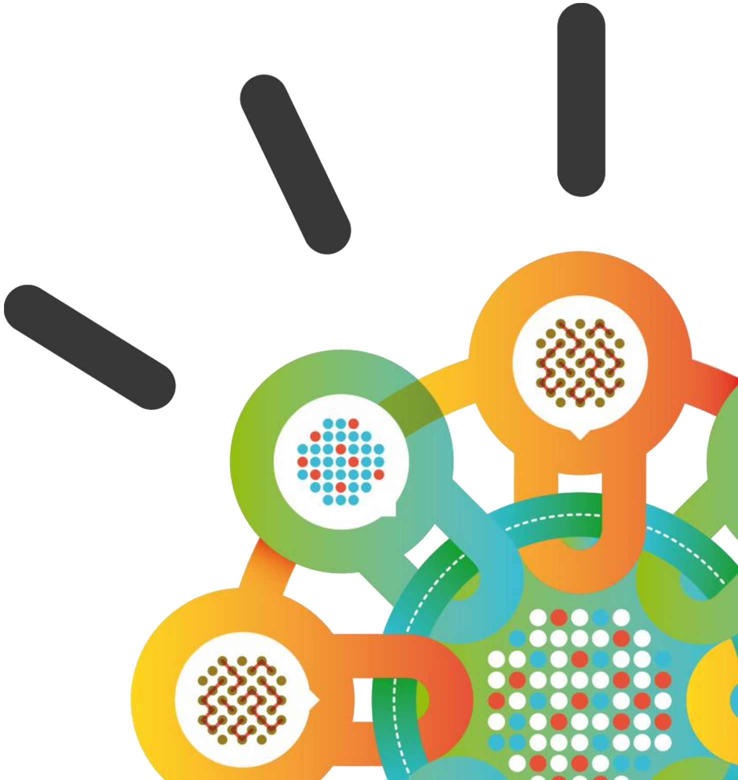
Security Intelligence.
Think Integrated.

The Value of Integration

Dramatically Differentiating

IBM Security Solutions vs. our competition

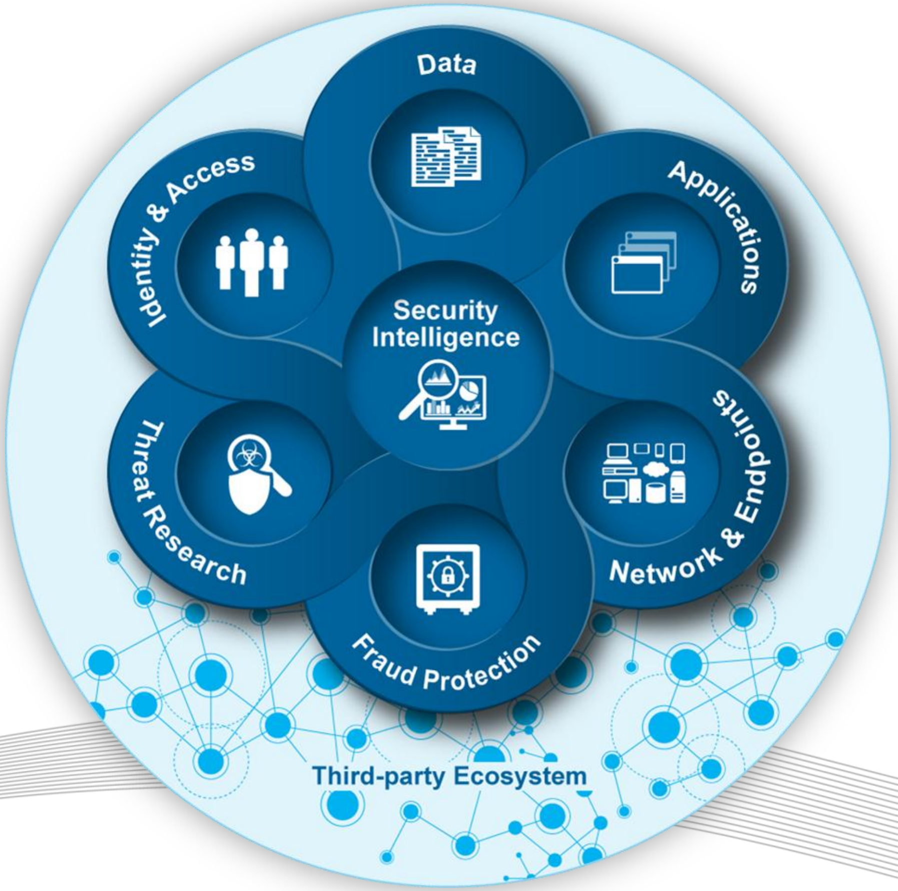


IBM internal and Business Partner use only

Security can be a complex landscape…

85 tools from 45 vendors

Expand the value of security solutions through integration



Integrated intelligence

Correlate and analyze siloed information from hundreds of sources to automatically detect and respond to threats

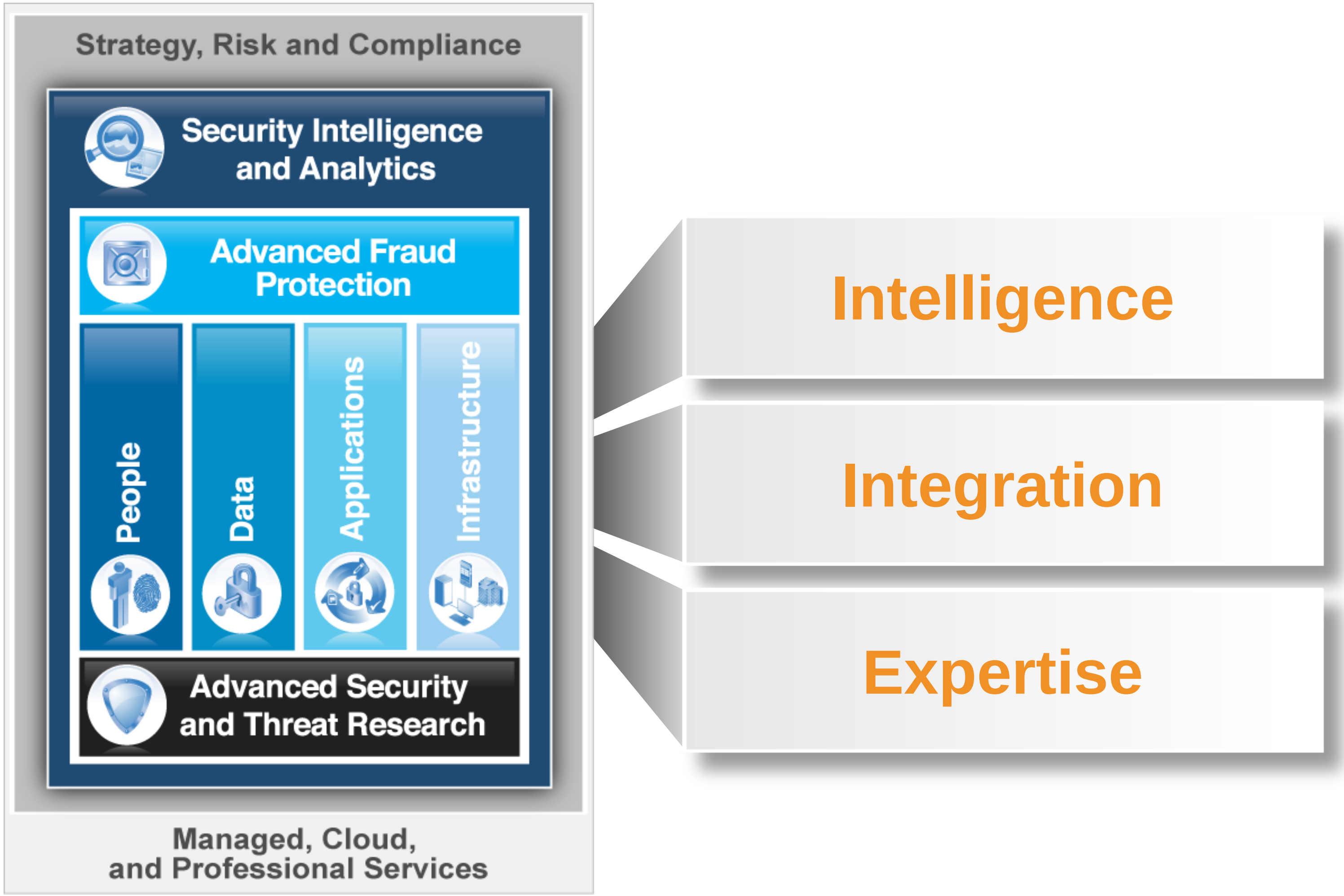
Integrated protection

Enhance security with security solutions that interact across domains to provide cohesive, easy to manage protection

Integrated research

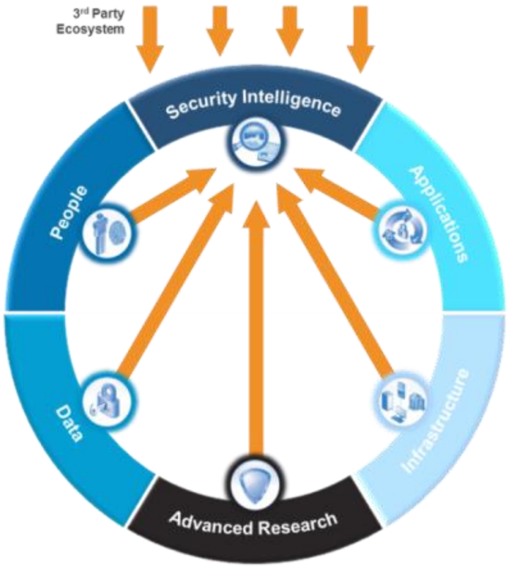
Incorporate the latest information on vulnerabilities, exploits and malware into intelligent security solutions across domains

IBM delivers intelligence, integration and expertise across a comprehensive framework


Strategy, Risk and Compliance
Security Intelligence and Analytics
Advanced Fraud Protection
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Managed, Cloud, and Professional Services
Intelligence
Integration
Expertise

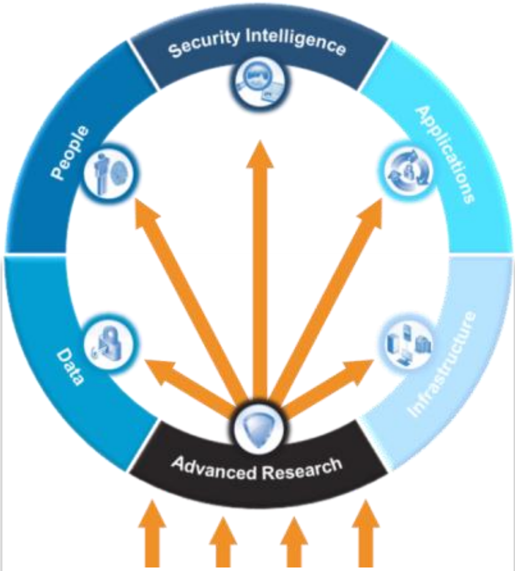
Integration Increases security, collapses silos, and reduces complexity

Integrated Intelligence.



Consolidate and correlate siloed information from hundreds of sources

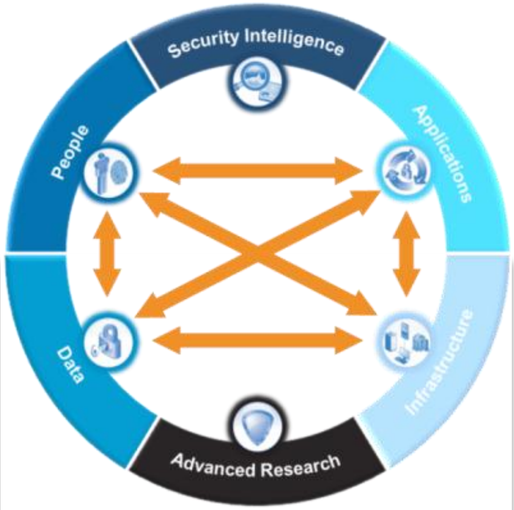
Integrated Research.



Stay ahead of the changing threat landscape

X-FORCE
X-Force Threat Intelligence Cloud

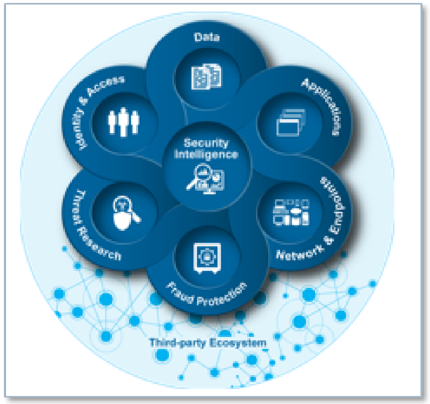
Integrated Protection.



Link security and vulnerability information across domains

Integration Reference Document – 15 Páginas de descripciones

IBM Security Product Integration Reference



IBM's security products are highly integrated – across IBM solutions and with non-IBM solutions via standards adoption.

Where integration standards exist, we follow them (and often make significant contributions to those standards). Where they don't exist, we develop technologies to drive/enhance integration and interoperability. Consider the examples of both types of integration in the table that follows.

Blue-highlighted text indicates areas where IBM is delivering integration or interoperability that is unique in the industry.

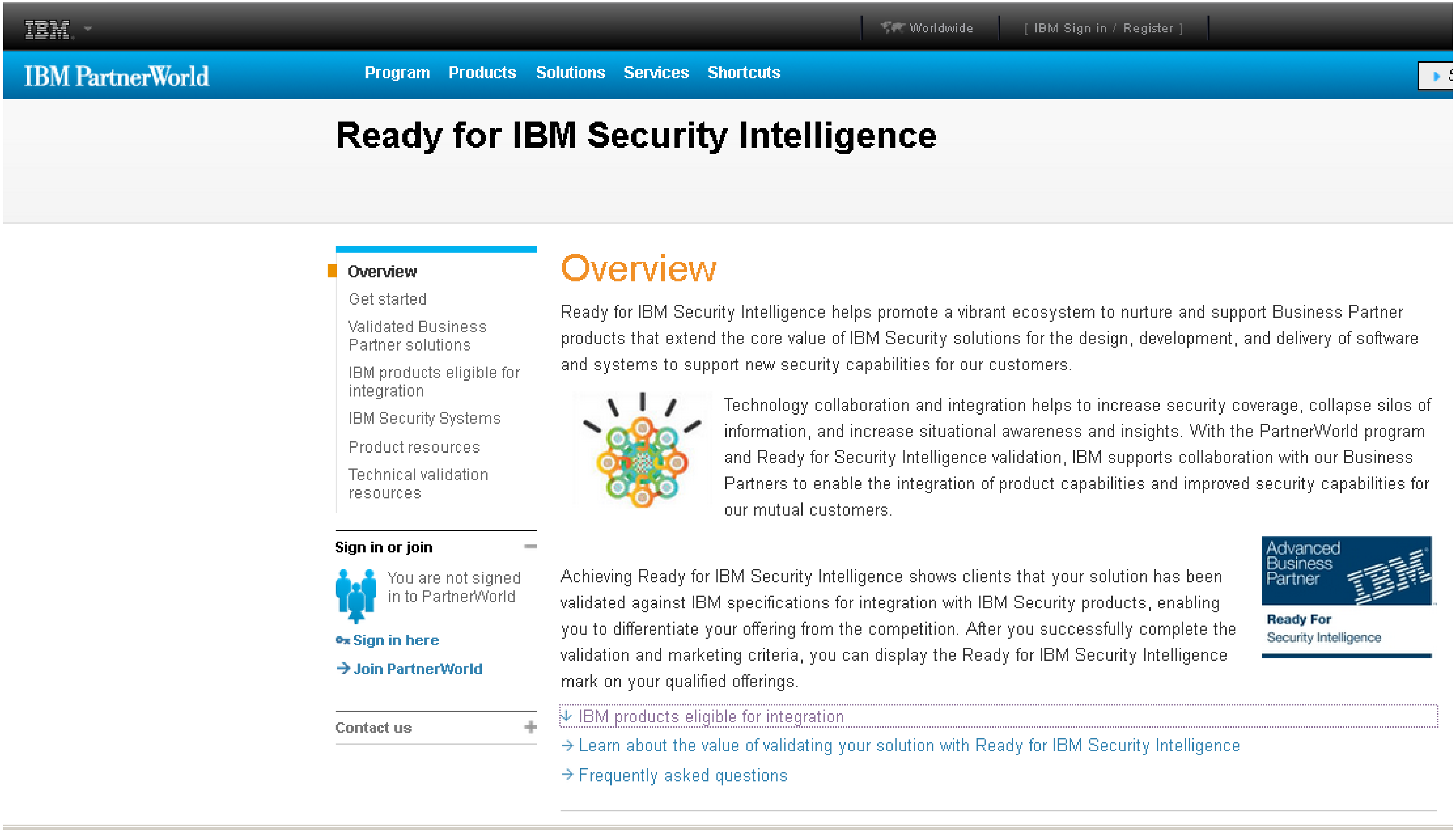
Following this table of integration examples are 2 appendixes:

- Appendix A highlights a major area of integration focus within IBM Security Systems – the IBM Threat Protection System.
- Appendix B places the integration examples in the context of the CAMS categories – Cloud, Analytics, Mobile and Social … thereby providing examples of how this integration helps customers benefit from security integration in CAMS projects/outcomes.

IBM Security Framework Segment	Standards-Based Integration Examples	Proprietary Integration Examples
Security Intelligence	• QRadar supports a wide range of event collection standards - syslog, SNMP, OpSec, SDEE, JDBC and others. • QRadar is unique in terms of the depth to which it can add to the collected security intelligence and factor it into a more accurate picture of attack status and what to do about it. It is expandable with event processor, flow processor, and combined event and flow processor appliances. It can directly collect NetFlow, J-Flow, sFlow and IPFIX data. • QRadar supports the IF-MAP standard for	• Device support modules (DSMs) have been written to allow the QRadar platform to accept, analyze and derive meaning from event and audit log information originating from a vast array of hardware and software sources, including both z mainframe and distributed sources. For the latest list of products supported by QRadar SIEM DSMs, see the "IBM Security QRadar DSM Configuration Guide" on the "IBM Security QRadar SIEM Product Documentation for 7.2.1" page • From the perspective of integration across IBM security products, QRadar DSMs are available for Trusteer Apex, IBM Security Access Manager, IBM

IBM Security Framework Segment	Standards-Based Integration Examples	Proprietary Integration Examples
People (Identity and Access Management)	• The LDAP V3 standard is implemented in highly scalable, highly available IBM Security Directory Server product, which is delivered in many IBM security, transactional, and other solutions today. • IBM Security Directory Server is The Open Group LDAP v2 certified, and its last Common Criteria certification was at an EAL 4 level. • Access Manager for Web can work with IBM Security Directory Server or with many other, LDAP V3-compliant registries • Access Manager for Web supports SSO and Web Access Management (WAM) to Web and application servers as well as Kerberos and J2EE environments and can support a broad range of single sign-on methods. • SAM ESSO supports a broad array of multi-factor authentication devices, including: ○ Charismathics USB Key (smart card) ○ HID Prox Cards ○ HID iClass Cards ○ Indala Cards ○ Mifare Cards ○ RFIDeas' iTag ○ EM Cards ○ XyLoc Cards ○ RFIDeas pcProx-Sonar ○ UPEK fingerprint readers ○ DigitalPersona fingerprint readers ○ Lenovo ThinkPad fingerprint readers ○ Other BioAPI compliant readers, subject to test certification ○ Other BIO-key supported readers, subject to test certification ○ VASCO OTP tokens ○ Authenex OTP (OATH) tokens ○ Other OATH compliant tokens, subject to test certification ○ Cell phone authentication ○ Smart cards compatible with Gemalto, Charismatics and SafeSign certified middleware • Access Manager's support for HTTP 1.1 essentially makes it interoperable with any of today's browsers, whether on a workstation, laptop, tablet or mobile phone	• Customers attempting to access an Access Manager protected resource can be required to use a Trusteer Secure Browser for access. • The Trusteer Mobile Browser can make Access Manager aware of the status of the connecting mobile device, preventing, for example, connections from infected or jail-broken phones. • A primary strength of the Access Manager family of products is its integration with a wealth of target applications, directories and environments. The impressive specifics behind this are covered in the IBM Security Integration Factory page. • The IAM portfolio is standardizing on Cognos reporting. At present Identity Manager and Federated Identity Manager use Cognos reporting. • IBM's Access Management Appliances (physical and virtual) are threat aware, thanks to the Web application subset of X-Force's Protocol Analysis Module (PAM) being implemented in the appliances. X-Force feeds provide Access Manager customers with the latest protection against web application attacks. • Identity Manager's role-based management integrates seamlessly with an Access Manager for Web's set of group definitions and corresponding access rules. Identity Manager can create/manage Access Manager for Web's groups. • Identity Manager can synchronize Access Manager for Web passwords • Identity Manager includes an Access Manager for Web adapter. Therefore, all of the value accruing to the automated lifecycle management of Identity Manager's workflow and its reconciliation/recertification capabilities apply to Access Manager for Web and its target applications. • The Web SSO that Access Manager for Web provides can include SSO for Identity Manager administrators into the Identity Manager administrator GUI. • Access Managers supports .NET, ASP.NET, IIS, SharePoint, Exchange and Office 365. • IBM Security Directory Integrator's connectors form the 'fit and finish' glue code for countless identity and access management implementations. Its purpose is interoperability and it is used (among many other examples) to build Identity Manager adapters, to build identity warehouses in Access Manager, to handle identity token mapping in Federated Identity Manager, and much more. Through its flexibility, Directory Integrator allows

Ready for IBM Security Intelligence



Ready for IBM Security Intelligence

Overview
Get started
Validated Business Partner solutions
IBM products eligible for integration
IBM Security Systems
Product resources
Technical validation resources

Sign in or join

You are not signed in to PartnerWorld

Overview

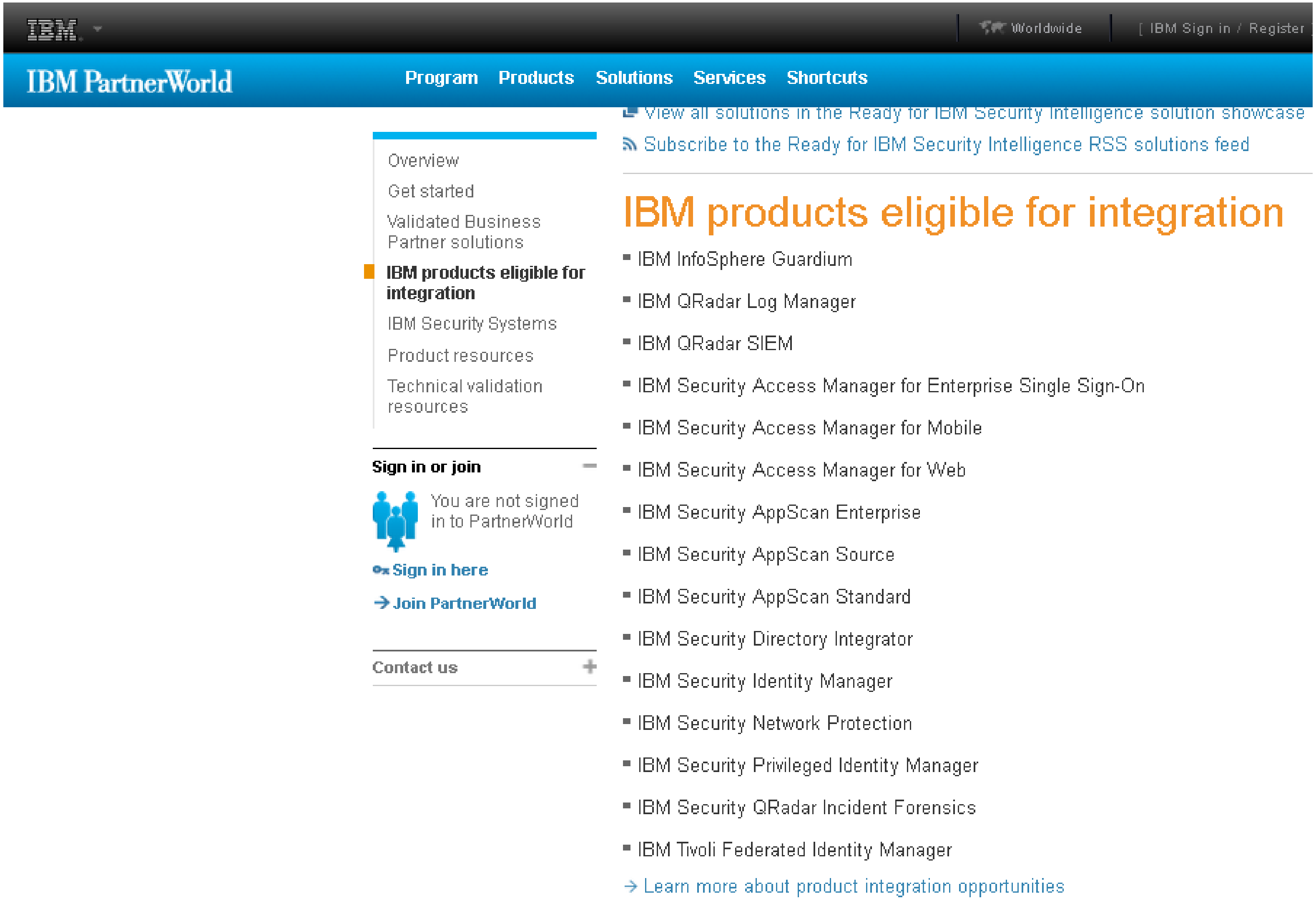
Ready for IBM Security Intelligence helps promote a vibrant ecosystem to nurture and support Business Partner products that extend the core value of IBM Security solutions for the design, development, and delivery of software and systems to support new security capabilities for our customers.

Technology collaboration and integration helps to increase security coverage, collapse silos of information, and increase situational awareness and insights. With the PartnerWorld program and Ready for Security Intelligence validation, IBM supports collaboration with our Business Partners to enable the integration of product capabilities and improved security capabilities for our mutual customers.

Achieving Ready for IBM Security Intelligence shows clients that your solution has been validated against IBM specifications for integration with IBM Security products, enabling you to differentiate your offering from the competition. After you successfully complete the validation and marketing criteria, you can display the Ready for IBM Security Intelligence mark on your qualified offerings.

