.222	207.231.140.233	at-stg-vsp-01
TCP_Port_Scan	Medium	745	Sep 06 12 18:38:15 EST	207.231.140.222	207.231.140.233	at-stg-vsp-01



General Service Related

Service Level Agreement	
Service Overview	
Security Manager Overview	

IDS/IPS Sensors

Global Attack Metrics	
Your Attack Metrics	
Attacks on Vulnerable Assets	
Prevented Attacks Report	
Vulnerability Impact	
Event Counts By	
Source IP's	
Destination IP's	
Event Names	
Sensors	
Sensors, Event Names, IP's	
Event Trend	
Event Name Trend	
Multiple Events Breakout Trend	

Vulnerability Management

Enterprise	
Reports (Create New)	
Vulnerabilities	
Sites	
PCI	
Reports (Create New)	
Vulnerabilities	
Sites	

Firewall

Firewall Summary Report	
Traffic Analysis - Denied	
Traffic Analysis - Email	
Traffic Analysis - Web Activity by IP	
Traffic Analysis - Web Activity by Website	
Protocol Usage - Allowed	
Protocol Usage - Denied	
Connections Summary - Allowed	
Connections Summary - Denied	
Targeted IP Addresses	
Rule Utilization Analysis	
Suspicious Host Correlation Report	

Log Management

SELM Server Device Listing By Site	
Event Counts By	
Device	
Log Aggregator	
System Activity Events	
System Activity Events Details	
System Activity Events By User	
System Activity Events by PCI Requirement <small>? How do PCI system activity reports work?</small>	
PCI 1: Install and maintain a firewall configuration to protect cardholder data	
PCI 2: Do not use vendor-supplied defaults for system passwords and other security parameters	
PCI 4: Encrypt transmission of cardholder data across open, public networks	
PCI 5: Use and regularly update anti-virus software	
PCI 6: Develop and maintain secure systems and applications	
PCI 7: Restrict access to cardholder data by business need-to-know	
PCI 8: Assign a unique ID to each person with computer access	
PCI 10: Track and monitor all access to network resources and cardholder data	



Thank you !