IBM products eligible for integration
Learn about the value of validating your solution with Ready for IBM Security Intelligence
Frequently asked questions

Ready for IBM Security Intelligence



View all solutions in the Ready for IBM Security Intelligence solution showcase

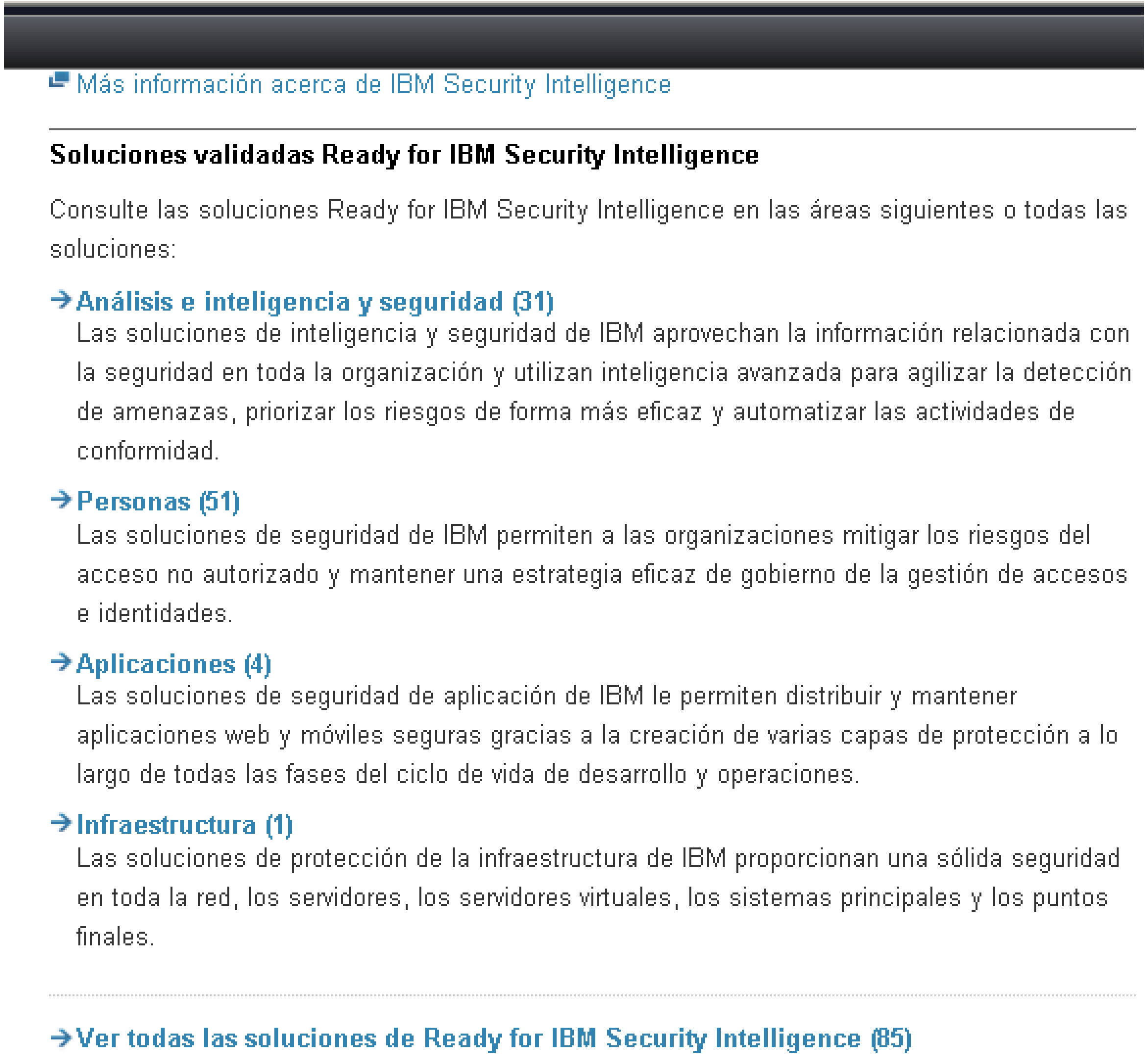
Subscribe to the Ready for IBM Security Intelligence RSS solutions feed

IBM products eligible for integration

- IBM InfoSphere Guardium
- IBM QRadar Log Manager
- IBM QRadar SIEM
- IBM Security Access Manager for Enterprise Single Sign-On
- IBM Security Access Manager for Mobile
- IBM Security Access Manager for Web
- IBM Security AppScan Enterprise
- IBM Security AppScan Source
- IBM Security AppScan Standard
- IBM Security Directory Integrator
- IBM Security Identity Manager
- IBM Security Network Protection
- IBM Security Privileged Identity Manager
- IBM Security QRadar Incident Forensics
- IBM Tivoli Federated Identity Manager

→ Learn more about product integration opportunities

Ready for IBM Security Intelligence



Más información acerca de IBM Security Intelligence

Soluciones validadas Ready for IBM Security Intelligence

Consulte las soluciones Ready for IBM Security Intelligence en las áreas siguientes o todas las soluciones:

→ **Análisis e inteligencia y seguridad (31)**
Las soluciones de inteligencia y seguridad de IBM aprovechan la información relacionada con la seguridad en toda la organización y utilizan inteligencia avanzada para agilizar la detección de amenazas, priorizar los riesgos de forma más eficaz y automatizar las actividades de conformidad.

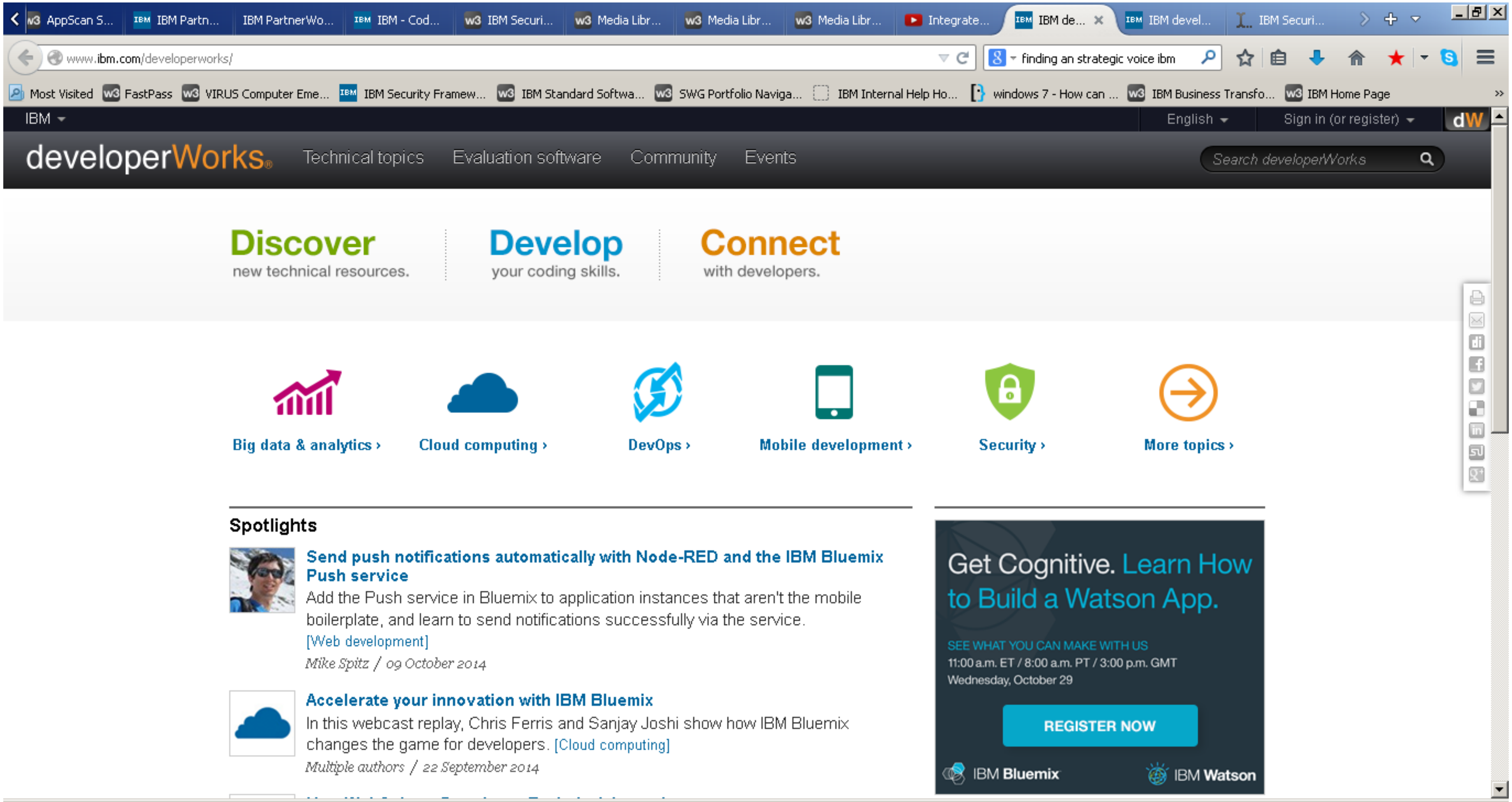
→ **Personas (51)**
Las soluciones de seguridad de IBM permiten a las organizaciones mitigar los riesgos del acceso no autorizado y mantener una estrategia eficaz de gobierno de la gestión de accesos e identidades.

→ **Aplicaciones (4)**
Las soluciones de seguridad de aplicación de IBM le permiten distribuir y mantener aplicaciones web y móviles seguras gracias a la creación de varias capas de protección a lo largo de todas las fases del ciclo de vida de desarrollo y operaciones.

→ **Infraestructura (1)**
Las soluciones de protección de la infraestructura de IBM proporcionan una sólida seguridad en toda la red, los servidores, los servidores virtuales, los sistemas principales y los puntos finales.

→ **Ver todas las soluciones de Ready for IBM Security Intelligence (85)**

DeveloperWorks



Discover new technical resources.

Develop your coding skills.

Connect with developers.

Spotlights

Send push notifications automatically with Node-RED and the IBM Bluemix Push service

Add the Push service in Bluemix to application instances that aren't the mobile boilerplate, and learn to send notifications successfully via the service.

[Web development]

Mike Spitz / 09 October 2014

Accelerate your innovation with IBM Bluemix

In this webcast replay, Chris Ferris and Sanjay Joshi show how IBM Bluemix changes the game for developers. [Cloud computing]

Multiple authors / 22 September 2014

Get Cognitive. Learn How to Build a Watson App.

SEE WHAT YOU CAN MAKE WITH US

11:00 a.m. ET / 8:00 a.m. PT / 3:00 p.m. GMT

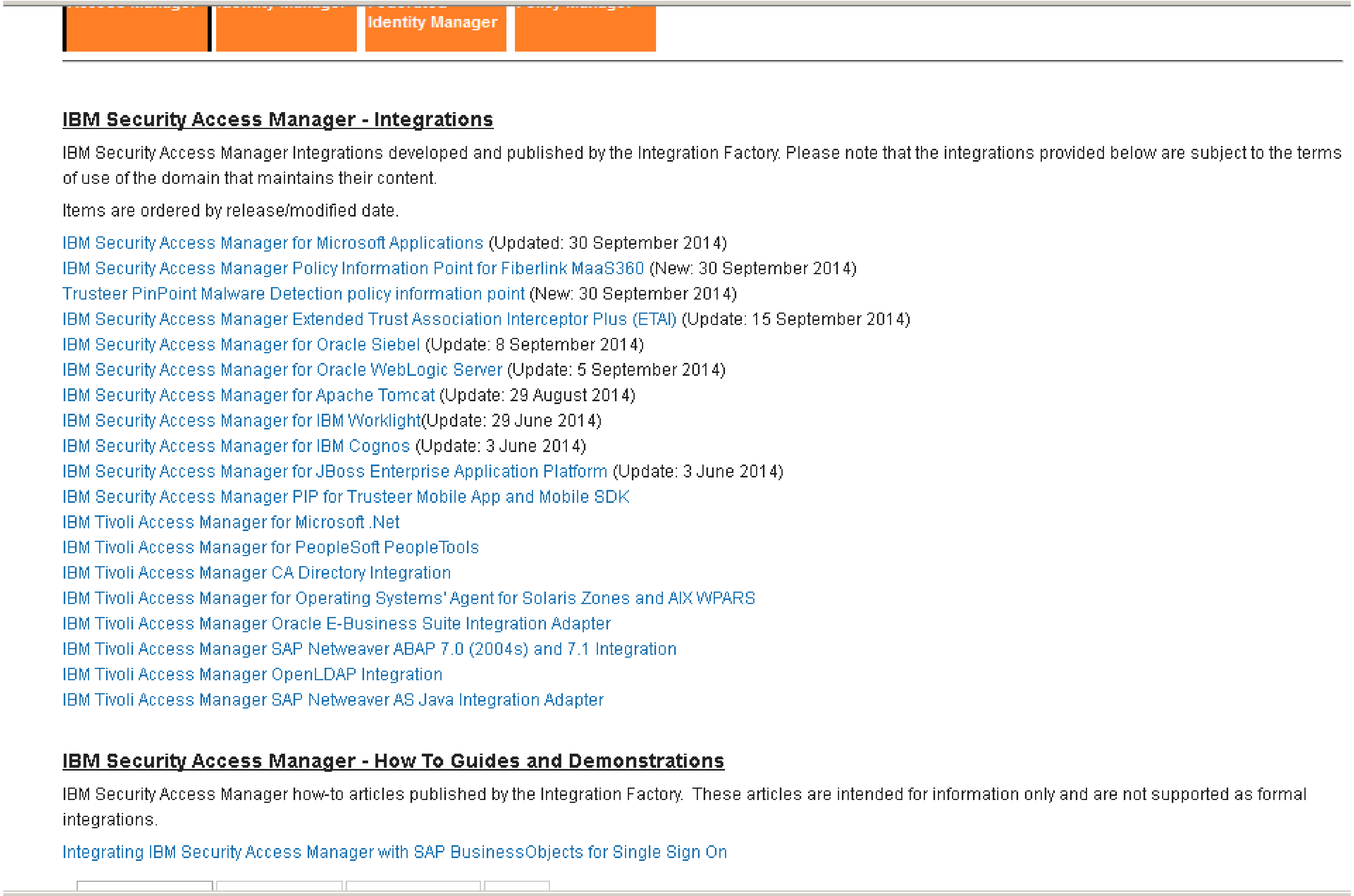
Wednesday, October 29

REGISTER NOW

IBM Bluemix

IBM Watson

Developer Works



IBM Security Access Manager - Integrations

IBM Security Access Manager Integrations developed and published by the Integration Factory. Please note that the integrations provided below are subject to the terms of use of the domain that maintains their content.

Items are ordered by release/modified date.

IBM Security Access Manager for Microsoft Applications (Updated: 30 September 2014)
IBM Security Access Manager Policy Information Point for Fiberlink MaaS360 (New: 30 September 2014)
Trusteer PinPoint Malware Detection policy information point (New: 30 September 2014)
IBM Security Access Manager Extended Trust Association Interceptor Plus (ETAI) (Update: 15 September 2014)
IBM Security Access Manager for Oracle Siebel (Update: 8 September 2014)
IBM Security Access Manager for Oracle WebLogic Server (Update: 5 September 2014)
IBM Security Access Manager for Apache Tomcat (Update: 29 August 2014)
IBM Security Access Manager for IBM Worklight(Update: 29 June 2014)
IBM Security Access Manager for IBM Cognos (Update: 3 June 2014)
IBM Security Access Manager for JBoss Enterprise Application Platform (Update: 3 June 2014)
IBM Security Access Manager PIP for Trusteer Mobile App and Mobile SDK
IBM Tivoli Access Manager for Microsoft .Net
IBM Tivoli Access Manager for PeopleSoft PeopleTools
IBM Tivoli Access Manager CA Directory Integration
IBM Tivoli Access Manager for Operating Systems' Agent for Solaris Zones and AIX WPARS
IBM Tivoli Access Manager Oracle E-Business Suite Integration Adapter
IBM Tivoli Access Manager SAP Netweaver ABAP 7.0 (2004s) and 7.1 Integration
IBM Tivoli Access Manager OpenLDAP Integration
IBM Tivoli Access Manager SAP Netweaver AS Java Integration Adapter

IBM Security Access Manager - How To Guides and Demonstrations

IBM Security Access Manager how-to articles published by the Integration Factory. These articles are intended for information only and are not supported as formal integrations.

Integrating IBM Security Access Manager with SAP BusinessObjects for Single Sign On

Integration Highlight (Multiple Controls): IBM Threat Protection System

1 Smarter Prevention

Trusteer Apex Endpoint Malware Protection

NEW *Java Lockdown Protection - granular control of untrusted code, cloud-based file inspection, and QRadar integration*

IBM Security Network Protection XGS

NEW *Advanced Threat Quarantine integration from QRadar and third-party products, inclusion of Trusteer intelligence into XGS*

2 Security Intelligence

IBM Security QRadar Security Intelligence

NEW *Data Node appliance, new flow and event APIs, and QRadar Vulnerability Manager scanning improvements*

Continuous Response 3

IBM Security QRadar Incident Forensics

NEW *Integrated forensics module with full packet search and visual reconstruction of relationships*

IBM Emergency Response Services

NEW *Increased global coverage and expertise related to malware analysis and forensics*

Global Threat Intelligence 4

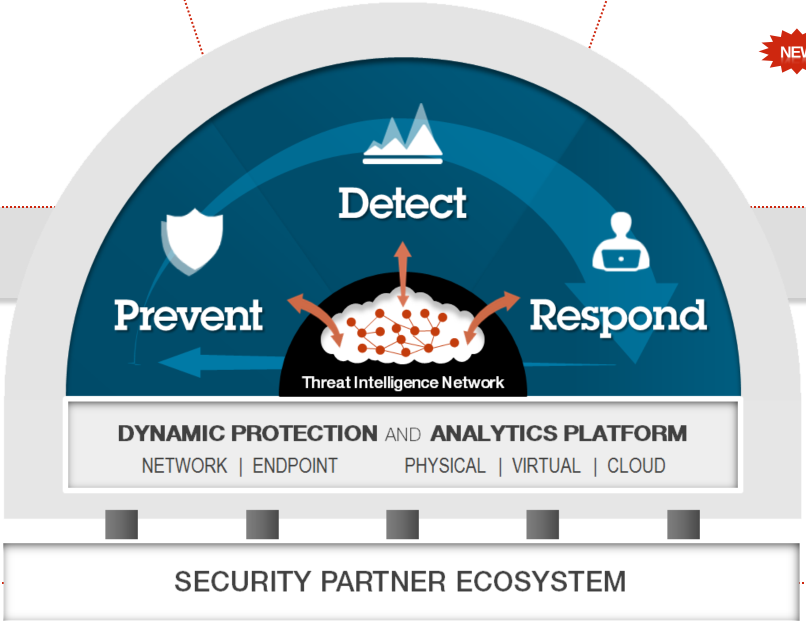
IBM X-Force Threat Intelligence

NEW *New real-time sharing of Trusteer threat intelligence from 100M+ endpoints with X-Force*

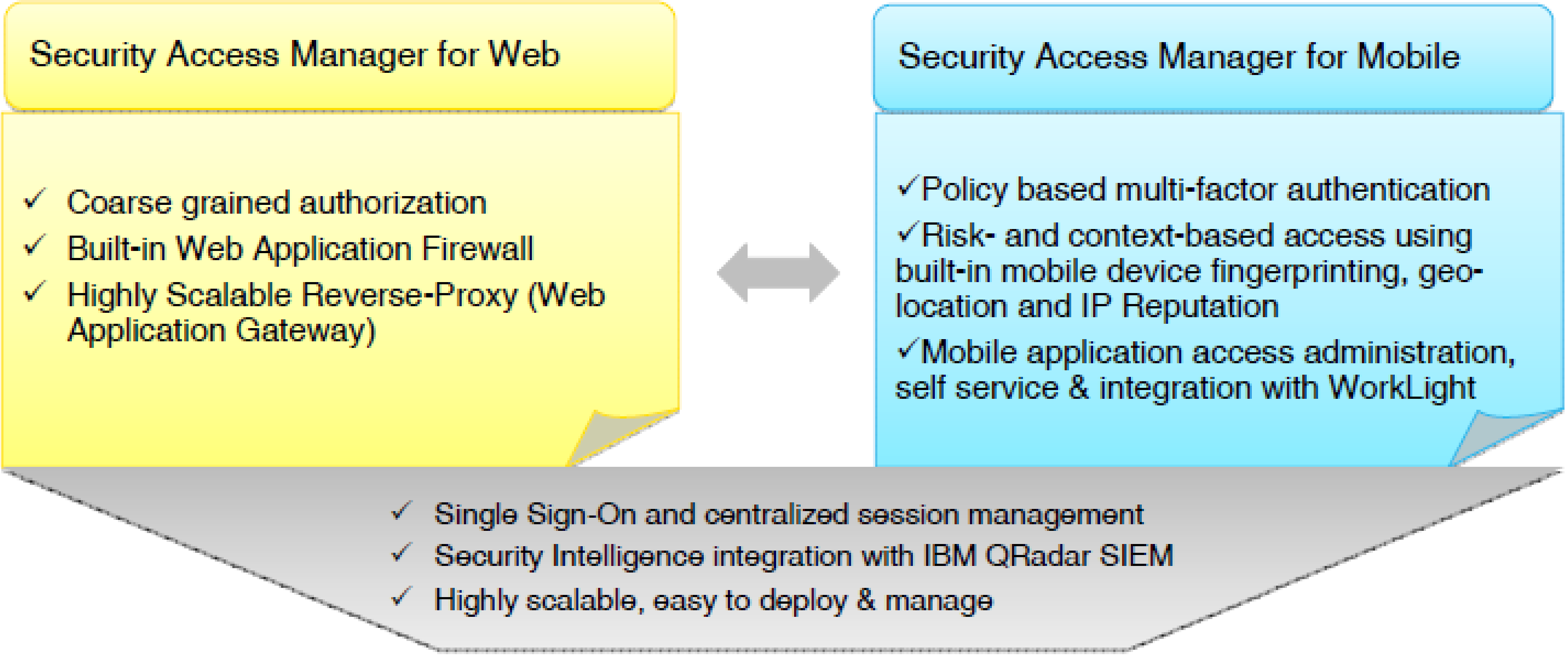
5 Open Integrations

Ready for IBM Security Intelligence Ecosystem

NEW *New functionality from partners including FireEye, TrendMicro, Damballa and other protection vendors*


Detect
Prevent
Respond
Threat Intelligence Network
DYNAMIC PROTECTION AND ANALYTICS PLATFORM
NETWORK | ENDPOINT
PHYSICAL | VIRTUAL | CLOUD
SECURITY PARTNER ECOSYSTEM

Integration Highlight (Multiple Controls): IBM Security Access Manager for Mobile



Security Access Manager for Web

- ✓ Coarse grained authorization
- ✓ Built-in Web Application Firewall
- ✓ Highly Scalable Reverse-Proxy (Web Application Gateway)

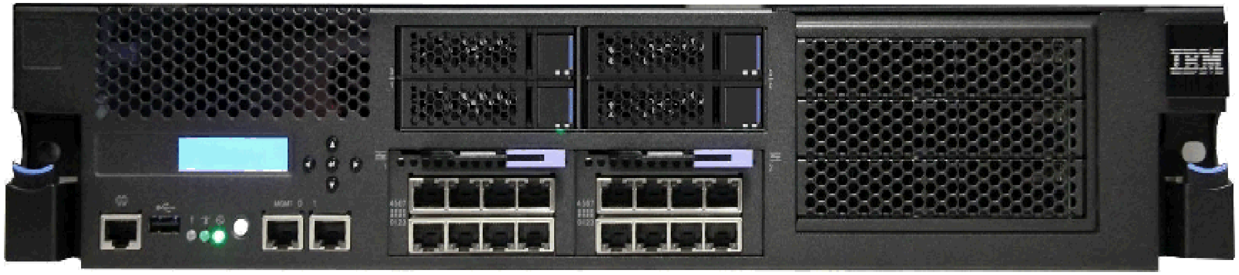
Security Access Manager for Mobile

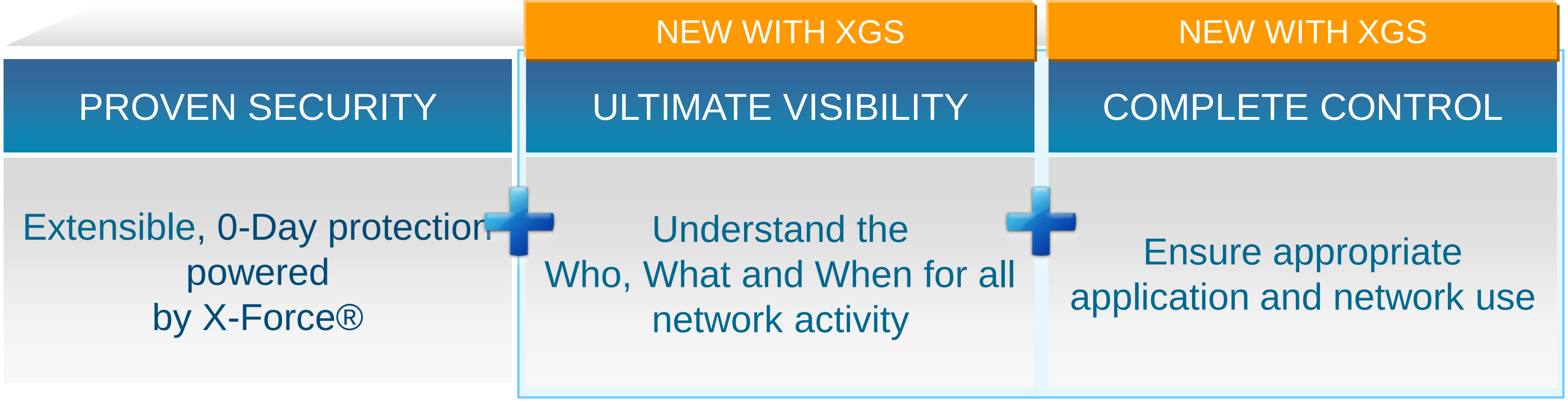
- ✓Policy based multi-factor authentication
- ✓Risk- and context-based access using built-in mobile device fingerprinting, geo-location and IP Reputation
- ✓Mobile application access administration, self service & integration with WorkLight

- ✓ Single Sign-On and centralized session management
- ✓ Security Intelligence integration with IBM QRadar SIEM
- ✓ Highly scalable, easy to deploy & manage

Available in virtual or hardware form factors

Integration Highlight (Intra-Control): XGS





NEW WITH XGS

NEW WITH XGS

PROVEN SECURITY

Extensible, 0-Day protection powered by X-Force®

ULTIMATE VISIBILITY

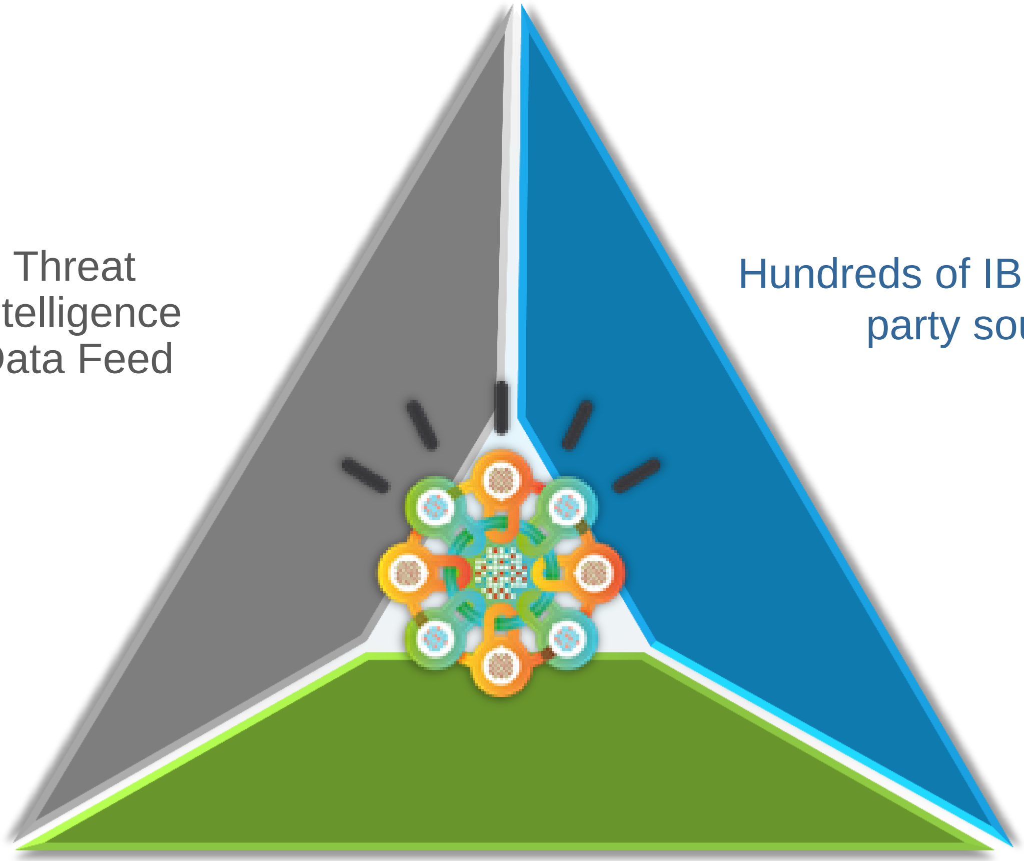
Understand the Who, What and When for all network activity

COMPLETE CONTROL

Ensure appropriate application and network use

IBM Security Network Protection XGS 5000
builds on the proven security of IBM intrusion prevention solutions
by delivering the addition of next generation visibility and control
to help balance security and business requirements

Integration Highlight (Security Intelligence):



Threat Intelligence Data Feed

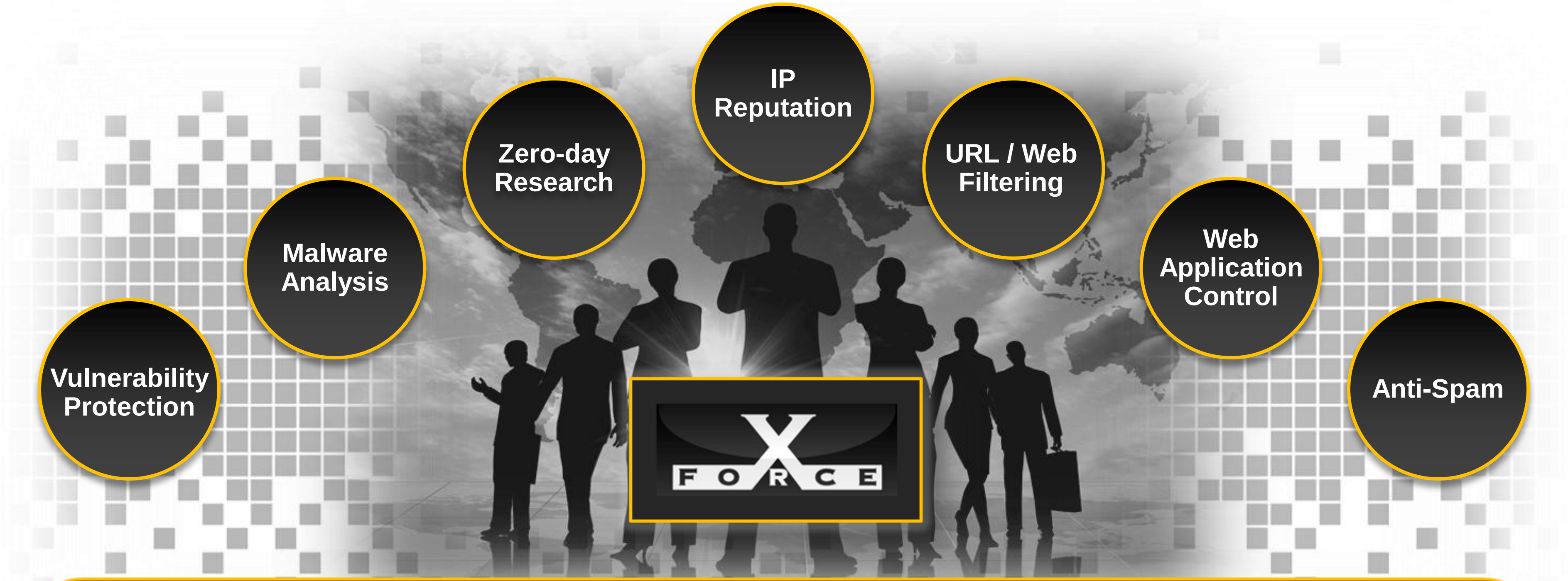
Hundreds of IBM and third-party sources

Security Intelligence Platform

Security Intelligence, Threat Intelligence and **Advanced Threat Protection** Integration is core to the IBM Security market value

IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape



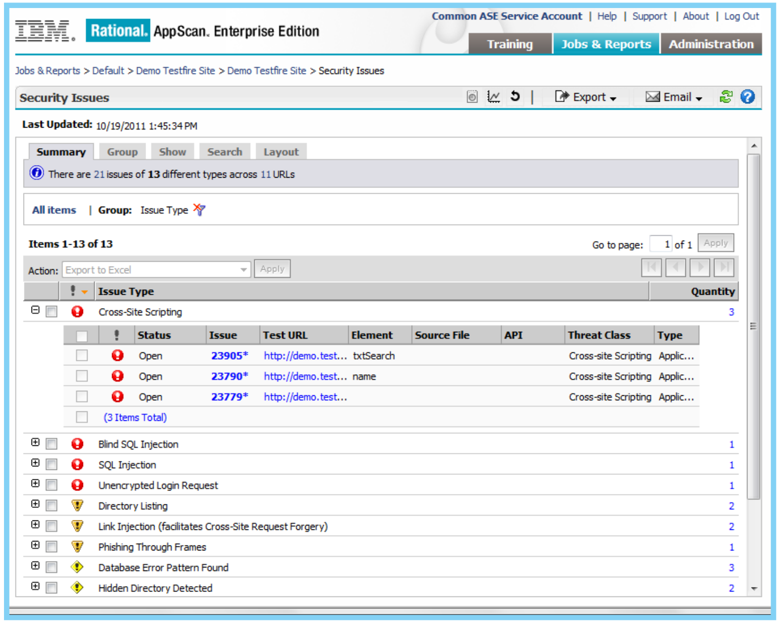
The IBM X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow’s security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

Identify and mitigate Web application security risk

Check your applications for security vulnerabilities with AppScan

- ✓ **Security analyst performs automated security assessments of new or already deployed Web applications**
- ✓ **Security analyst reviews findings and identifies vulnerabilities**
- ✓ **Application development team are notified about security vulnerabilities**


IBM. Rational. AppScan. Enterprise Edition
Common ASE Service Account | Help | Support | About | Log Out
Training
Jobs & Reports
Administration
Jobs & Reports > Default > Demo Testfire Site > Demo Testfire Site > Security Issues
Security Issues
Export
Email
Summary
Group
Show
Search
Layout
All items | Group: Issue Type
Go to page: 1 of 1 Apply
Action: Export to Excel Apply

Last Updated: 10/19/2011 1:45:34 PM

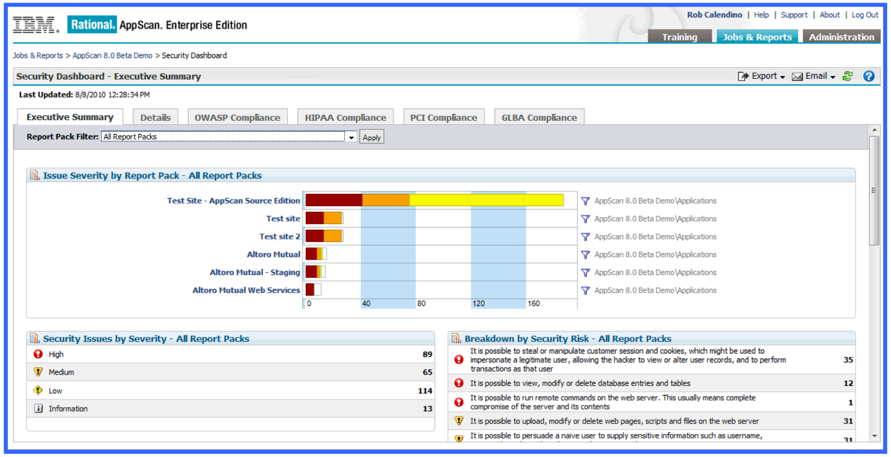
There are 21 issues of 13 different types across 11 URLs

Items 1-13 of 13

!	Issue Type	Quantity
❗	Cross-Site Scripting	3
❗	Blind SQL Injection	1
❗	SQL Injection	1
❗	Unencrypted Login Request	1
⚠	Directory Listing	2
⚠	Link Injection (facilitates Cross-Site Request Forgery)	2
⚠	Phishing Through Frames	1
◆	Database Error Pattern Found	3
◆	Hidden Directory Detected	2

Cross-Site Scripting:

☐	!	Status	Issue	Test URL	Element	Source File	API	Threat Class	Type
☐	❗	Open	23905*	http://demo.test…	txtSearch			Cross-site Scripting	Applic…
☐	❗	Open	23790*	http://demo.test…	name			Cross-site Scripting	Applic…
☐	❗	Open	23779*	http://demo.test…				Cross-site Scripting	Applic…
☐	(3 Items Total)								


IBM. Rational. AppScan. Enterprise Edition
Rob Calendino | Help | Support | About | Log Out
Training
Jobs & Reports
Administration
Jobs & Reports > AppScan 8.0 Beta Demo > Security Dashboard
Security Dashboard - Executive Summary
Export
Email
Executive Summary
Details
OWASP Compliance
HIPAA Compliance
PCI Compliance
GLBA Compliance
Report Pack Filter: All Report Packs Apply
Issue Severity by Report Pack - All Report Packs
Test Site - AppScan Source Edition
Test site
Test site 2
Altoro Mutual
Altoro Mutual - Staging
Altoro Mutual Web Services
0
40
80
120
160
AppScan 8.0 Beta Demo\Applications
AppScan 8.0 Beta Demo\Applications
AppScan 8.0 Beta Demo\Applications
AppScan 8.0 Beta Demo\Applications
AppScan 8.0 Beta Demo\Applications
AppScan 8.0 Beta Demo\Applications

Last Updated: 8/8/2010 12:28:34 PM

Security Issues by Severity - All Report Packs

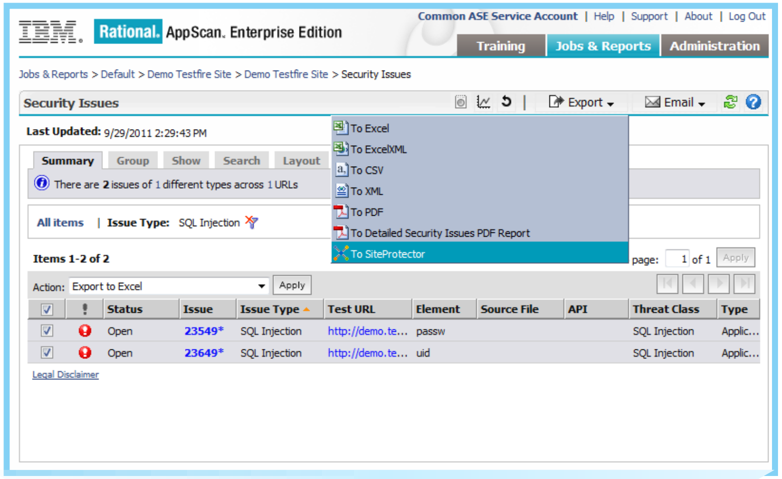
❗	High	89
⚠	Medium	65
◆	Low	114
ℹ	Information	13

Breakdown by Security Risk - All Report Packs

❗	It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user	35
❗	It is possible to view, modify or delete database entries and tables	12
❗	It is possible to run remote commands on the web server. This usually means complete compromise of the server and its contents	1
⚠	It is possible to upload, modify or delete web pages, scripts and files on the web server	31
⚠	It is possible to persuade a naive user to supply sensitive information such as username,	31

Publish security vulnerabilities information to SiteProtector

- ✓ **Security analyst publishes application security vulnerabilities information to SiteProtector**
- ✓ **Vulnerable application assets are identified and made visible**
- ✓ **Network analyst is notified**



Jobs & Reports > Default > Demo Testfire Site > Demo Testfire Site > Security Issues

Security Issues

Last Updated: 9/29/2011 2:29:43 PM

There are **2** issues of 1 different types across 1 URLs

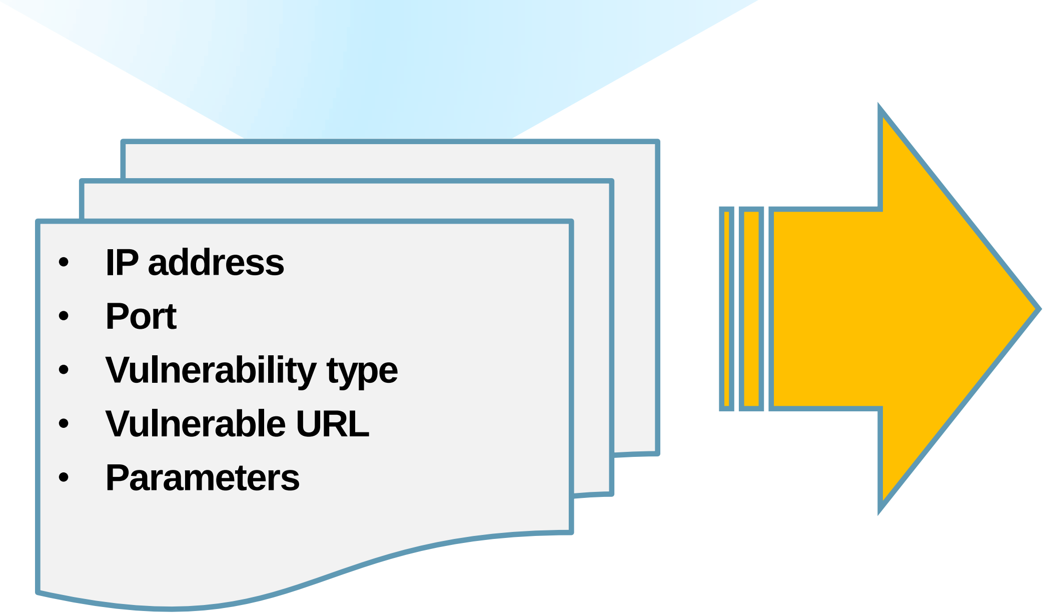
All items | **Issue Type:** SQL Injection

Items 1-2 of 2

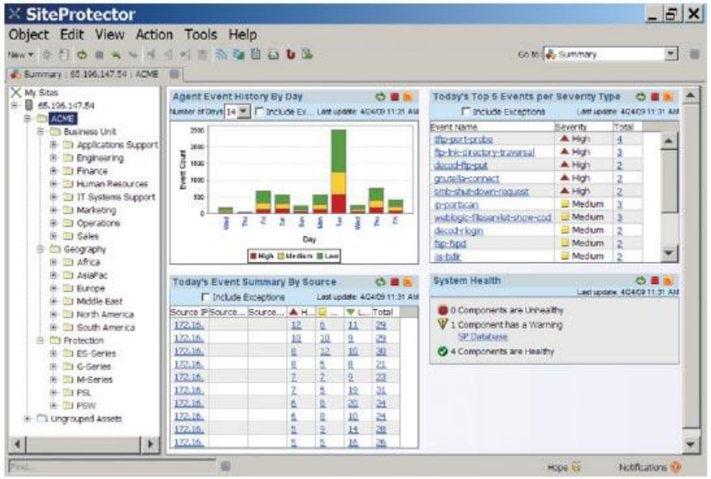
page: 1 of 1

Action: Export to Excel

☑	!	Status	Issue	Issue Type	Test URL	Element	Source File	API	Threat Class	Type
☑	●	Open	23549*	SQL Injection	http://demo.te...	passw			SQL Injection	Applic...
☑	●	Open	23649*	SQL Injection	http://demo.te...	uid			SQL Injection	Applic...



- **IP address**
- **Port**
- **Vulnerability type**
- **Vulnerable URL**
- **Parameters**

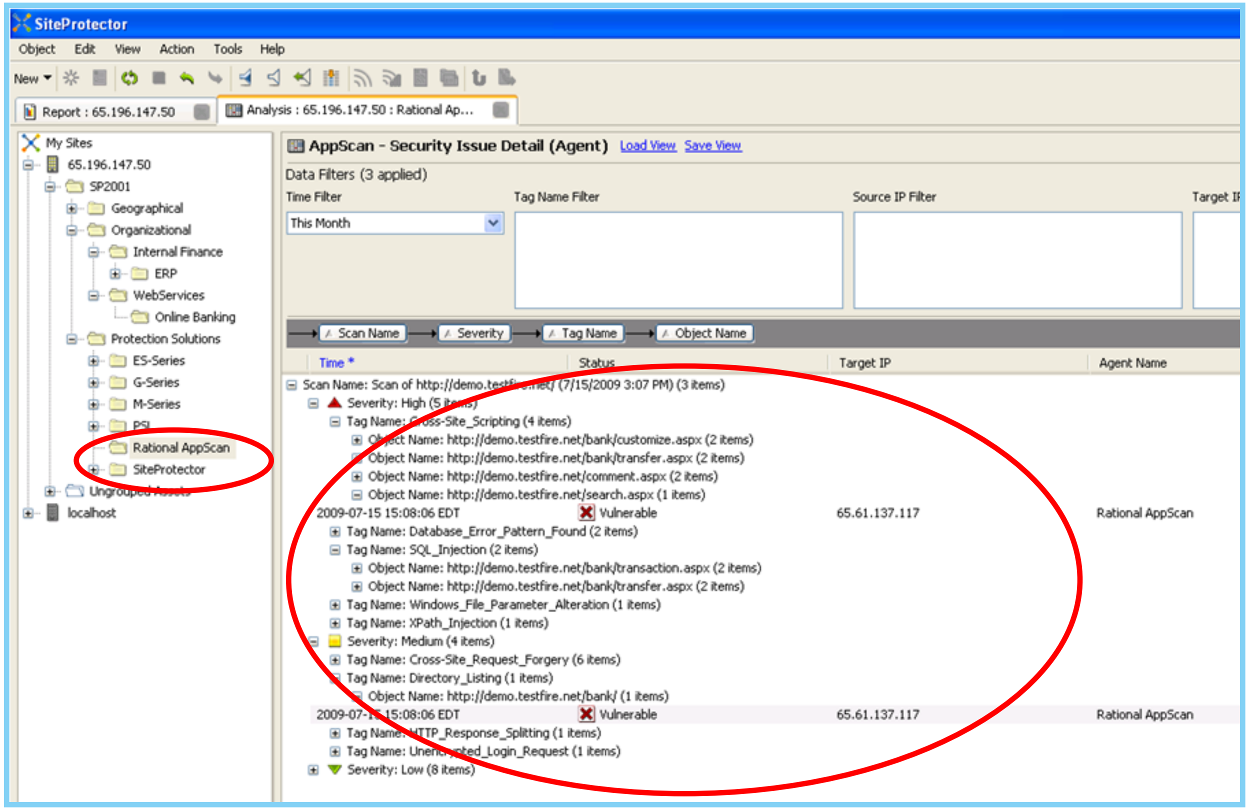


Event Name	Severity	Total
ftp-port-probe	High	4
ftp-link-directory-traversal	High	3
decod-ftp-put	High	2
gnutella-connect	High	2
smb-shut-down-request	High	2
ip-portscan	Medium	3
weblogic-fileservlet-show-cod	Medium	3
decod-rlogin	Medium	2
ftp-ftpd	Medium	2
ia-bdir	Medium	2

Source IP	Source...	Source...	H...	...	L...	Total
172.16.			12	6	11	29
172.16.			10	10	9	29
172.16.			8	12	10	30
172.16.			8	5	8	21
172.16.			7	7	9	23
172.16.			7	5	19	31
172.16.			6	8	20	34
172.16.			6	8	10	24
172.16.			5	9	14	28
172.16.			5	5	16	26

0 Components are Unhealthy
1 Component has a Warning
SP Database
4 Components are Healthy

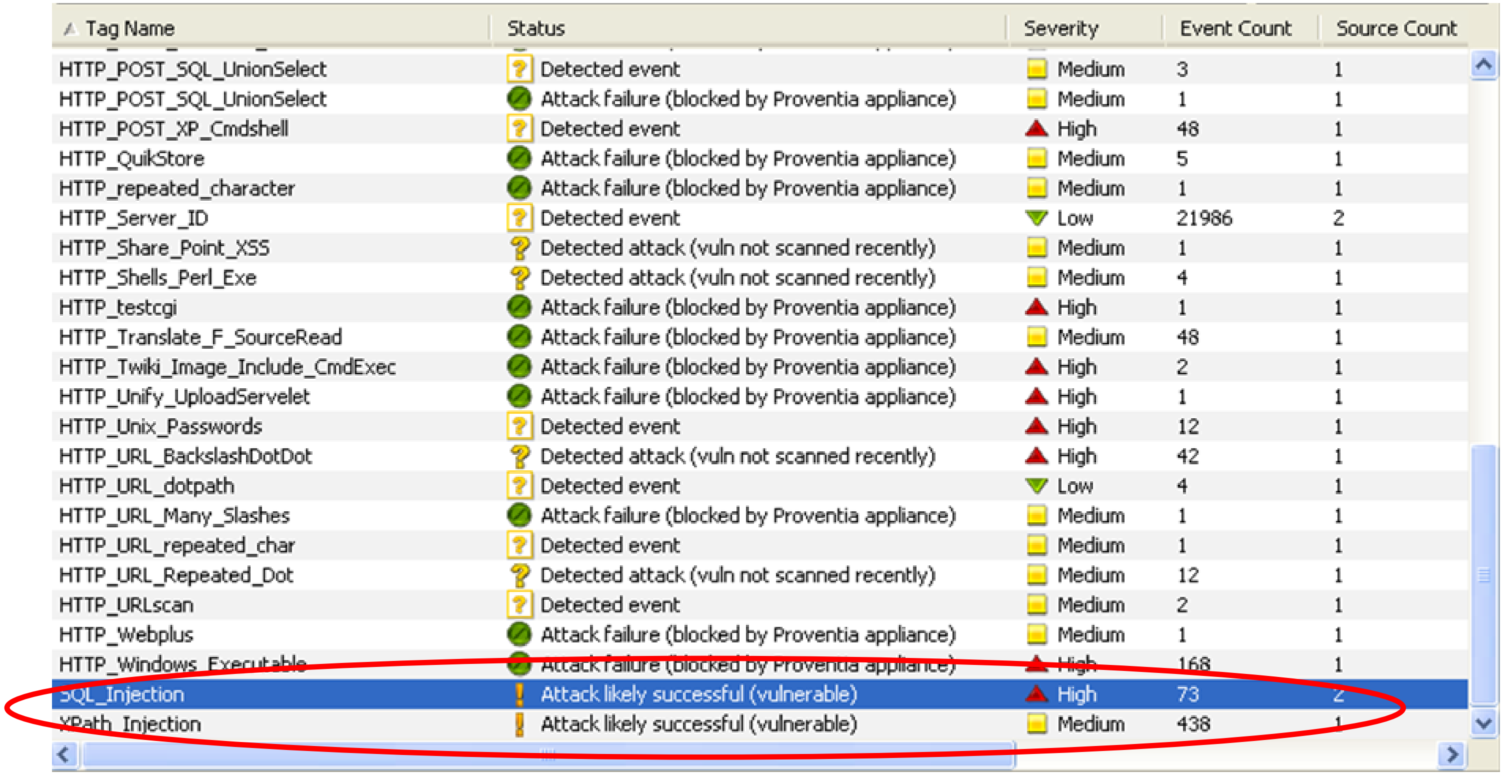
SiteProtector displays application security vulnerabilities



```
Time *                      Status        Target IP         Agent Name
Scan Name: Scan of http://demo.testfire.net/ (7/15/2009 3:07 PM) (3 items)
  Severity: High (5 items)
    Tag Name: Cross-Site_Scripting (4 items)
      Object Name: http://demo.testfire.net/bank/customize.aspx (2 items)
      Object Name: http://demo.testfire.net/bank/transfer.aspx (2 items)
      Object Name: http://demo.testfire.net/comment.aspx (2 items)
      Object Name: http://demo.testfire.net/search.aspx (1 items)
  2009-07-15 15:08:06 EDT   Vulnerable    65.61.137.117     Rational AppScan
    Tag Name: Database_Error_Pattern_Found (2 items)
    Tag Name: SQL_Injection (2 items)
      Object Name: http://demo.testfire.net/bank/transaction.aspx (2 items)
      Object Name: http://demo.testfire.net/bank/transfer.aspx (2 items)
    Tag Name: Windows_File_Parameter_Alteration (1 items)
    Tag Name: XPath_Injection (1 items)
  Severity: Medium (4 items)
    Tag Name: Cross-Site_Request_Forgery (6 items)
    Tag Name: Directory_Listing (1 items)
      Object Name: http://demo.testfire.net/bank/ (1 items)
  2009-07-15 15:08:06 EDT   Vulnerable    65.61.137.117     Rational AppScan
    Tag Name: HTTP_Response_Splitting (1 items)
    Tag Name: Unencrypted_Login_Request (1 items)
  Severity: Low (8 items)
```

- ✓ **Network analyst reviews application security vulnerabilities**
- ✓ **Network analyst monitors vulnerable application assets**

SiteProtector SecurityFusion™ module provides security intelligence



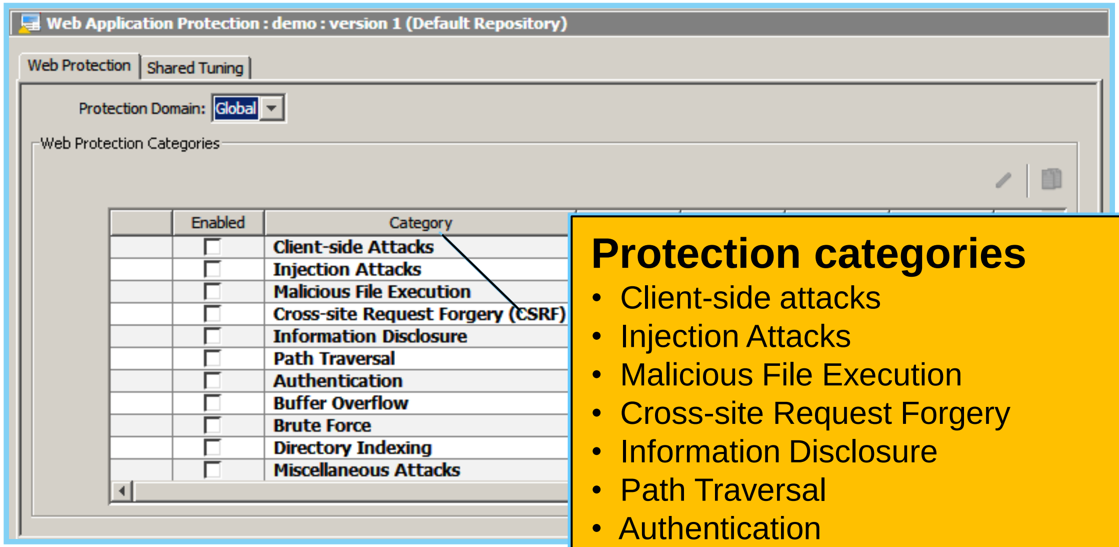
Tag Name	Status	Severity	Event Count	Source Count
HTTP_POST_SQL_UnionSelect	Detected event	Medium	3	1
HTTP_POST_SQL_UnionSelect	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_POST_XP_Cmdshell	Detected event	High	48	1
HTTP_QuikStore	Attack failure (blocked by Proventia appliance)	Medium	5	1
HTTP_repeated_character	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_Server_ID	Detected event	Low	21986	2
HTTP_Share_Point_XSS	Detected attack (vuln not scanned recently)	Medium	1	1
HTTP_Shells_Perl_Exe	Detected attack (vuln not scanned recently)	Medium	4	1
HTTP_testcgi	Attack failure (blocked by Proventia appliance)	High	1	1
HTTP_Translate_F_SourceRead	Attack failure (blocked by Proventia appliance)	Medium	48	1
HTTP_Twiki_Image_Include_CmdExec	Attack failure (blocked by Proventia appliance)	High	2	1
HTTP_Unify_UploadServelet	Attack failure (blocked by Proventia appliance)	High	1	1
HTTP_Unix_Passwords	Detected event	High	12	1
HTTP_URL_BackslashDotDot	Detected attack (vuln not scanned recently)	High	42	1
HTTP_URL_dotpath	Detected event	Low	4	1
HTTP_URL_Many_Slashes	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_URL_repeated_char	Detected event	Medium	1	1
HTTP_URL_Repeated_Dot	Detected attack (vuln not scanned recently)	Medium	12	1
HTTP_URLscan	Detected event	Medium	2	1
HTTP_Webplus	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_Windows_Executable	Attack failure (blocked by Proventia appliance)	High	168	1
SQL_Injection	Attack likely successful (vulnerable)	High	73	2
XPath_Injection	Attack likely successful (vulnerable)	Medium	438	1

!

- ✓ IDS/IPS real-time malicious HTTP traffic is correlated with vulnerable application assets
- ✓ SiteProtector alerts network analyst when attacks are likely to succeed
- ✓ Network analyst takes action

Until application fix is available, mitigate risk with IBM Security IPS

- ✓ **Network analyst creates a virtual patch by turning on IBM Security IPS Web application protection policy**
- ✓ **Network analyst enables protection categories in the policy based on the types of discovered vulnerabilities with AppScan**



Web Application Protection : demo : version 1 (Default Repository)

Protection Domain: Global

Web Protection Categories

	Enabled	Category
	□	Client-side Attacks
	□	Injection Attacks
	□	Malicious File Execution
	□	Cross-site Request Forgery (CSRF)
	□	Information Disclosure
	□	Path Traversal
	□	Authentication
	□	Buffer Overflow
	□	Brute Force
	□	Directory Indexing
	□	Miscellaneous Attacks

Protection categories

- Client-side attacks
- Injection Attacks
- Malicious File Execution
- Cross-site Request Forgery
- Information Disclosure
- Path Traversal
- Authentication
- Buffer Overflow
- Brute Force
- Directory Indexing
- Miscellaneous Attacks

Summary of benefits

- ✓ **Quickly identify application vulnerabilities with AppScan**
- ✓ **Raise visibility of security risk by publishing vulnerabilities information to IBM Security SiteProtector**
- ✓ **Monitor vulnerable application assets and raise threat alerts using the SiteProtector SecurityFusion™ module**
- ✓ **Take action for mitigating risk by configuring virtual patches with IBM Security IPS until application security updates are available**

IBM Security Access Manager integration with Trusteer Secure Mobile Browser

Scenario Walkthrough

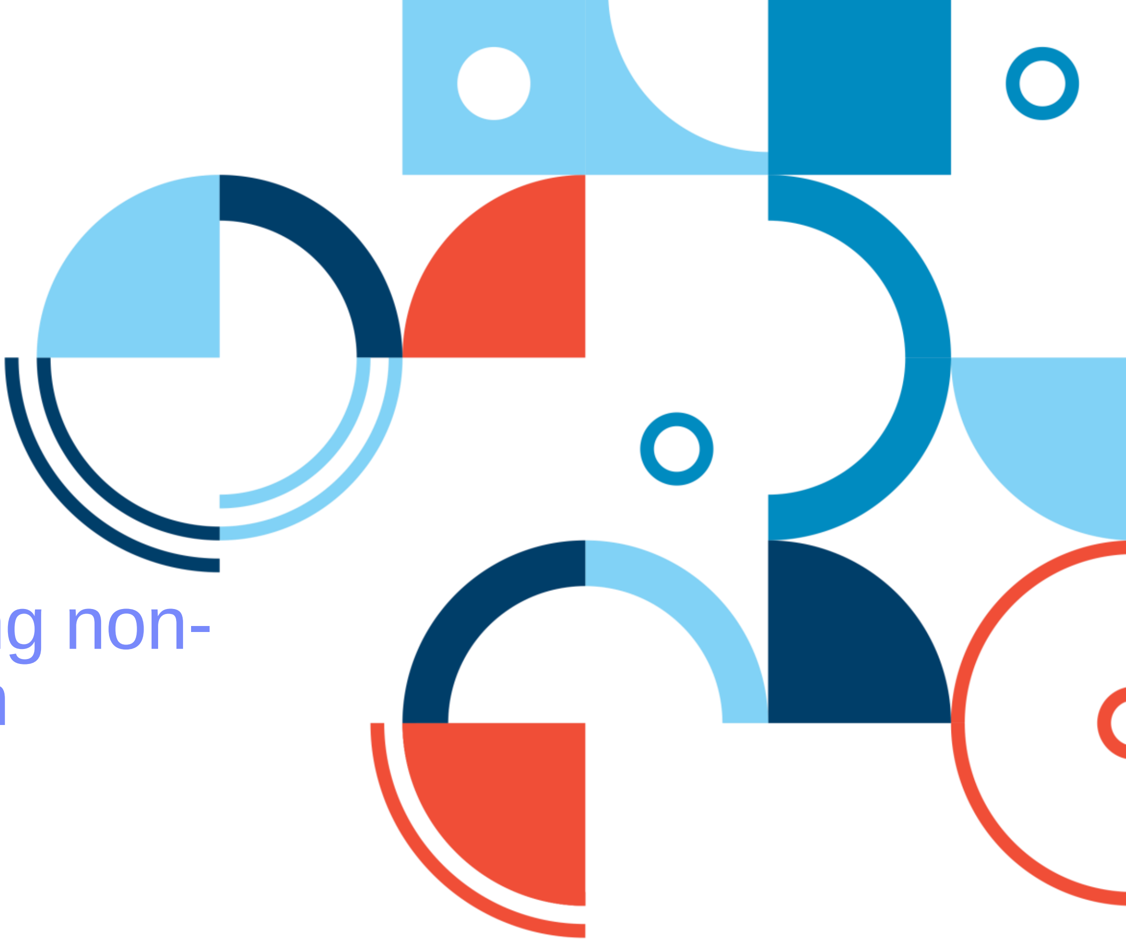
IBM Security Access Manager PIP for Trusteer Mobile App and Mobile SDK downloadable files

Pulse2014
The Premier Cloud Conference

February 23 – 26
MGM Grand – Las Vegas, Nevada

Scenarios

- Scenario 1:
  - Preventing non-secure browsers from connecting
- Scenario 2:
  - Mobile Malware & high-risk device detection and enforcement



Scenario 1: Preventing non-secure browsers from connecting

Pulse2014

The Premier Cloud Conference

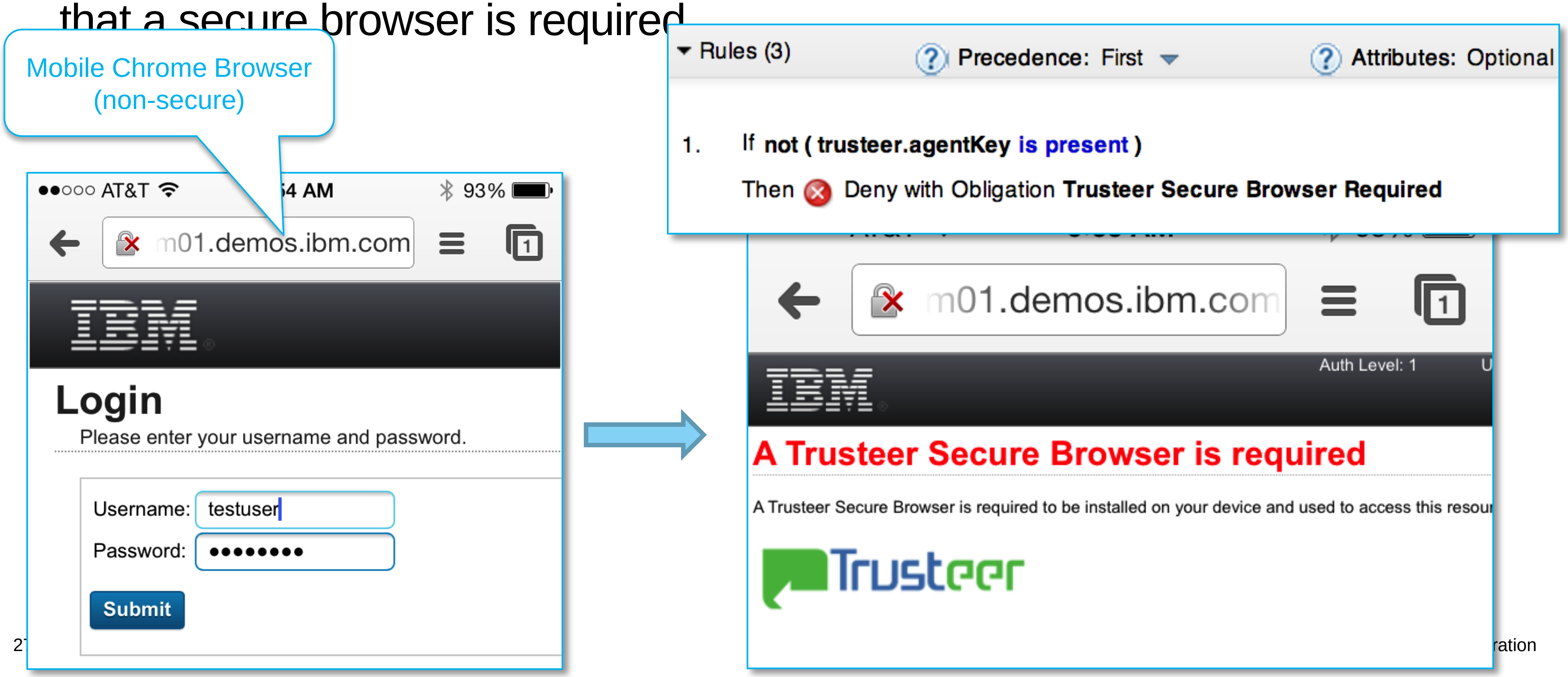
February 23 – 26

MGM Grand – Las Vegas, Nevada

Scenario 1: Preventing non-secure browsers from connecting

- **Value**:
  - Decreasing the risk of malware, customize user experience & no application changes required.

- Simple policy can be authored that directs users to a page notifying them that a secure browser is required



Mobile Chrome Browser (non-secure)

Login

Please enter your username and password.

Username: testuser

Password: ●●●●●●●●

1. If not (trusteer.agentKey is present)
   Then Deny with Obligation **Trusteer Secure Browser Required**

A Trusteer Secure Browser is required

A Trusteer Secure Browser is required to be installed on your device and used to access this resou

Scenario 2: Mobile malware & high-risk device detection and enforcement

Pulse2014

The Premier Cloud Conference

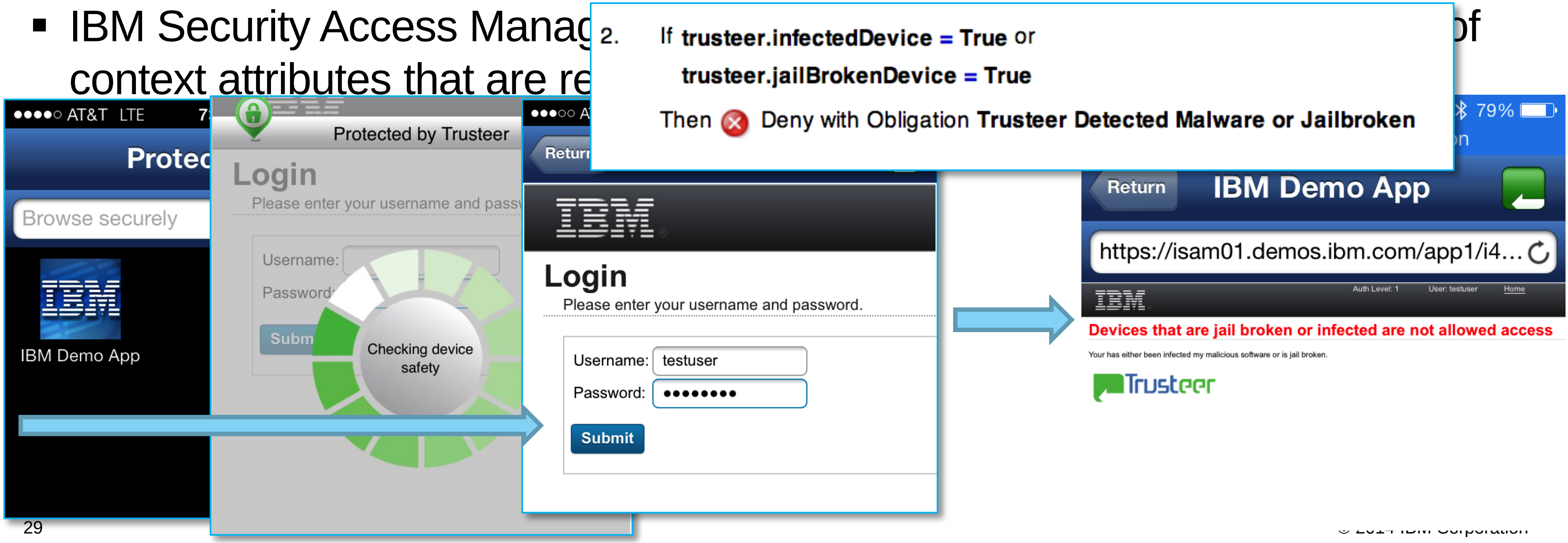
February 23 – 26

MGM Grand – Las Vegas, Nevada

Scenario 2: Mobile malware & high-risk detection and enforcement

- **Value**:
  - Reduce the risk of malware collecting sensitive data.

- The Trusteer Secure Browser when connecting with registered web applications will transmit in the HTTP request details about the connecting mobile device.
- IBM Security Access Manag of context attributes that are re



2. If **trusteer.infectedDevice = True** or **trusteer.jailBrokenDevice = True**
Then ⊗ Deny with Obligation **Trusteer Detected Malware or Jailbroken**

●●●●○ AT&T LTE 7
Protec
Browse securely
IBM Demo App

Protected by Trusteer
Login
Please enter your username and pass
Username:
Password
Subm
Checking device safety

●●●○○ A
Return
Login
Please enter your username and password.
Username: testuser
Password: ●●●●●●●●●
Submit

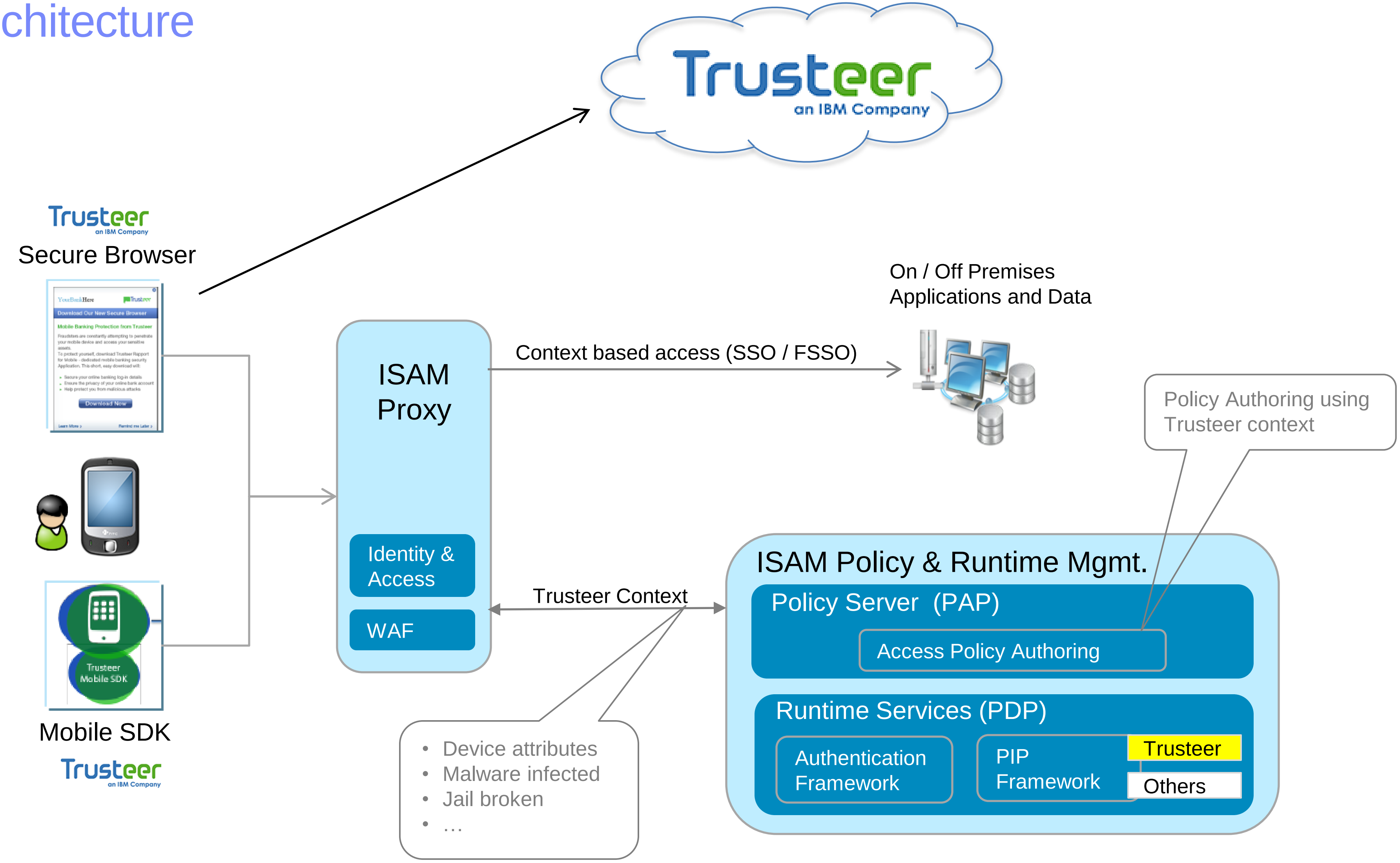
79%
Return
IBM Demo App
https://isam01.demos.ibm.com/app1/i4…
Auth Level: 1
User: testuser
Home
Devices that are jail broken or infected are not allowed access
Your has either been infected my malicious software or is jail broken.
Trusteer

Architecture

Pulse2014
The Premier Cloud Conference

February 23 – 26
MGM Grand – Las Vegas, Nevada

Architecture



YourBankHere Trusteer

Download Our New Secure Browser

Mobile Banking Protection from Trusteer

Fraudsters are constantly attempting to penetrate your mobile device and access your sensitive assets.
To protect yourself, download Trusteer Rapport for Mobile - dedicated mobile banking security Application. This short, easy download will:

- Secure your online banking log-in details
- Ensure the privacy of your online bank account
- Help protect you from malicious attacks

Download Now

Learn More › Remind me Later ›

- Device attributes
- Malware infected
- Jail broken
- …

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security

© Copyright IBM Corporation 2014. THE INFORMATION IN THESE MATERIALS ARE PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided. 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. These materials are current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country 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, ibm.com and other IBM products and services are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Security Talk: zSecure & QRadar Integration

Jamie Pease CISA, CISM, CISSP, MBCS CITP
System z Security Specialist

Robert Kennedy
WW Sales Enablement Lead

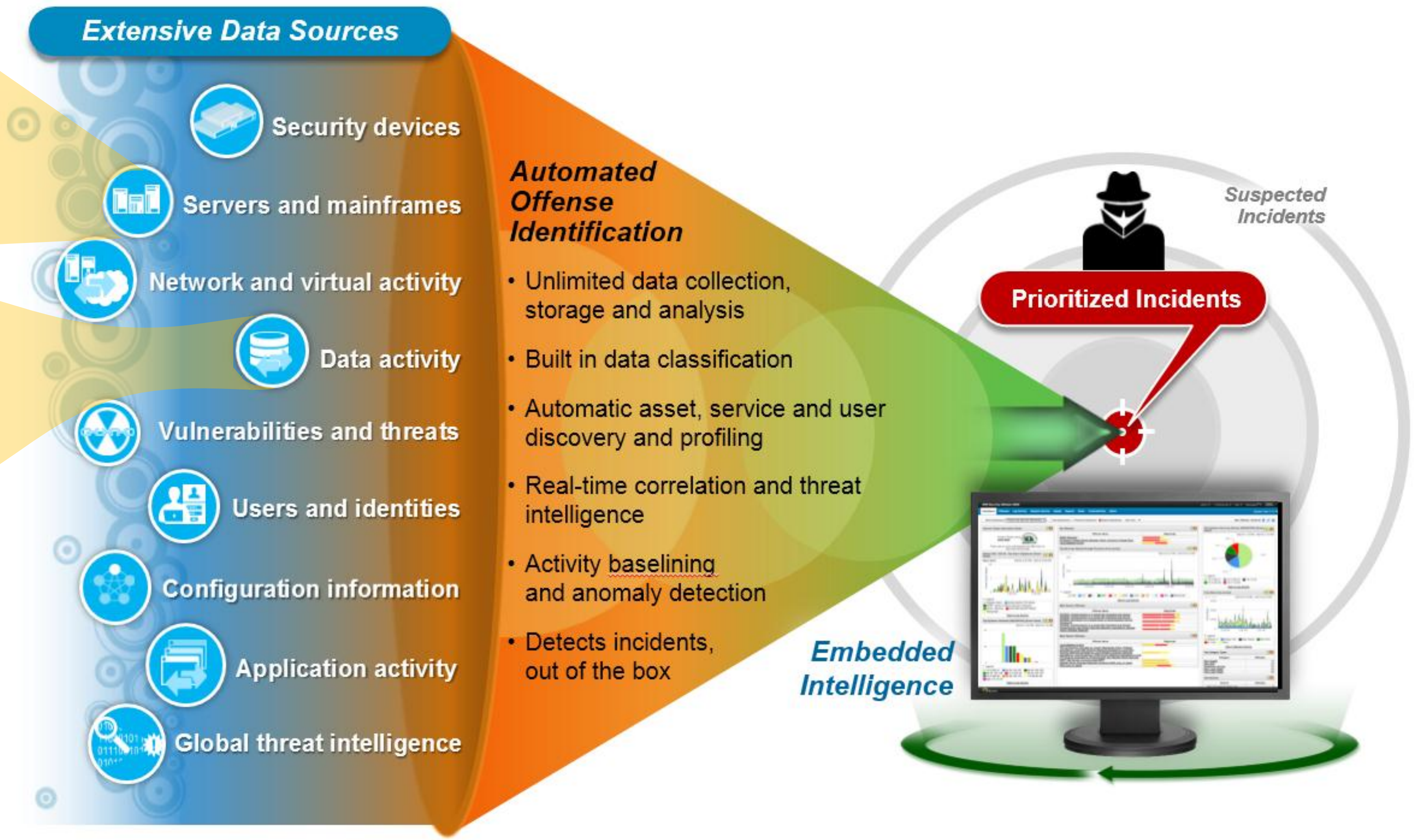
Pulse2014
The Premier Cloud Conference

February 23 – 26
MGM Grand – Las Vegas, Nevada

Security intelligence automated offense identification for System z

zSecure
- z/OS
- RACF
- ACF2, TSS
- CICS

Guardium
- DB2
- IMS
- VSAM



- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents, out of the box

Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

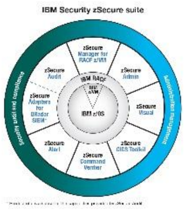
Mainframe QRadar Integration: zSecure vs. legacy integration

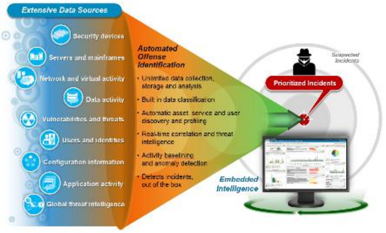
Integration	zSecure (Alert & Audit) integration	Legacy z/OS integration
Real Time Event Capture	Yes, via Alert	No, only historical SMF data
Extended User/Resource Information	Yes	No
Inputs:		
• RACF	Yes	Yes
• ACF2	Yes	Yes
• Top Secret	Yes	Yes
• DB2	Yes	No
• CICS	Yes	No
• z/OS UNIX	Yes	No
• FTP, Telnet	Yes	No
• Dataset Access	Yes	No
• PDS Member updates	Yes	No

- ✓ zSecure provides real time input; Legacy only accesses historical SMF datasets
- ✓ zSecure adds descriptions to events, Legacy provides no descriptions
- ✓ zSecure provides a wide range of input; Legacy only provides RACF records
- ✓ zSecure provides more comprehensive input, improving the quality of the analysis
- ✓ Bottom line: the customer gets what they pay for.

Value of zSecure integration with QRadar

- Plugs a hole in the Enterprise Security Monitoring practice
- Provides a holistic, centralised approach for Security Monitoring
- Supports separation of duties – stop the legacy practice of self-policing!
- Maximise QRadar capabilities for:
  - Log management
  - Anomaly detection
  - Incident forensics
  - Configuration Management
  - Vulnerability Management
  - Risk management

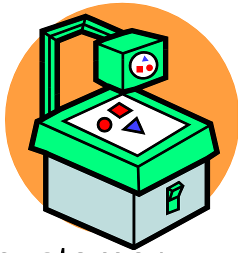

IBM Security zSecure suite
zSecure Manager for RACF z/VM
zSecure Admin
zSecure Visual
zSecure CICS Toolkit
zSecure Command Verifier
zSecure Alert
zSecure Adapters for QRadar SIEM*
zSecure Audit
IBM RACF
IBM z/VM
IBM z/OS
Security audit and compliance
Administration management


Extensive Data Sources
Security devices
Servers and mainframes
Network and virtual activity
Data activity
Vulnerabilities and threats
Users and identities
Configuration information
Application activity
Global threat intelligence
Automated Offense Identification
• Unlimited data collection, storage and analysis
• Built in data classification
• Automatic asset, service and user discovery and profiling
• Real-time correlation and threat intelligence
• Activity baselining and anomaly detection
• Detects incidents, out of the box
Suspected Incidents
Prioritized Incidents
Embedded Intelligence

- Enhances the monitoring experience with graphical displays and user friendly reporting
- Extend best practices and comply with regulatory/legal/compliance requirements

Demoing to customers

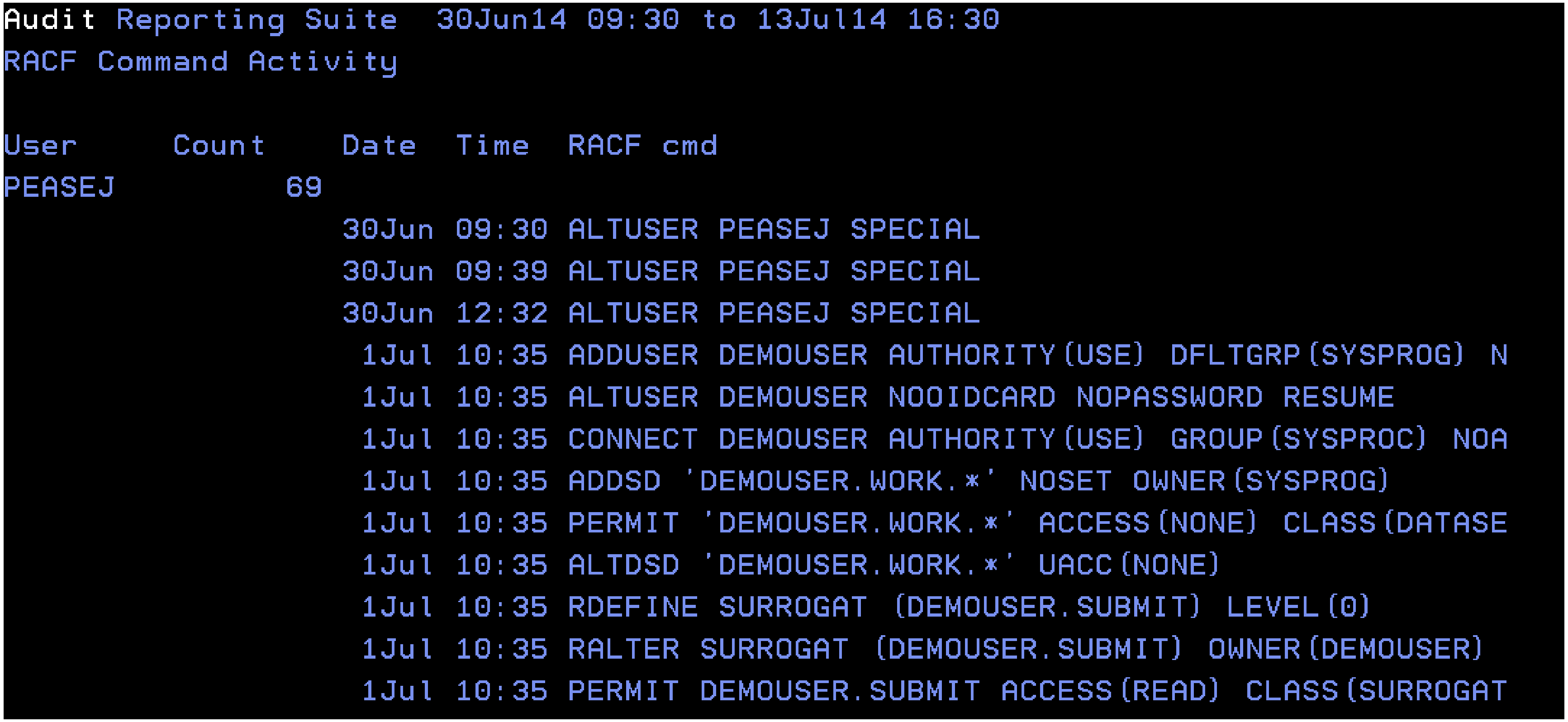
- zSecurity and QRadar Client Technical Professionals (CTPs) have access to a demo cookbook/recording (click here) . . .
  - ➢ Demo environments available . . .
    - ✓ Laptop based (no internet access, faster response, canned)
    - ✓ Live server (internet access, feed live events, highly adaptable)



- Depending on your audience, zSecurity and QRadar CTPs should co-present at customer meetings/workshops . . . For example:-
  - ➢ A QRadar CTP may require support in front of a System z audience
  - ➢ A zSecurity CTP may require a QRadar CTP to be present where detailed SIEM knowledge is required
- 10 minute zSecure/QRadar integration demo recording available from next week
  - – Can be used in customer meetings

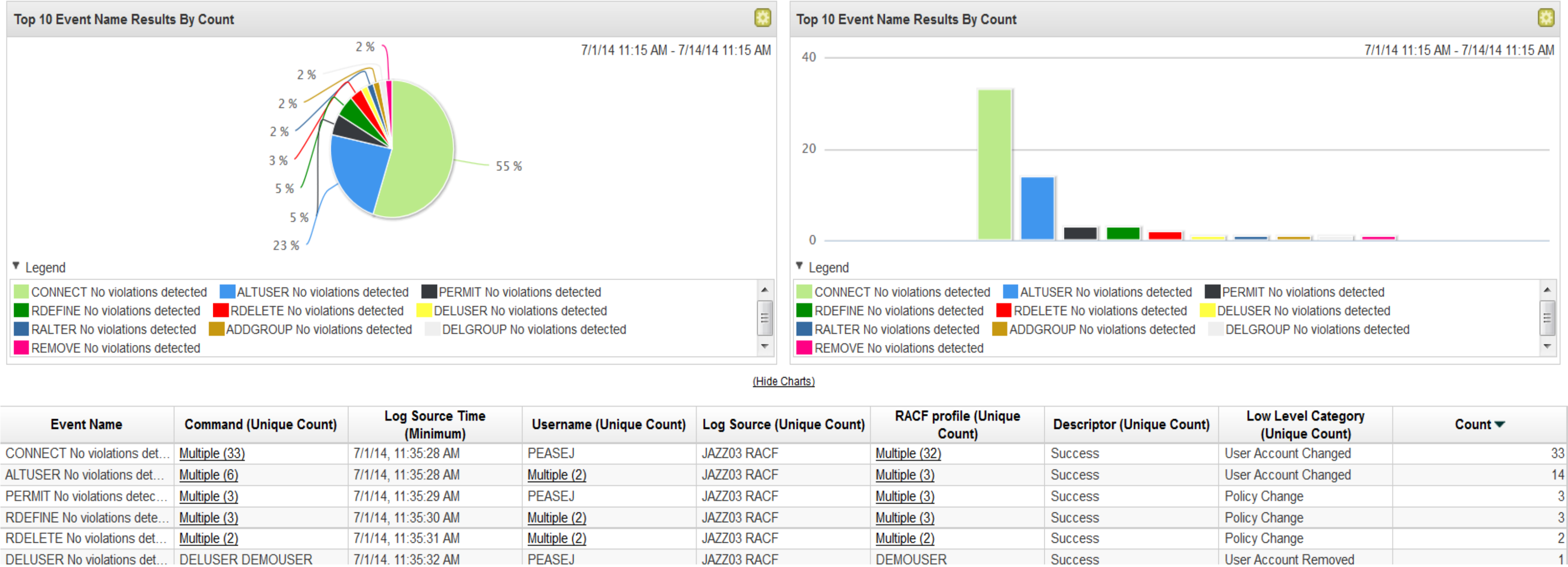
Demo walkthrough

How about if you could transform this . . .



```
Audit Reporting Suite  30Jun14 09:30 to 13Jul14 16:30
RACF Command Activity

User     Count    Date  Time  RACF cmd
PEASEJ         69
                  30Jun 09:30 ALTUSER PEASEJ SPECIAL
                  30Jun 09:39 ALTUSER PEASEJ SPECIAL
                  30Jun 12:32 ALTUSER PEASEJ SPECIAL
                   1Jul 10:35 ADDUSER DEMOUSER AUTHORITY(USE) DFLTGRP(SYSPROG) N
                   1Jul 10:35 ALTUSER DEMOUSER NOOIDCARD NOPASSWORD RESUME
                   1Jul 10:35 CONNECT DEMOUSER AUTHORITY(USE) GROUP(SYSPROC) NOA
                   1Jul 10:35 ADDSD 'DEMOUSER.WORK.*' NOSET OWNER(SYSPROG)
                   1Jul 10:35 PERMIT 'DEMOUSER.WORK.*' ACCESS(NONE) CLASS(DATASE
                   1Jul 10:35 ALTDSD 'DEMOUSER.WORK.*' UACC(NONE)
                   1Jul 10:35 RDEFINE SURROGAT (DEMOUSER.SUBMIT) LEVEL(0)
                   1Jul 10:35 RALTER SURROGAT (DEMOUSER.SUBMIT) OWNER(DEMOUSER)
                   1Jul 10:35 PERMIT DEMOUSER.SUBMIT ACCESS(READ) CLASS(SURROGAT
```

Into this . . .



Top 10 Event Name Results By Count

7/1/14 11:15 AM - 7/14/14 11:15 AM

▼ Legend

🟩 CONNECT No violations detected 🟦 ALTUSER No violations detected ■ PERMIT No violations detected
🟩 RDEFINE No violations detected 🟥 RDELETE No violations detected 🟨 DELUSER No violations detected
🟦 RALTER No violations detected 🟧 ADDGROUP No violations detected □ DELGROUP No violations detected
🟥 REMOVE No violations detected

Top 10 Event Name Results By Count

7/1/14 11:15 AM - 7/14/14 11:15 AM

▼ Legend

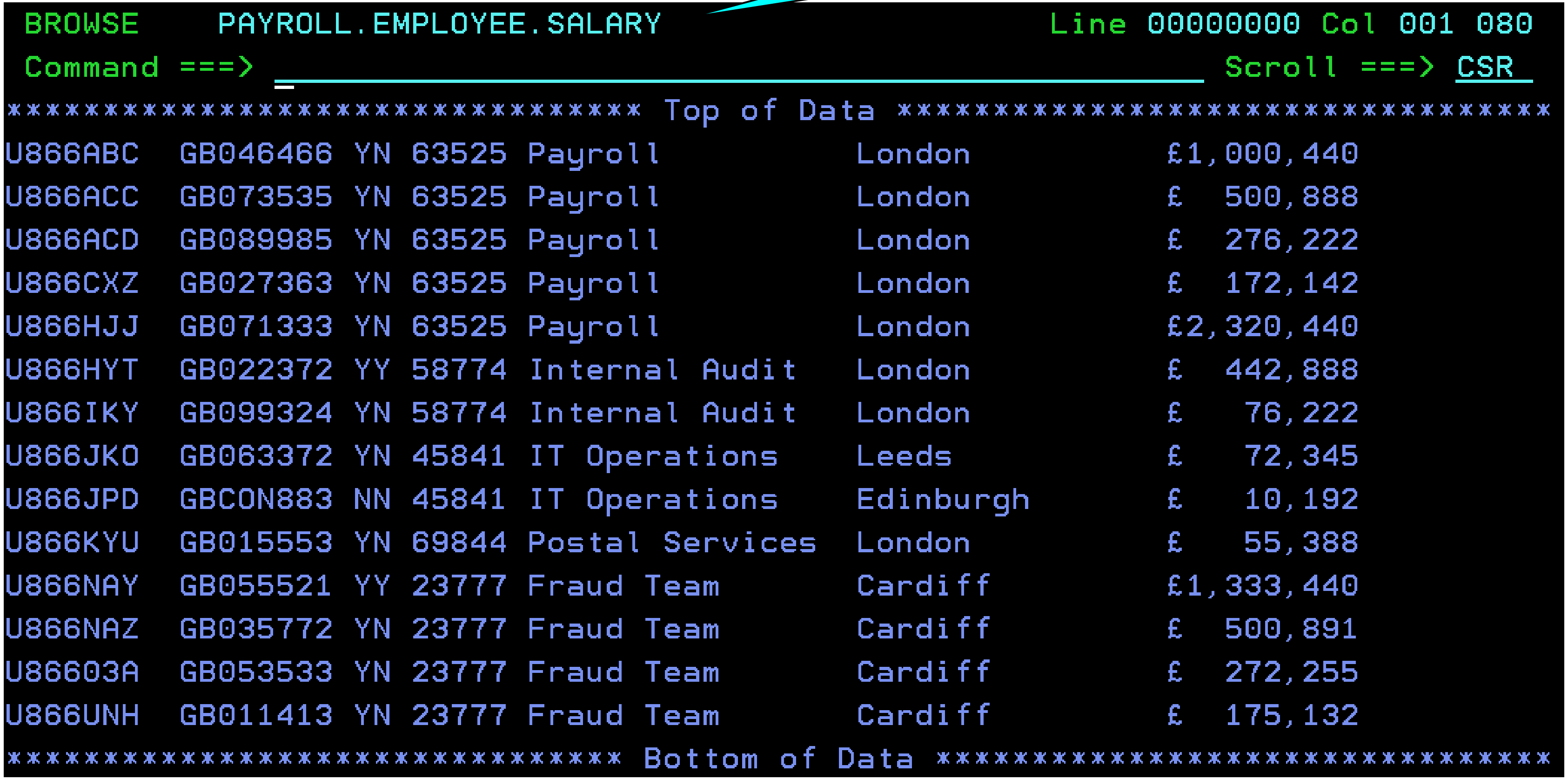
🟩 CONNECT No violations detected 🟦 ALTUSER No violations detected ■ PERMIT No violations detected
🟩 RDEFINE No violations detected 🟥 RDELETE No violations detected 🟨 DELUSER No violations detected
🟦 RALTER No violations detected 🟧 ADDGROUP No violations detected □ DELGROUP No violations detected
🟥 REMOVE No violations detected

(Hide Charts)

Event Name	Command (Unique Count)	Log Source Time (Minimum)	Username (Unique Count)	Log Source (Unique Count)	RACF profile (Unique Count)	Descriptor (Unique Count)	Low Level Category (Unique Count)	Count ▼
CONNECT No violations det…	Multiple (33)	7/1/14, 11:35:28 AM	PEASEJ	JAZZ03 RACF	Multiple (32)	Success	User Account Changed	33
ALTUSER No violations det…	Multiple (6)	7/1/14, 11:35:28 AM	Multiple (2)	JAZZ03 RACF	Multiple (3)	Success	User Account Changed	14
PERMIT No violations detec…	Multiple (3)	7/1/14, 11:35:29 AM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success	Policy Change	3
RDEFINE No violations dete…	Multiple (3)	7/1/14, 11:35:30 AM	Multiple (2)	JAZZ03 RACF	Multiple (3)	Success	Policy Change	3
RDELETE No violations det…	Multiple (2)	7/1/14, 11:35:31 AM	Multiple (2)	JAZZ03 RACF	Multiple (2)	Success	Policy Change	2
DELUSER No violations det…	DELUSER DEMOUSER	7/1/14, 11:35:32 AM	PEASEJ	JAZZ03 RACF	DEMOUSER	Success	User Account Removed	1

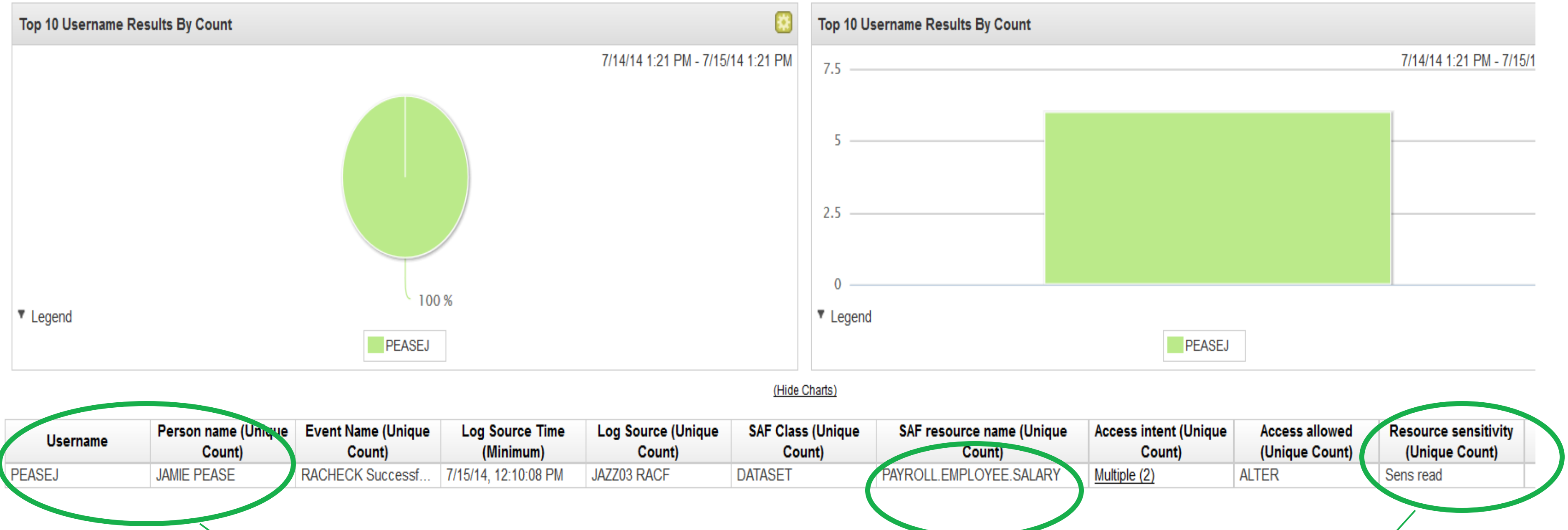
Scenario # 1 – Inappropriate access to sensitive data on z/OS

System Programmer
accesses a Payroll file on
System z



```
 BROWSE    PAYROLL.EMPLOYEE.SALARY                    Line 00000000 Col 001 080
 Command ===>                                                  Scroll ===> CSR
********************************* Top of Data **********************************
U866ABC  GB046466 YN 63525 Payroll          London          £1,000,440
U866ACC  GB073535 YN 63525 Payroll          London          £  500,888
U866ACD  GB089985 YN 63525 Payroll          London          £  276,222
U866CXZ  GB027363 YN 63525 Payroll          London          £  172,142
U866HJJ  GB071333 YN 63525 Payroll          London          £2,320,440
U866HYT  GB022372 YY 58774 Internal Audit   London          £  442,888
U866IKY  GB099324 YN 58774 Internal Audit   London          £   76,222
U866JKO  GB063372 YN 45841 IT Operations    Leeds           £   72,345
U866JPD  GBCON883 NN 45841 IT Operations    Edinburgh       £   10,192
U866KYU  GB015553 YN 69844 Postal Services  London          £   55,388
U866NAY  GB055521 YY 23777 Fraud Team       Cardiff         £1,333,440
U866NAZ  GB035772 YN 23777 Fraud Team       Cardiff         £  500,891
U86603A  GB053533 YN 23777 Fraud Team       Cardiff         £  272,255
U866UNH  GB011413 YN 23777 Fraud Team       Cardiff         £  175,132
******************************** Bottom of Data ********************************
```

Scenario # 1 – Monitoring inappropriate access to sensitive data


Top 10 Username Results By Count
7/14/14 1:21 PM - 7/15/14 1:21 PM
100 %
Legend
PEASEJ
Top 10 Username Results By Count
7/14/14 1:21 PM - 7/15/1
7.5
5
2.5
0
Legend
PEASEJ
(Hide Charts)

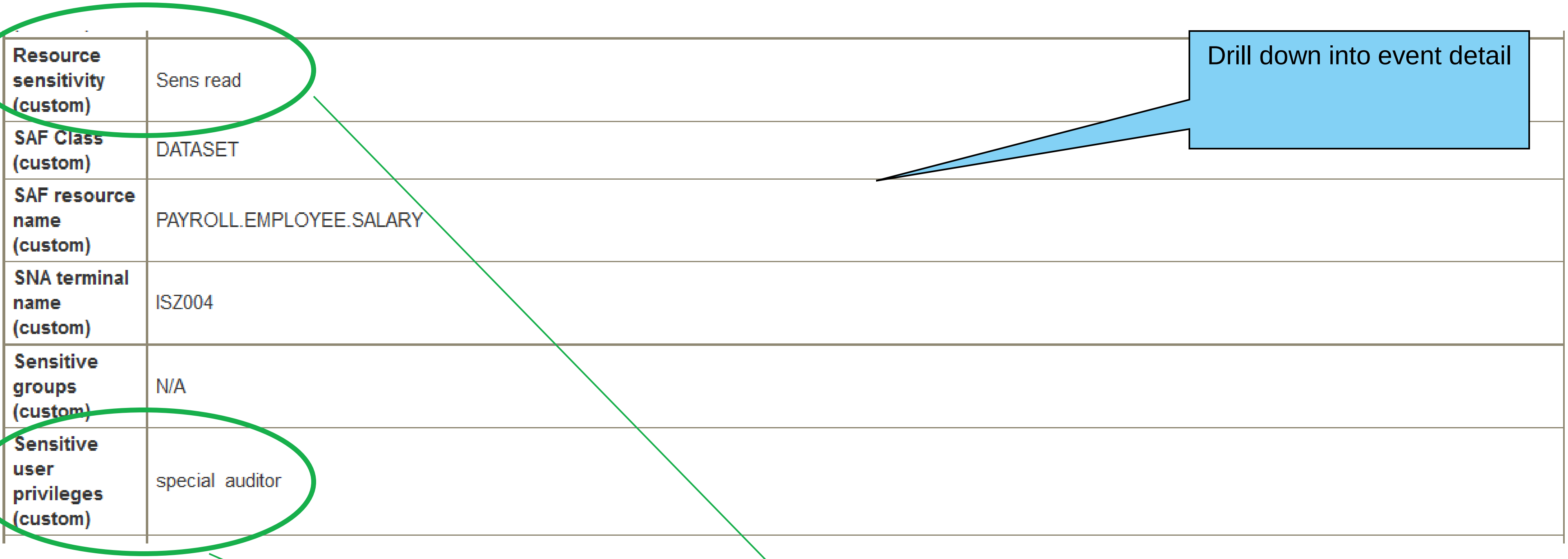
Username	Person name (Unique Count)	Event Name (Unique Count)	Log Source Time (Minimum)	Log Source (Unique Count)	SAF Class (Unique Count)	SAF resource name (Unique Count)	Access intent (Unique Count)	Access allowed (Unique Count)	Resource sensitivity (Unique Count)
PEASEJ	JAMIE PEASE	RACHECK Successf...	7/15/14, 12:10:08 PM	JAZZ03 RACF	DATASET	PAYROLL.EMPLOYEE.SALARY	Multiple (2)	ALTER	Sens read

Who accessed the sensitive resource

What they accessed

Resource is sensitive for read access

Scenario # 1 – Monitoring inappropriate access to sensitive data



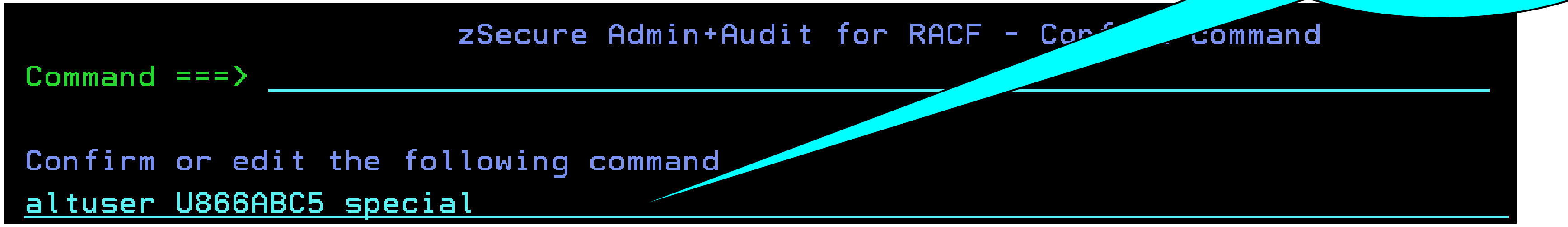
Resource sensitivity (custom)	Sens read
SAF Class (custom)	DATASET
SAF resource name (custom)	PAYROLL.EMPLOYEE.SALARY
SNA terminal name (custom)	ISZ004
Sensitive groups (custom)	N/A
Sensitive user privileges (custom)	special auditor

Drill down into event detail

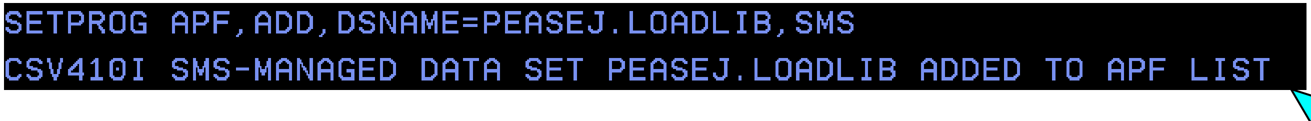
zSecure has enriched event data – assists the Security Officer to understand the user involved and what they accessed

Scenario # 2 – Privileged User Activities occurring on System z

Assigning powerful RACF attributes



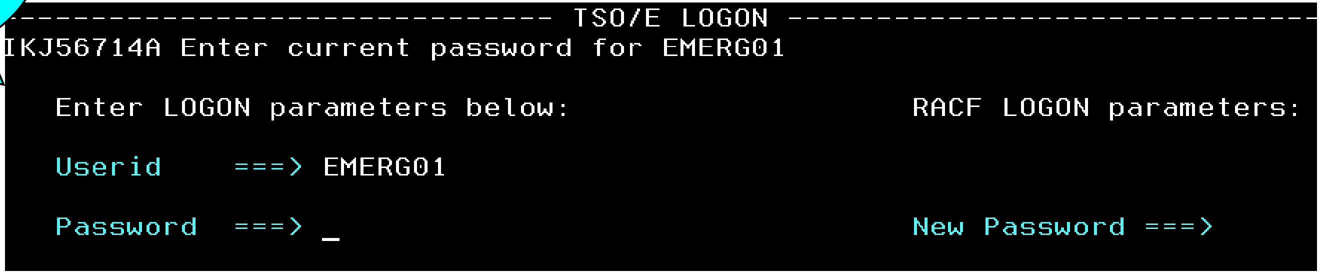
```
                  zSecure Admin+Audit for RACF - Confirm command
Command ===> ________________________________________________________________

Confirm or edit the following command
altuser U866ABC5 special
```



```
SETPROG APF,ADD,DSNAME=PEASEJ.LOADLIB,SMS
CSV410I SMS-MANAGED DATA SET PEASEJ.LOADLIB ADDED TO APF LIST
```

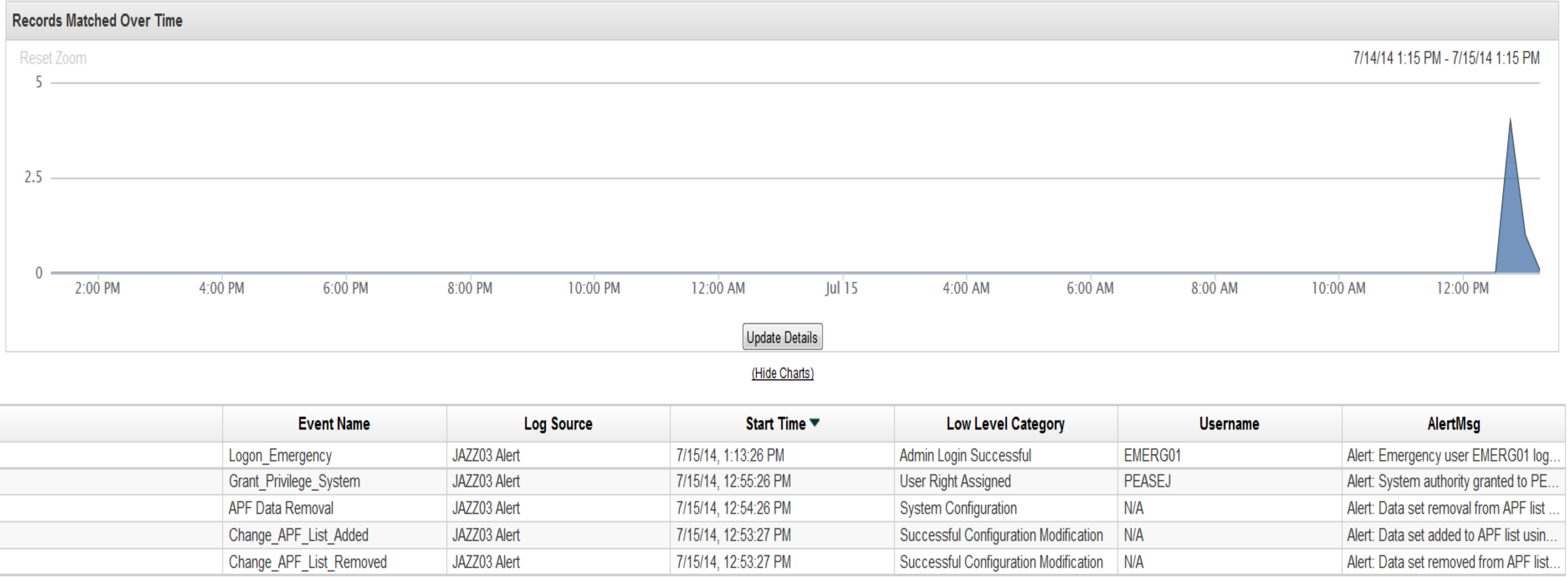
Modifying the Trusted Computing Base

Logon with powerful emergency user IDs



```
------------------------------- TSO/E LOGON -----------------------------------
IKJ56714A Enter current password for EMERG01

  Enter LOGON parameters below:                    RACF LOGON parameters:

  Userid    ===> EMERG01

  Password  ===> _                                 New Password ===>
```

Scenario # 2 – Monitoring Privileged User activities in QRadar



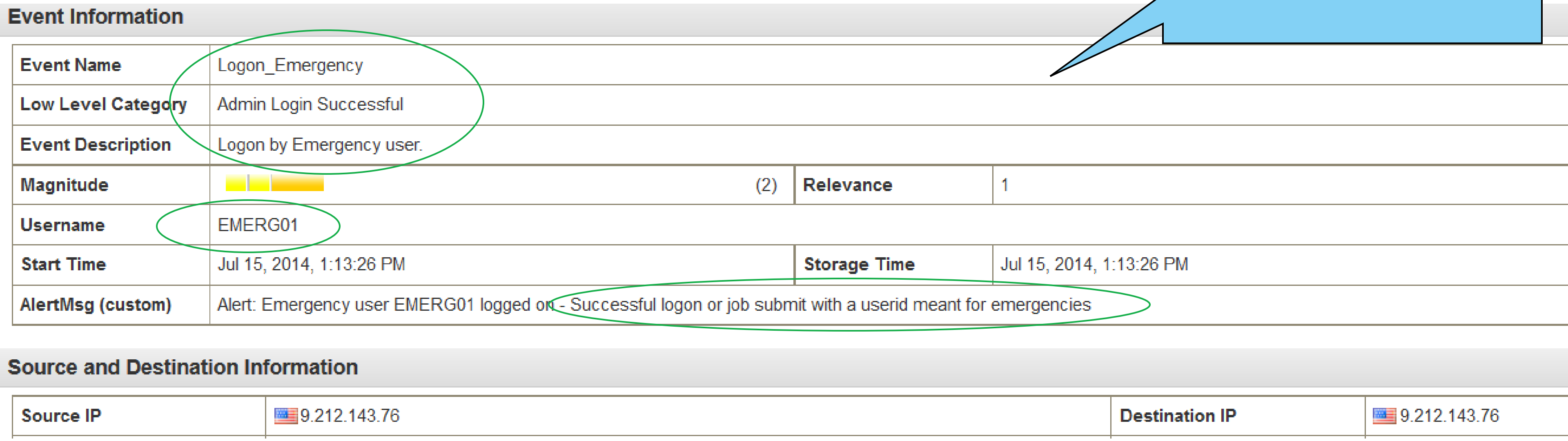
	Event Name	Log Source	Start Time ▼	Low Level Category	Username	AlertMsg
	Logon_Emergency	JAZZ03 Alert	7/15/14, 1:13:26 PM	Admin Login Successful	EMERG01	Alert: Emergency user EMERG01 log...
	Grant_Privilege_System	JAZZ03 Alert	7/15/14, 12:55:26 PM	User Right Assigned	PEASEJ	Alert: System authority granted to PE...
	APF Data Removal	JAZZ03 Alert	7/15/14, 12:54:26 PM	System Configuration	N/A	Alert: Data set removal from APF list ...
	Change_APF_List_Added	JAZZ03 Alert	7/15/14, 12:53:27 PM	Successful Configuration Modification	N/A	Alert: Data set added to APF list usin...
	Change_APF_List_Removed	JAZZ03 Alert	7/15/14, 12:53:27 PM	Successful Configuration Modification	N/A	Alert: Data set removed from APF list...

Events sent to QRadar, seconds later

Collected and sent to QRadar by **zSecure Alert**

Scenario # 2 – Monitoring Privileged User activities in QRadar

Drill down into event detail



Event Information

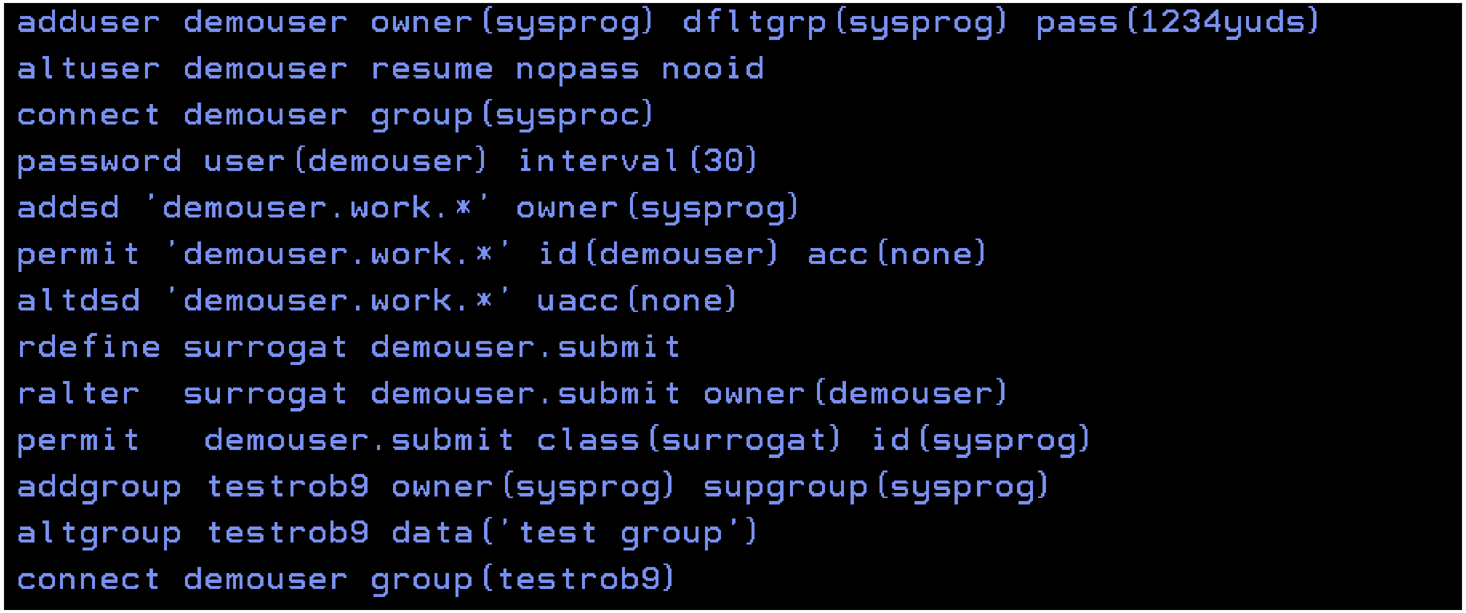
Event Name	Logon_Emergency		
Low Level Category	Admin Login Successful		
Event Description	Logon by Emergency user.		
Magnitude	(2)	Relevance	1
Username	EMERG01		
Start Time	Jul 15, 2014, 1:13:26 PM	Storage Time	Jul 15, 2014, 1:13:26 PM
AlertMsg (custom)	Alert: Emergency user EMERG01 logged on - Successful logon or job submit with a userid meant for emergencies		

Source and Destination Information

Source IP	9.212.143.76	Destination IP	9.212.143.76

Detailed information alerts us to the fact that an emergency user ID has been used – big problem for mainframe customers!

Scenario # 3 – Security Administrator activities occurring on System z

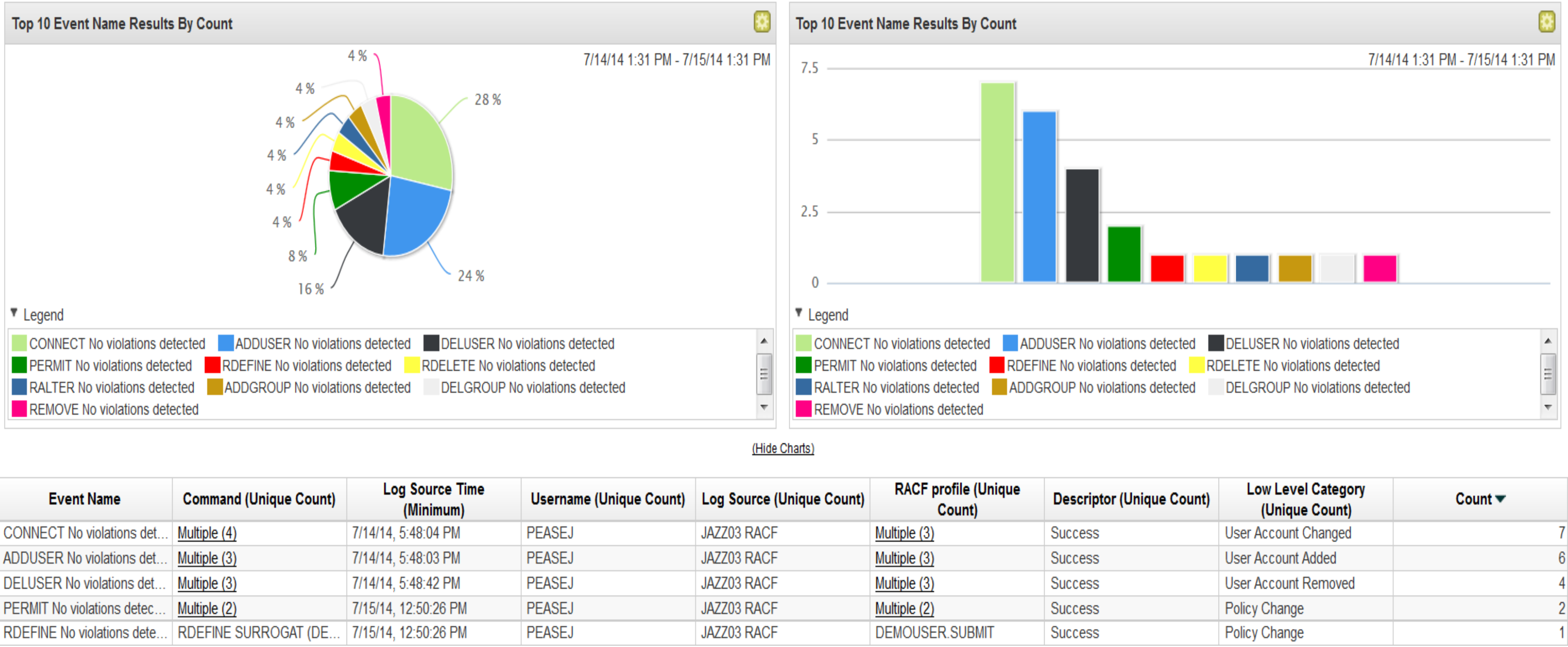


```
adduser demouser owner(sysprog) dfltgrp(sysprog) pass(1234yuds)
altuser demouser resume nopass nooid
connect demouser group(sysproc)
password user(demouser) interval(30)
addsd 'demouser.work.*' owner(sysprog)
permit 'demouser.work.*' id(demouser) acc(none)
altdsd 'demouser.work.*' uacc(none)
rdefine surrogat demouser.submit
ralter  surrogat demouser.submit owner(demouser)
permit   demouser.submit class(surrogat) id(sysprog)
addgroup testrob9 owner(sysprog) supgroup(sysprog)
altgroup testrob9 data('test group')
connect demouser group(testrob9)
```

Executing RACF Commands

Security Administrator is creating new security definitions on the mainframe

Scenario # 3 – Monitoring Security Administrator activities



Top 10 Event Name Results By Count

7/14/14 1:31 PM - 7/15/14 1:31 PM

Legend

🟩 CONNECT No violations detected 🟦 ADDUSER No violations detected ■ DELUSER No violations detected
🟩 PERMIT No violations detected 🟥 RDEFINE No violations detected 🟨 RDELETE No violations detected
🟦 RALTER No violations detected 🟧 ADDGROUP No violations detected □ DELGROUP No violations detected
🟥 REMOVE No violations detected

Top 10 Event Name Results By Count

7/14/14 1:31 PM - 7/15/14 1:31 PM

Legend

🟩 CONNECT No violations detected 🟦 ADDUSER No violations detected ■ DELUSER No violations detected
🟩 PERMIT No violations detected 🟥 RDEFINE No violations detected 🟨 RDELETE No violations detected
🟦 RALTER No violations detected 🟧 ADDGROUP No violations detected □ DELGROUP No violations detected
🟥 REMOVE No violations detected

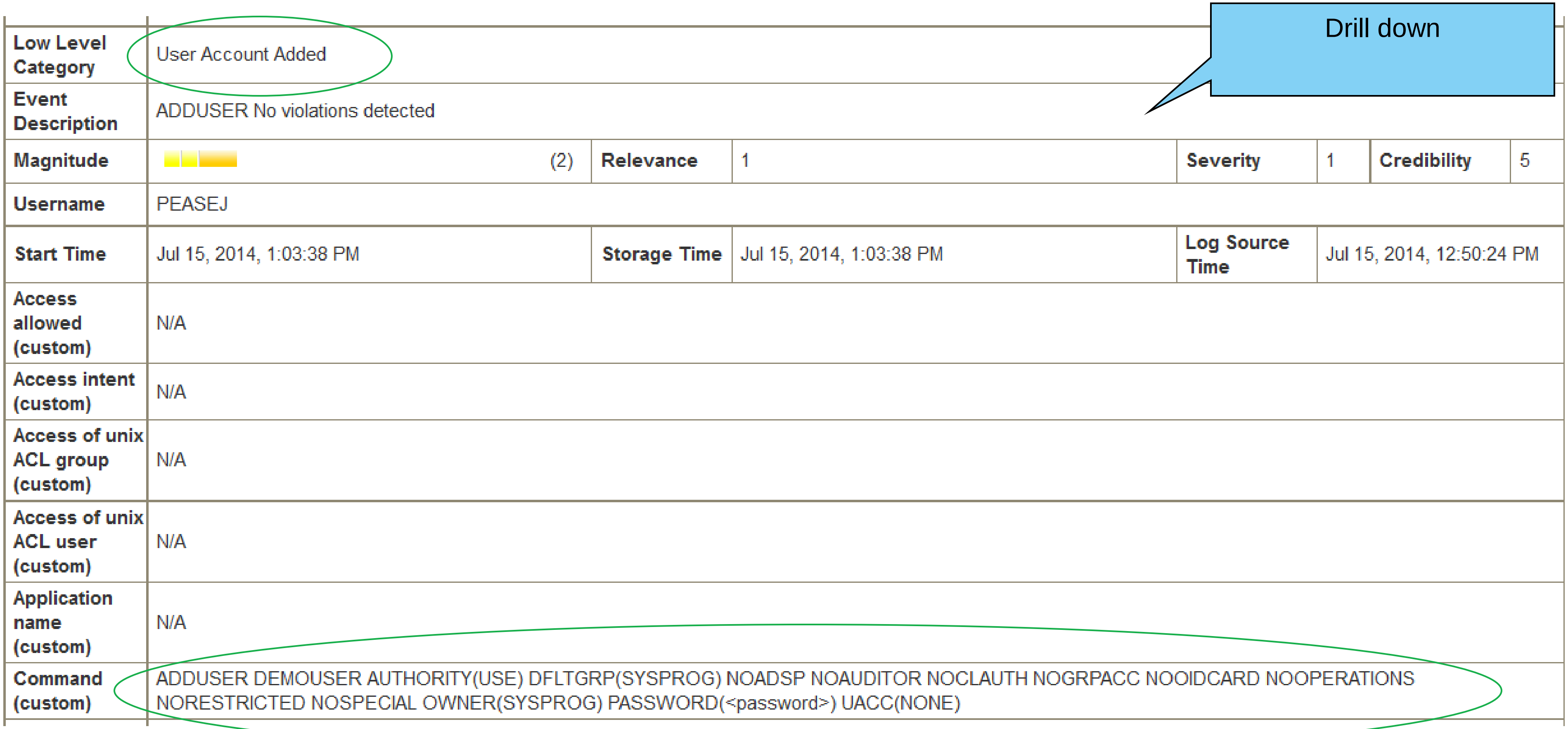
(Hide Charts)

Event Name	Command (Unique Count)	Log Source Time (Minimum)	Username (Unique Count)	Log Source (Unique Count)	RACF profile (Unique Count)	Descriptor (Unique Count)	Low Level Category (Unique Count)	Count ▼
CONNECT No violations det...	Multiple (4)	7/14/14, 5:48:04 PM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success	User Account Changed	7
ADDUSER No violations det...	Multiple (3)	7/14/14, 5:48:03 PM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success	User Account Added	6
DELUSER No violations det...	Multiple (3)	7/14/14, 5:48:42 PM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success	User Account Removed	4
PERMIT No violations detec...	Multiple (2)	7/15/14, 12:50:26 PM	PEASEJ	JAZZ03 RACF	Multiple (2)	Success	Policy Change	2
RDEFINE No violations dete...	RDEFINE SURROGAT (DE...	7/15/14, 12:50:26 PM	PEASEJ	JAZZ03 RACF	DEMOUSER.SUBMIT	Success	Policy Change	1

A view of the RACF commands that have been executed over a 24 hour period – mainframe customers typically run this type of report on a daily basis!

Event data collected by **zSecure Audit**

Scenario # 3 – Monitoring Security Administrator activities

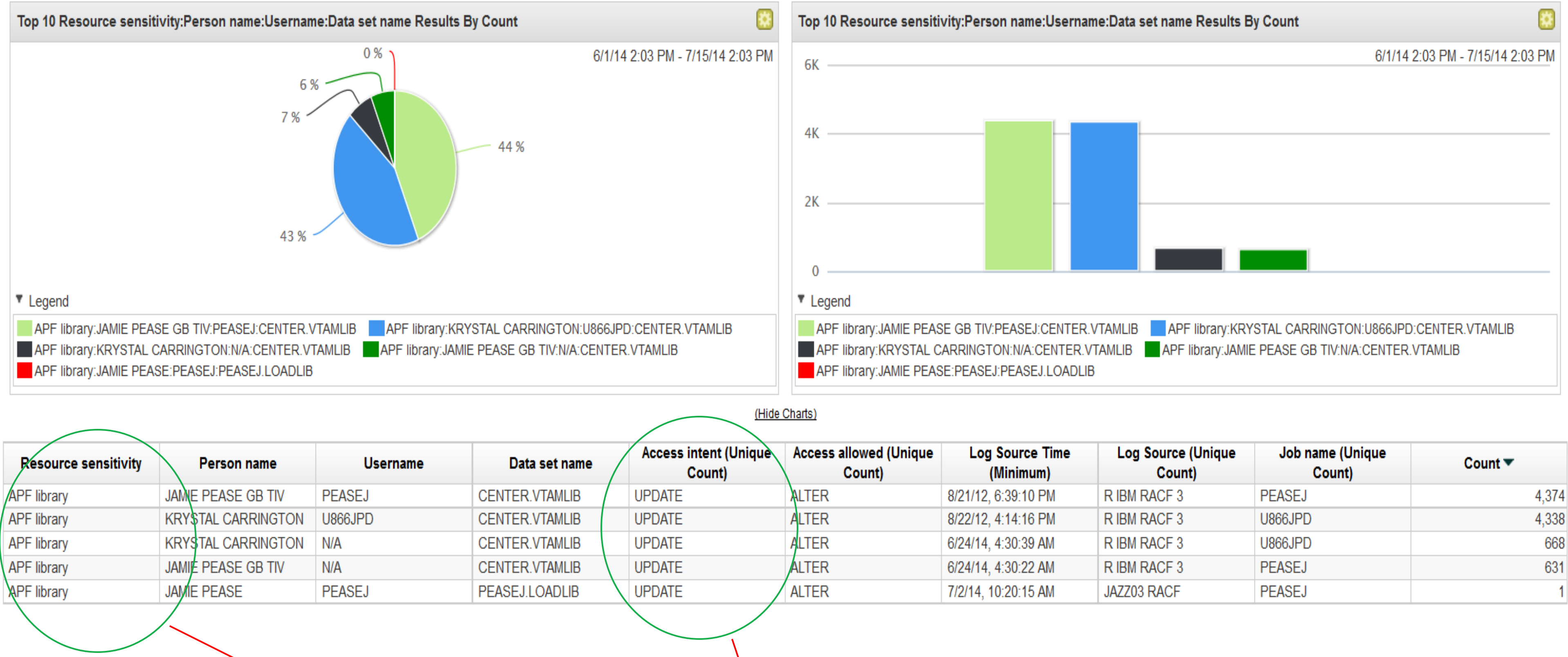


Low Level Category	User Account Added						
Event Description	ADDUSER No violations detected						
Magnitude	🟨🟨🟨 (2)	**Relevance**	1	**Severity**	1	**Credibility**	5
Username	PEASEJ						
Start Time	Jul 15, 2014, 1:03:38 PM	**Storage Time**	Jul 15, 2014, 1:03:38 PM	**Log Source Time**	Jul 15, 2014, 12:50:24 PM		
Access allowed (custom)	N/A						
Access intent (custom)	N/A						
Access of unix ACL group (custom)	N/A						
Access of unix ACL user (custom)	N/A						
Application name (custom)	N/A						
Command (custom)	ADDUSER DEMOUSER AUTHORITY(USE) DFLTGRP(SYSPROG) NOADSP NOAUDITOR NOCLAUTH NOGRPACC NOOIDCARD NOOPERATIONS NORESTRICTED NOSPECIAL OWNER(SYSPROG) PASSWORD(<password>) UACC(NONE)						

Drill down

The actual RACF command that was executed by the Security Administrator

Scenario # 4 – Monitoring your System Programmers



Top 10 Resource sensitivity:Person name:Username:Data set name Results By Count

6/1/14 2:03 PM - 7/15/14 2:03 PM

▾ Legend

🟩 APF library:JAMIE PEASE GB TIV:PEASEJ:CENTER.VTAMLIB 🟦 APF library:KRYSTAL CARRINGTON:U866JPD:CENTER.VTAMLIB
⬛ APF library:KRYSTAL CARRINGTON:N/A:CENTER.VTAMLIB 🟩 APF library:JAMIE PEASE GB TIV:N/A:CENTER.VTAMLIB
🟥 APF library:JAMIE PEASE:PEASEJ:PEASEJ.LOADLIB

Top 10 Resource sensitivity:Person name:Username:Data set name Results By Count

6/1/14 2:03 PM - 7/15/14 2:03 PM

▾ Legend

🟩 APF library:JAMIE PEASE GB TIV:PEASEJ:CENTER.VTAMLIB 🟦 APF library:KRYSTAL CARRINGTON:U866JPD:CENTER.VTAMLIB
⬛ APF library:KRYSTAL CARRINGTON:N/A:CENTER.VTAMLIB 🟩 APF library:JAMIE PEASE GB TIV:N/A:CENTER.VTAMLIB
🟥 APF library:JAMIE PEASE:PEASEJ:PEASEJ.LOADLIB

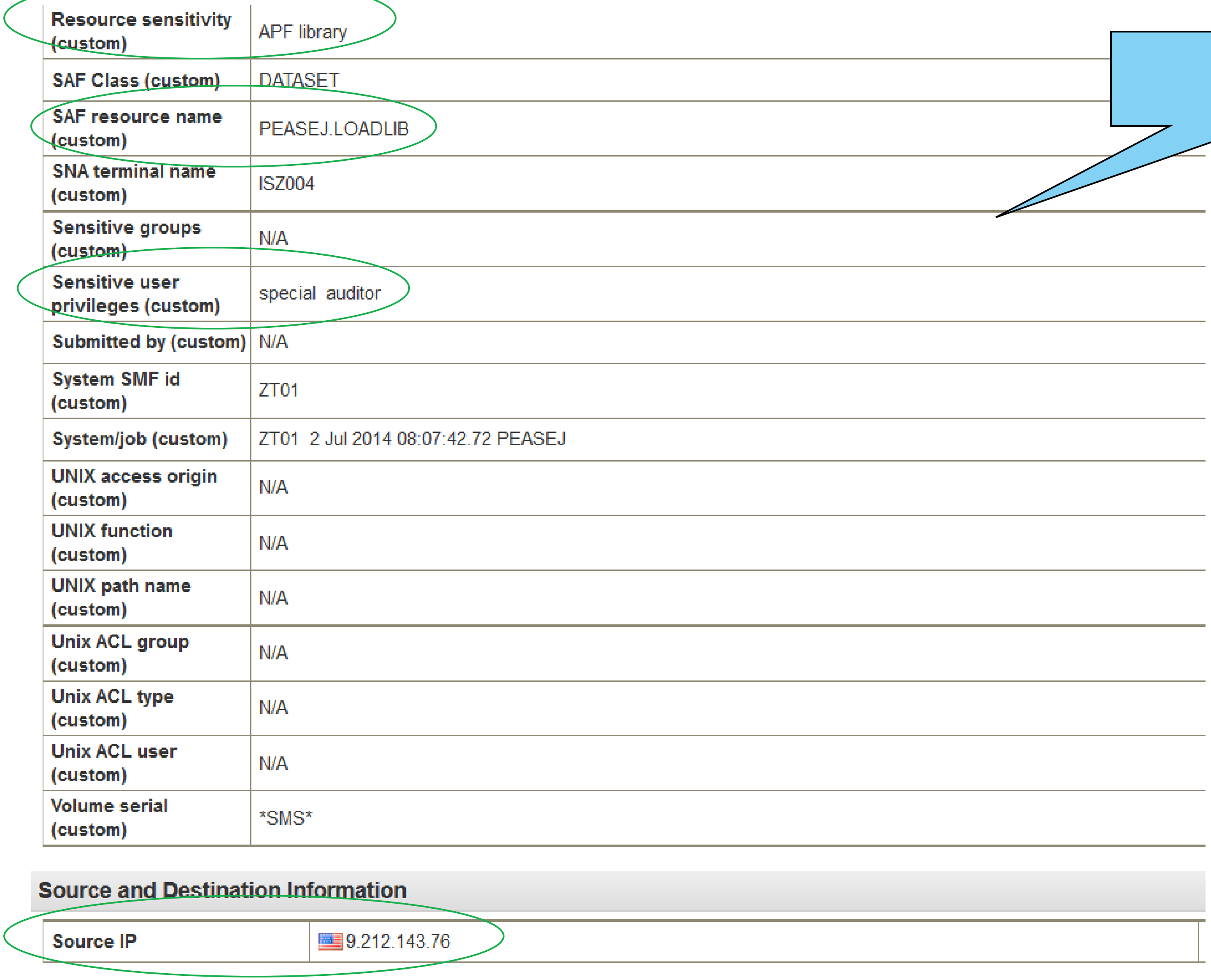
(Hide Charts)

Resource sensitivity	Person name	Username	Data set name	Access intent (Unique Count)	Access allowed (Unique Count)	Log Source Time (Minimum)	Log Source (Unique Count)	Job name (Unique Count)	Count ▾
APF library	JAMIE PEASE GB TIV	PEASEJ	CENTER.VTAMLIB	UPDATE	ALTER	8/21/12, 6:39:10 PM	R IBM RACF 3	PEASEJ	4,374
APF library	KRYSTAL CARRINGTON	U866JPD	CENTER.VTAMLIB	UPDATE	ALTER	8/22/12, 4:14:16 PM	R IBM RACF 3	U866JPD	4,338
APF library	KRYSTAL CARRINGTON	N/A	CENTER.VTAMLIB	UPDATE	ALTER	6/24/14, 4:30:39 AM	R IBM RACF 3	U866JPD	668
APF library	JAMIE PEASE GB TIV	N/A	CENTER.VTAMLIB	UPDATE	ALTER	6/24/14, 4:30:22 AM	R IBM RACF 3	PEASEJ	631
APF library	JAMIE PEASE	PEASEJ	PEASEJ.LOADLIB	UPDATE	ALTER	7/2/14, 10:20:15 AM	JAZZ03 RACF	PEASEJ	1

Highly sensitive resource – keys to the kingdom!

Could be used to circumvent system security

Scenario # 4 – Monitoring your System Programmers



Resource sensitivity (custom)	APF library
SAF Class (custom)	DATASET
SAF resource name (custom)	PEASEJ.LOADLIB
SNA terminal name (custom)	ISZ004
Sensitive groups (custom)	N/A
Sensitive user privileges (custom)	special auditor
Submitted by (custom)	N/A
System SMF id (custom)	ZT01
System/job (custom)	ZT01 2 Jul 2014 08:07:42.72 PEASEJ
UNIX access origin (custom)	N/A
UNIX function (custom)	N/A
UNIX path name (custom)	N/A
Unix ACL group (custom)	N/A
Unix ACL type (custom)	N/A
Unix ACL user (custom)	N/A
Volume serial (custom)	*SMS*

Source and Destination Information

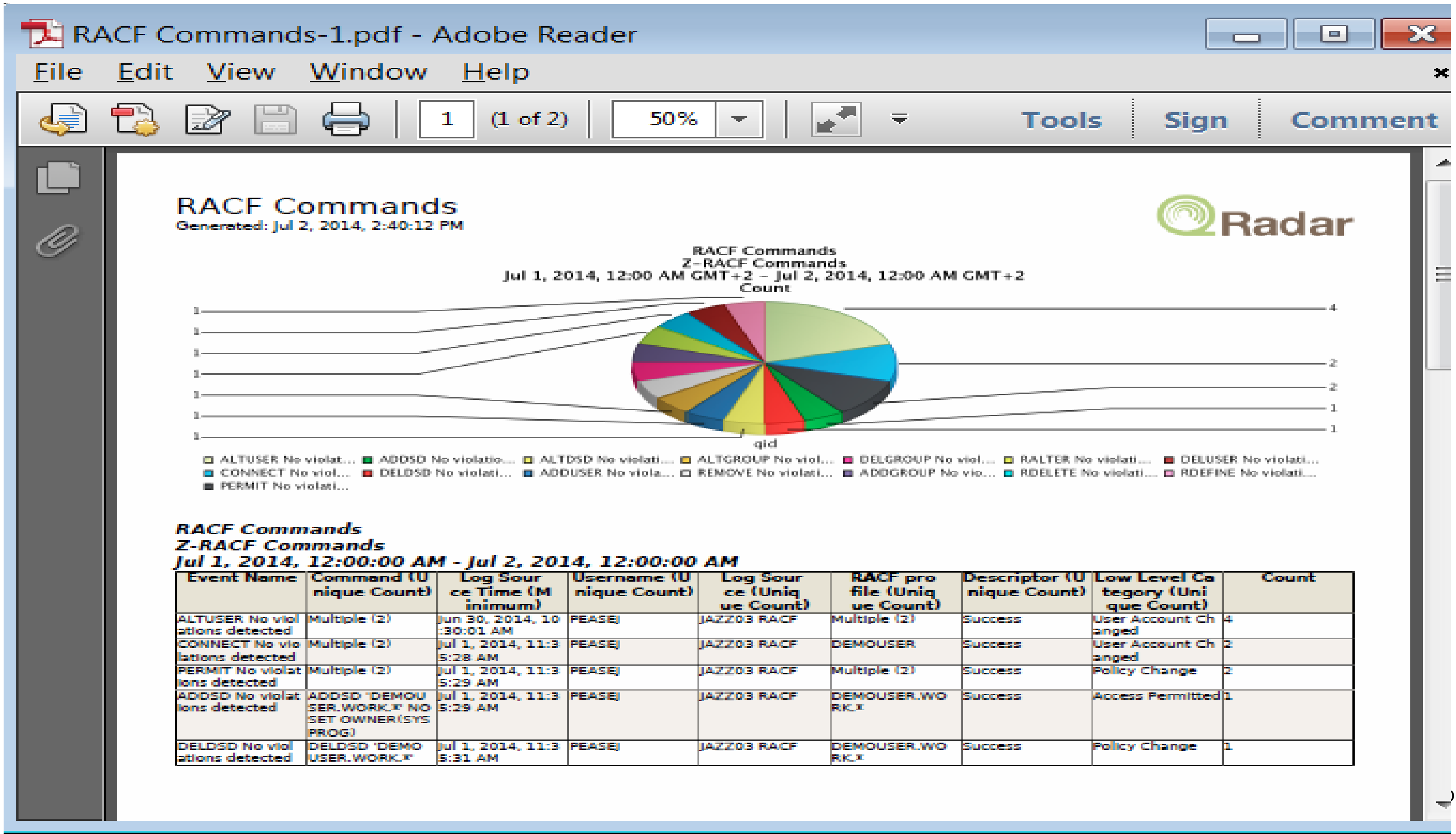
Source IP	9.212.143.76

Drill down

Scenario # 5 – Daily (scheduled) reporting

!	Report Name ▲	Group	Schedule
	Access to Payroll files	Security	Daily
	Alerts from previous day	Security	Daily
	RACF Commands	Security	Daily
	RACF Violations	Security	Daily
	Sensitive Dataset Updates	Security	Daily

Customers typically run scheduled monitoring reports

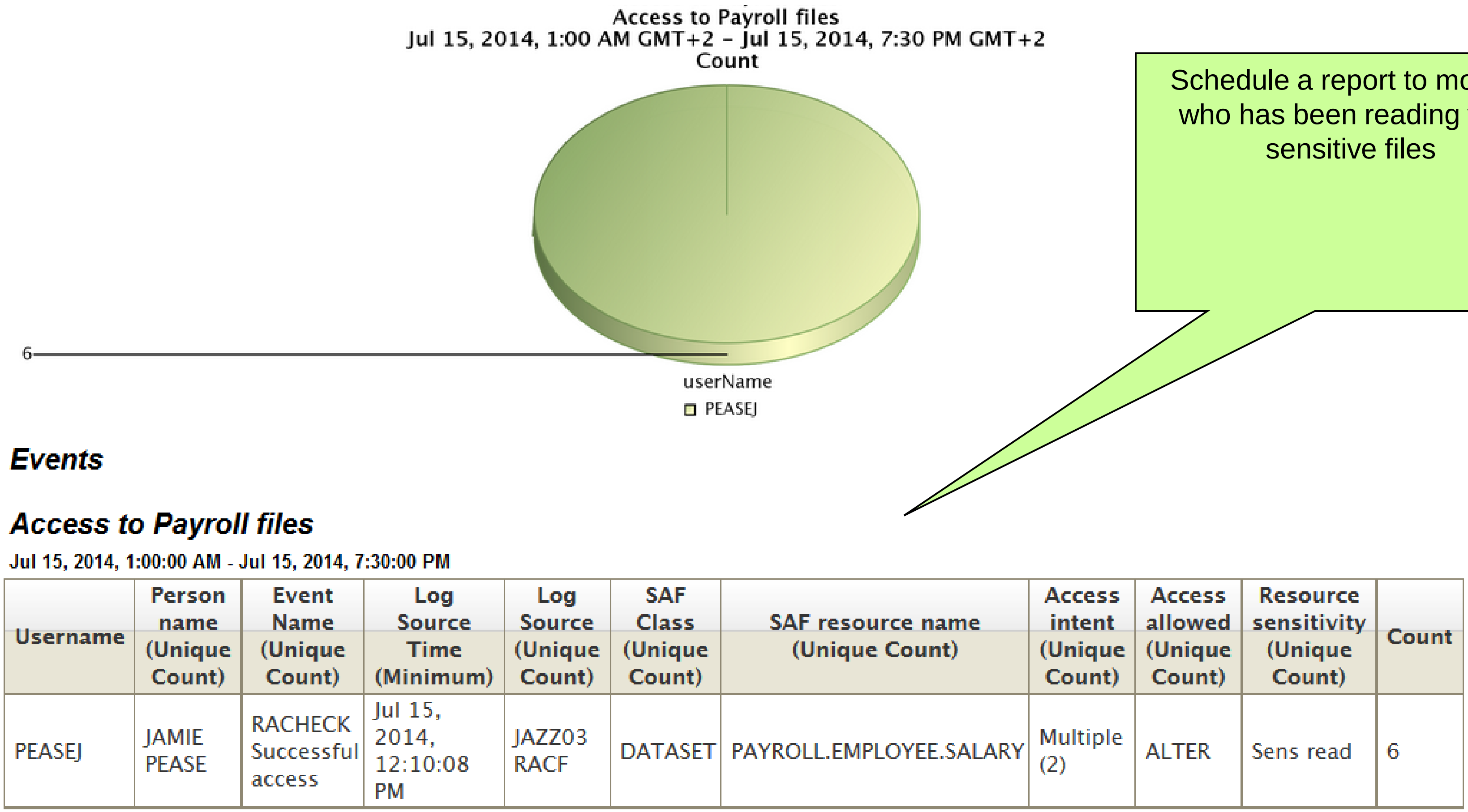


RACF Commands
Generated: Jul 2, 2014, 2:40:12 PM

RACF Commands
Z-RACF Commands
Jul 1, 2014, 12:00:00 AM - Jul 2, 2014, 12:00:00 AM

Event Name	Command (Unique Count)	Log Source Time (Minimum)	Username (Unique Count)	Log Source (Unique Count)	RACF profile (Unique Count)	Descriptor (Unique Count)	Low Level Category (Unique Count)	Count
ALTUSER No violations detected	Multiple (2)	Jun 30, 2014, 10:30:01 AM	PEASEJ	JAZZ03 RACF	Multiple (2)	Success	User Account Changed	4
CONNECT No violations detected	Multiple (2)	Jul 1, 2014, 11:35:28 AM	PEASEJ	JAZZ03 RACF	DEMOUSER	Success	User Account Changed	2
PERMIT No violations detected	Multiple (2)	Jul 1, 2014, 11:35:29 AM	PEASEJ	JAZZ03 RACF	Multiple (2)	Success	Policy Change	2
ADDSD No violations detected	ADDSD 'DEMOUSER.WORK.*' NOSET OWNER(SYSPROG)	Jul 1, 2014, 11:35:29 AM	PEASEJ	JAZZ03 RACF	DEMOUSER.WORK.*	Success	Access Permitted	1
DELDSD No violations detected	DELDSD 'DEMOUSER.WORK.*'	Jul 1, 2014, 11:35:31 AM	PEASEJ	JAZZ03 RACF	DEMOUSER.WORK.*	Success	Policy Change	1

Scenario # 5 – Daily (scheduled) reporting



Schedule a report to monitor who has been reading your sensitive files

Events

Access to Payroll files

Jul 15, 2014, 1:00:00 AM - Jul 15, 2014, 7:30:00 PM

Username	Person name (Unique Count)	Event Name (Unique Count)	Log Source Time (Minimum)	Log Source (Unique Count)	SAF Class (Unique Count)	SAF resource name (Unique Count)	Access intent (Unique Count)	Access allowed (Unique Count)	Resource sensitivity (Unique Count)	Count
PEASEJ	JAMIE PEASE	RACHECK Successful access	Jul 15, 2014, 12:10:08 PM	JAZZ03 RACF	DATASET	PAYROLL.EMPLOYEE.SALARY	Multiple (2)	ALTER	Sens read	6

Casos Combinados

Hardening environments is difficult and growing increasingly complex

The ever expanding number of endpoints, applications, databases and network devices create multiple attack surfaces

Integrated Defense Strategy

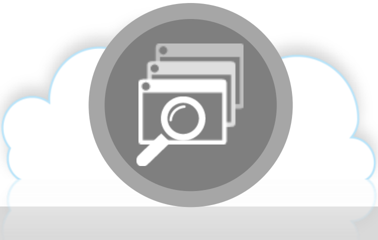
HARDEN | DETECT | ANALYZE

Endpoints

- Validate endpoint patch status

Applications

- Prevent web application vulnerabilities



Hardening challenges:

- Mobile device proliferation and adoption of BYOD
- Adoption of hybrid and public cloud
- Rapid growth of big data
- Continued exploitation of SQL injection and cross site scripting vulnerabilities

Networks

- Secure network traffic

Databases

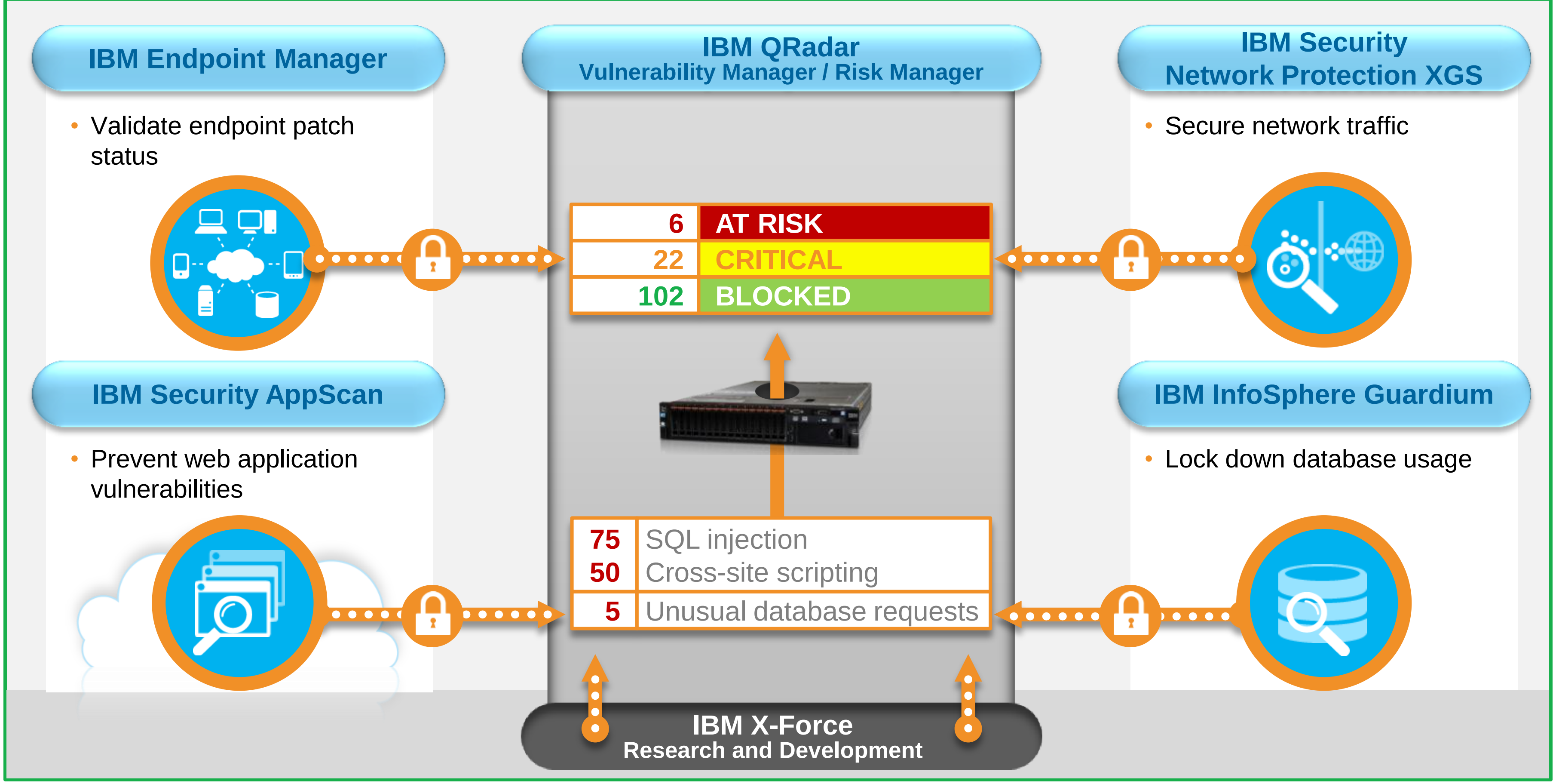
- Lock down database usage

Harden through integrated security solutions

Scan assets for vulnerabilities, prioritize the severity of each vulnerability, and patch or block the most critical

Integrated Defense Strategy

HARDEN › DETECT › ANALYZE



IBM Endpoint Manager

- Validate endpoint patch status

IBM QRadar
Vulnerability Manager / Risk Manager

IBM Security Network Protection XGS

- Secure network traffic

6	AT RISK
22	CRITICAL
102	BLOCKED

IBM Security AppScan

- Prevent web application vulnerabilities

IBM InfoSphere Guardium

- Lock down database usage

75	SQL injection
50	Cross-site scripting
5	Unusual database requests

IBM X-Force
Research and Development

How hardening works: practical steps

Harden Endpoints

- Manage hundreds of thousands of endpoints
- Automatically enforce security baselines across all endpoints

IBM Endpoint Manager

Harden Applications

- Leverage multiple source code scanning technologies
- Scan production web apps to detect vulnerabilities

IBM AppScan

Harden Network Traffic

- Virtually patch detected vulnerabilities
- Filter internet traffic according to security policies

IBM Network Protection XGS

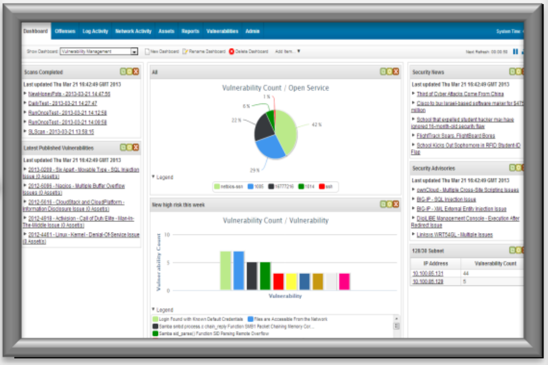
Harden Databases

- Scan database for security exposures
- Identify behavioral vulnerabilities

IBM InfoSphere Guardium

IBM QRadar
Vulnerability Manager / Risk Manager

Find and Prioritize Vulnerabilities



Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Vulnerabilities | Admin | System Time

Show Dashboard: Vulnerability Management | New Dashboard | Rename Dashboard | Delete Dashboard | Add Item... | Next Refresh: 00:00:50

Scans Completed

Last updated Thu Mar 21 10:42:49 GMT 2013

- NewHoneyPots - 2013-03-21 14:47:56
- DailyTest - 2013-03-21 14:27:47
- RunOnceTest - 2013-03-21 14:12:58
- RunOnceTest - 2013-03-21 14:08:58
- SLScan - 2013-03-21 13:58:15

Latest Published Vulnerabilities

Last updated Thu Mar 21 10:42:49 GMT 2013

- 2013-0289 - Six Apart - Movable Type - SQL Injection Issue (0 Assets)
- 2012-6086 - Nagios - Multiple Buffer Overflow Issues (0 Assets)
- 2012-5616 - CloudStack and CloudPlatform - Information Disclosure Issue (0 Assets)
- 2012-4818 - Activision - Call of Duty Elite - Man-In-The-Middle Issue (0 Assets)
- 2012-4461 - Linux - Kernel - Denial-Of-Service Issue (0 Assets)

All

New high risk this week

Vulnerability Count / Vulnerability
Vulnerability Count
10
5
0
Vulnerability
Legend
Login Found with Known Default Credentials
Files are Accessible From the Network
Samba smbd process.c chain_reply Function SMB1 Packet Chaining Memory Cor...
Samba sid_parse() Function SID Parsing Remote Overflow

Security News

Last updated Thu Mar 21 10:42:49 GMT 2013

- Third of Cyber Attacks Come From China
- Cisco to buy Israel-based software maker for $475 million
- School that expelled student hacker may have ignored 16-month-old security flaw
- FlightTrack Soars, FlightBoard Bores
- School Kicks Out Sophomore in RFID Student ID Flap

Security Advisories

Last updated Thu Mar 21 10:42:49 GMT 2013

- ownCloud - Multiple Cross-Site Scripting Issues
- BIG-IP - SQL Injection Issue
- BIG-IP - XML External Entity Injection Issue
- DigiLIBE Management Console - Execution After Redirect Issue
- Linksys WRT54GL - Multiple Issues

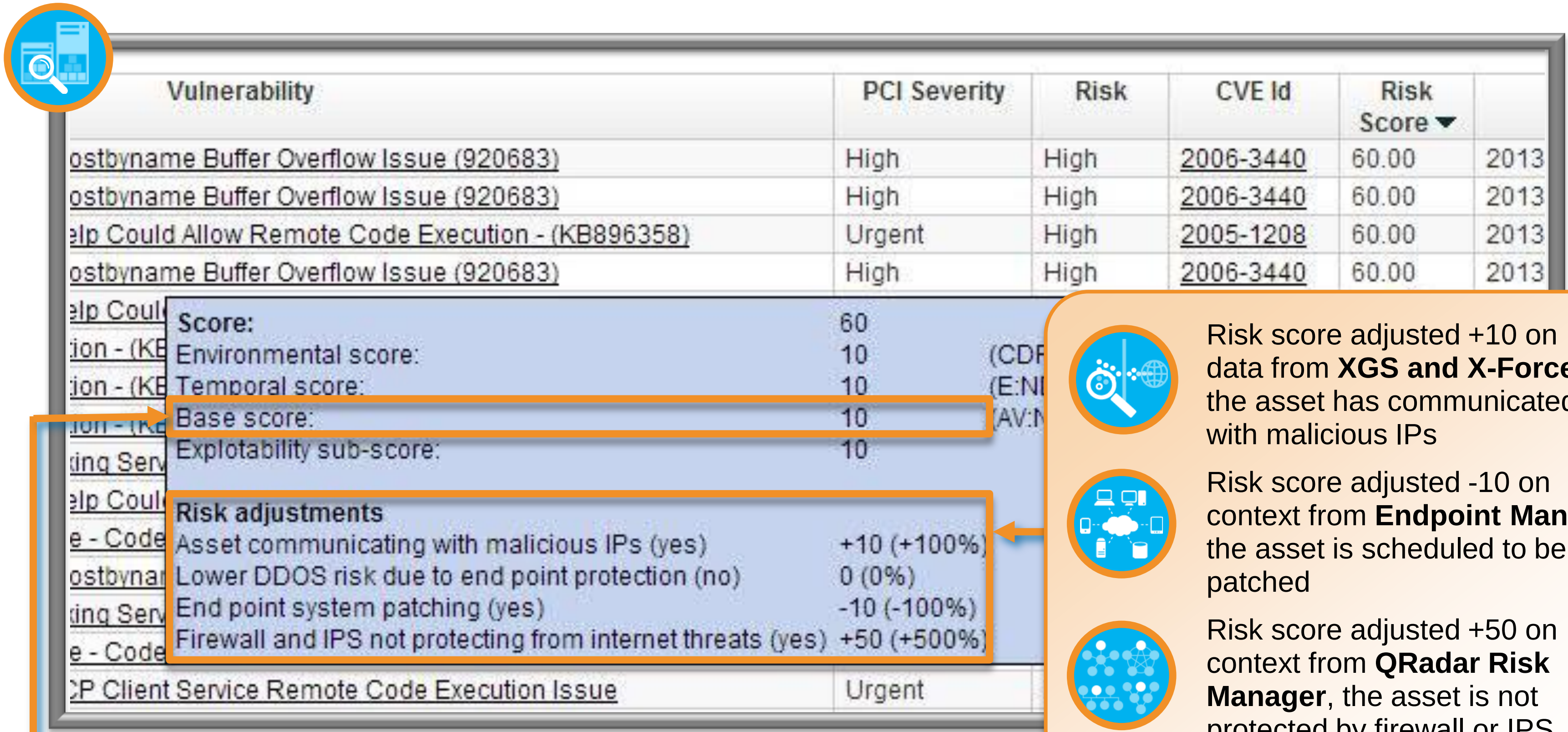
128/30 Subnet

IP Address	Vulnerability Count
10.100.85.131	44
10.100.85.128	5

The security administrator…

- Performs real-time vulnerability scans
- Ensures hardened network device configurations
- Views prioritization of vulnerabilities in context
- Addresses the most critical risks first

Integrated products provide rich context for vulnerability risk scoring



Vulnerability	PCI Severity	Risk	CVE Id	Risk Score ▼	
ostbyname Buffer Overflow Issue (920683)	High	High	2006-3440	60.00	2013
ostbyname Buffer Overflow Issue (920683)	High	High	2006-3440	60.00	2013
elp Could Allow Remote Code Execution - (KB896358)	Urgent	High	2005-1208	60.00	2013
ostbyname Buffer Overflow Issue (920683)	High	High	2006-3440	60.00	2013
elp Coul					
ion - (KE					
ion - (KE					
ion - (KE					
ing Serv					
elp Coul					
e - Code					
ostbynar					
ing Serv					
e - Code					
CP Client Service Remote Code Execution Issue	Urgent				

Score:	60	
Environmental score:	10	(CDF
Temporal score:	10	(E:NI
Base score:	10	(AV:N
Explotability sub-score:	10	
Risk adjustments		
Asset communicating with malicious IPs (yes)	+10 (+100%)	
Lower DDOS risk due to end point protection (no)	0 (0%)	
End point system patching (yes)	-10 (-100%)	
Firewall and IPS not protecting from internet threats (yes)	+50 (+500%)	

Risk score adjusted +10 on data from **XGS and X-Force**, the asset has communicated with malicious IPs

Risk score adjusted -10 on context from **Endpoint Manager**, the asset is scheduled to be patched

Risk score adjusted +50 on context from **QRadar Risk Manager**, the asset is not protected by firewall or IPS

- **QRadar Vulnerability Manage**r conducts native vulnerability scan and incorporates from other vulnerability sources
- Each vulnerability is given a base risk score, in this case 10

Hardening people is essential and becoming more complex

Multiple identity stores and increasing connections from outside the enterprise complicate identity security

Integrated Defense Strategy

HARDEN › DETECT › ANALYZE

Validate Identity

- Determine who is who

Integrate Identity

- Unify “Universe of identities”

Identity hardening challenges:

- Multiple user access points a weak link for attackers to break-in (employees, contractors, partners)
- Extending identity security to mobile, cloud and social interactions
- Highly privileged insiders have access to the “crown jewels”
- Compliance exposure from multiple identity silos and fragment user data
- Increasing security demands for real-time user activity data

Prevent Insider Threat and Identity Fraud

- Secure shared identities and prevent targeted attacks

Manage Identity

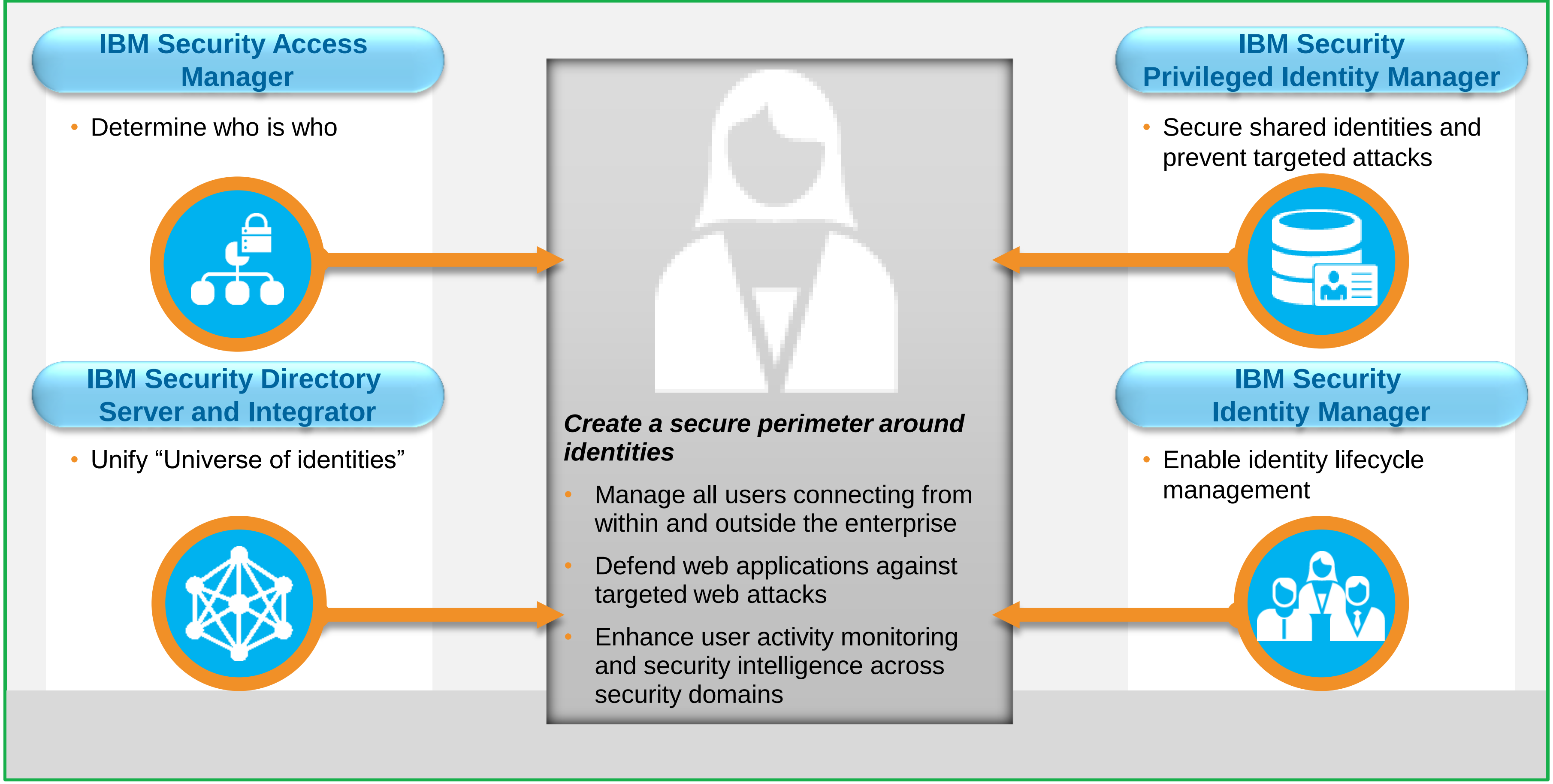
- Enable identity lifecycle management

Define a new perimeter with threat-aware Identity and Access Mgmt

Simplify identity silos to safeguard mobile, cloud and social interactions, mitigate insider threat and deliver intelligent identity and access assurance

Integrated Defense Strategy

HARDEN › DETECT › ANALYZE



IBM Security Access Manager

- Determine who is who

IBM Security Directory Server and Integrator

- Unify “Universe of identities”

Create a secure perimeter around identities

- Manage all users connecting from within and outside the enterprise
- Defend web applications against targeted web attacks
- Enhance user activity monitoring and security intelligence across security domains

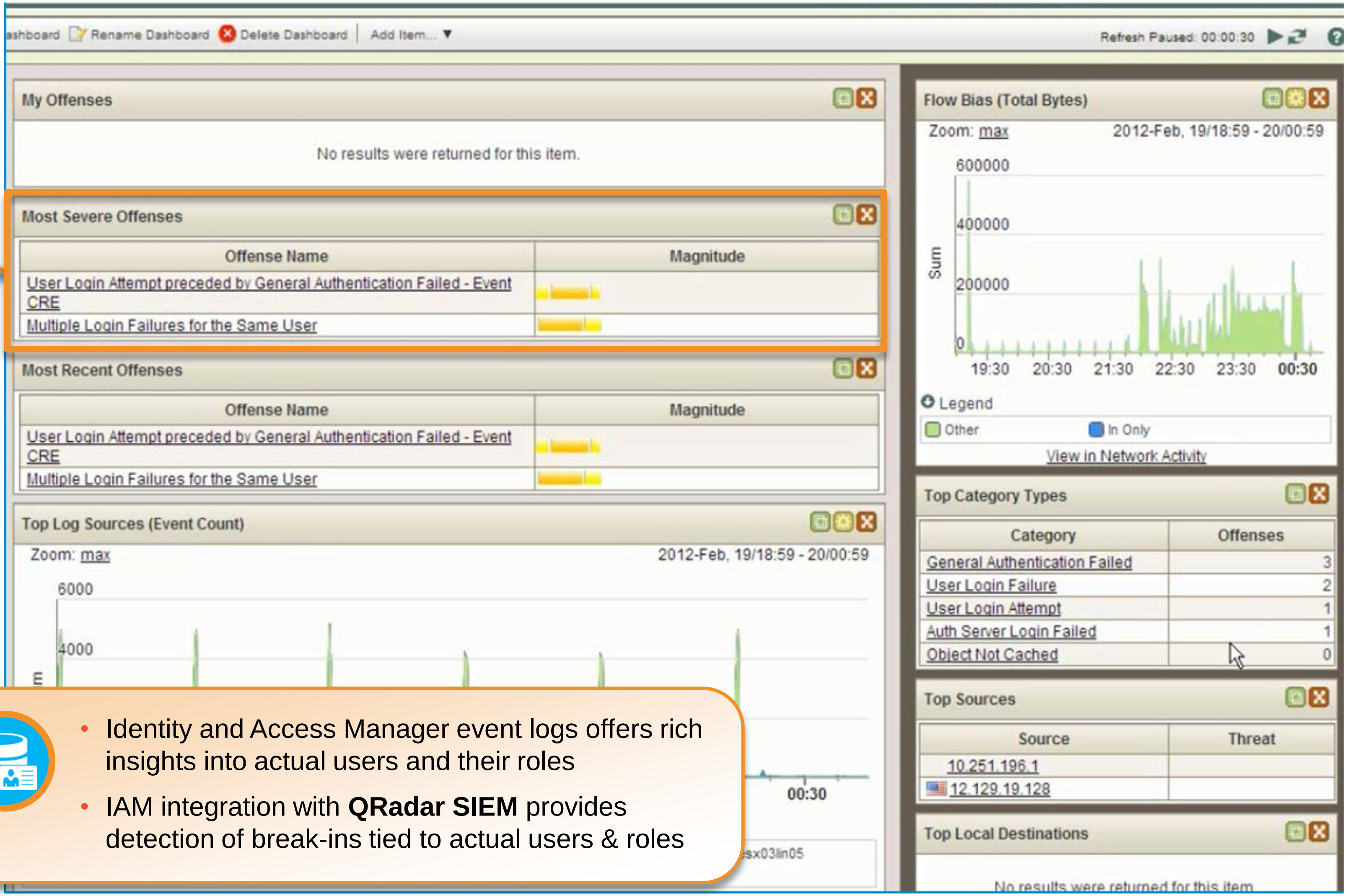
IBM Security Privileged Identity Manager

- Secure shared identities and prevent targeted attacks

IBM Security Identity Manager

- Enable identity lifecycle management

Integrated products provide user activity and anomalies detection



My Offenses

No results were returned for this item.

Most Severe Offenses

Offense Name	Magnitude
User Login Attempt preceded by General Authentication Failed - Event CRE	
Multiple Login Failures for the Same User	

Most Recent Offenses

Offense Name	Magnitude
User Login Attempt preceded by General Authentication Failed - Event CRE	
Multiple Login Failures for the Same User	

Top Log Sources (Event Count)

Zoom: max 2012-Feb, 19/18:59 - 20/00:59

Flow Bias (Total Bytes)

Zoom: max 2012-Feb, 19/18:59 - 20/00:59

View in Network Activity

Top Category Types

Category	Offenses
General Authentication Failed	3
User Login Failure	2
User Login Attempt	1
Auth Server Login Failed	1
Object Not Cached	0

Top Sources

Source	Threat
10.251.196.1	
12.129.19.128	

Top Local Destinations

No results were returned for this item.

- Identity and Access Manager event logs offers rich insights into actual users and their roles
- IAM integration with **QRadar SIEM** provides detection of break-ins tied to actual users & roles

Patient, sophisticated attackers make detection a challenge

Detect subtle anomalies across domains and correlate them to create a cohesive picture of threat activity

Integrated Defense Strategy

HARDEN | DETECT | ANALYZE

Network Traffic

- Blocks exploits as they traverse the network

Application Access

- Blocks attacks before they reach applications

Detect challenges:

- Attackers modify signatures to bypass signature based detection
- Users connect from new devices and locations
- Lack of control over privileged users passwords and access
- Increasing number endpoints, device types and operating systems

Privileged Users

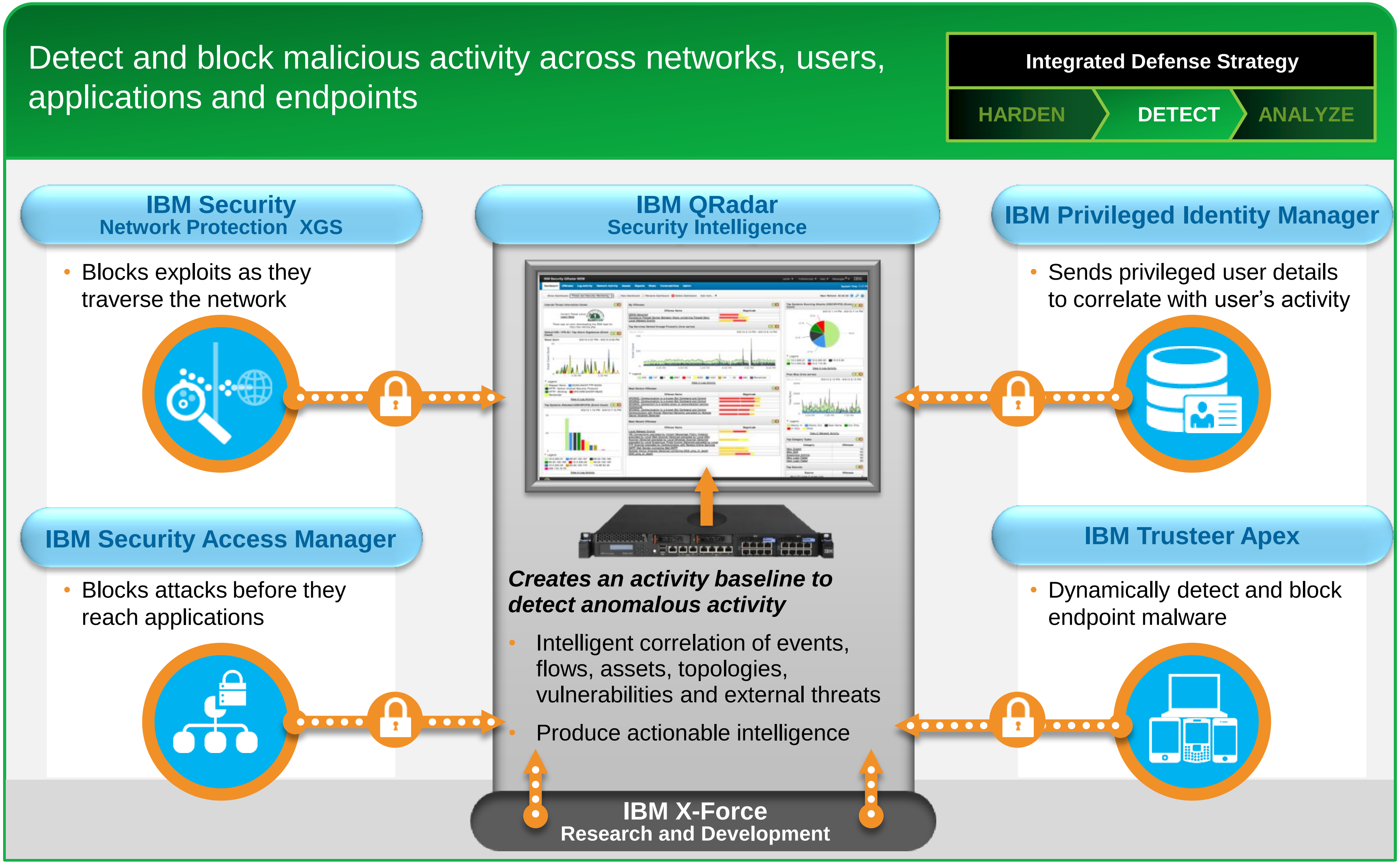
- Sends privileged user details to correlate with user's activity

Endpoint Protection

- Dynamically detect and block endpoint malware

Threat Research

Integrated capabilities enable real-time discovery and blocking



Detect and block malicious activity across networks, users, applications and endpoints

IBM Security Network Protection XGS

- Blocks exploits as they traverse the network

IBM Security Access Manager

- Blocks attacks before they reach applications

IBM QRadar Security Intelligence

Creates an activity baseline to detect anomalous activity

- Intelligent correlation of events, flows, assets, topologies, vulnerabilities and external threats
- Produce actionable intelligence

IBM Privileged Identity Manager

- Sends privileged user details to correlate with user's activity

IBM Trusteer Apex

- Dynamically detect and block endpoint malware

IBM X-Force Research and Development

Defend against persistent attacks with integrated capabilities

Email with malicious link

X-Force Research

Network Protection XGS

- XGS blocks zero-day exploit from malicious link after incorporating X-Force security content
- XGS natively creates network flow activity for QRadar to detect additional anomalies

Security Event
Network Flow

SQL injection

Access Manager AMP 5100

- Access Manager blocks SQL injection from web application and alerts QRadar

AppScan

SiteProtector

Network Protection XGS

- Based on QRadar alert, analyst runs AppScan to find the application vulnerability
- AppScan creates virtual patch in SiteProtector to block the attack at the network level
- SiteProtector deploys policy to Network Protection XGS devices

Security Event

Privilege escalation

Privileged Identity Manager

- Privileged Identity Manager detects anomalous privilege escalation
- Privileged Identity Manager records the session and sends the escalation event to QRadar

Security Event

Email with malicious file

Trusteer Apex

- Apex detects and block the zero-day exploit using application state context

Security Event

IBM QRadar SIEM

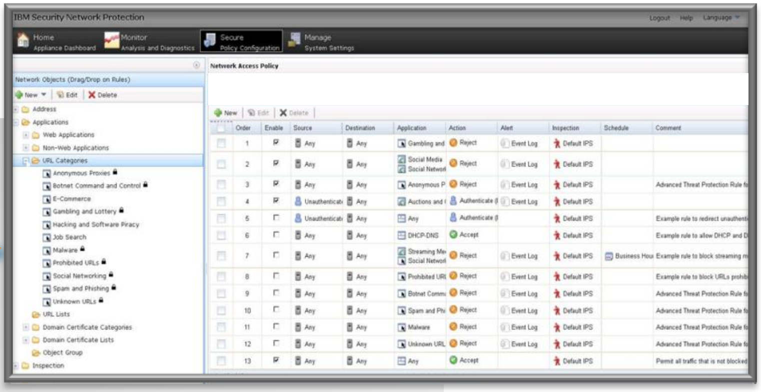
Investigate Alerts

- ✓ Event correlation
- ✓ Historic forensics
- ✓ Real-time analysis
- ✓ Predictive analytics

Incorporate the latest threat intelligence

IBM X-Force research is utilized in Network Protection XGS

1 Network Protection XGS console showing security policies



IBM Security Network Protection

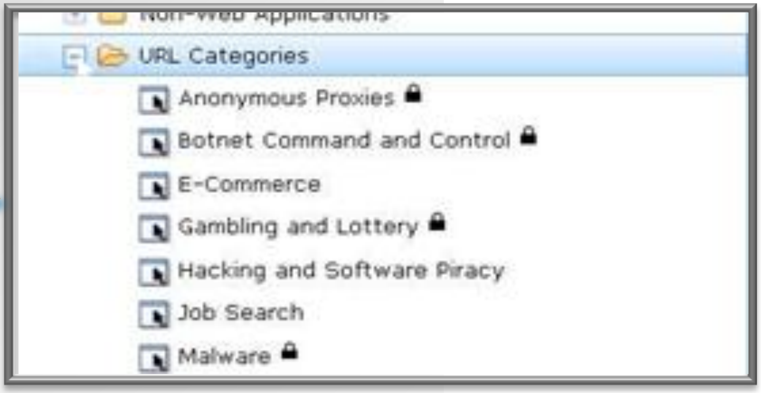
Network Objects (Drag/Drop on Rules)

- Address
- Applications
  - Web Applications
  - Non-Web Applications
  - URL Categories
    - Anonymous Proxies
    - Botnet Command and Control
    - E-Commerce
    - Gambling and Lottery
    - Hacking and Software Piracy
    - Job Search
    - Malware
    - Prohibited URLs
    - Social Networking
    - Spam and Phishing
    - Unknown URLs
  - URL Lists
  - Domain Certificate Categories
  - Domain Certificate Lists
  - Object Group
- Inspection

Network Access Policy

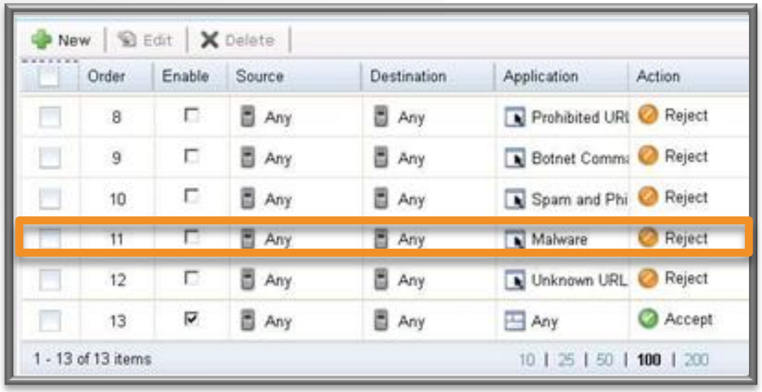
☐	Order	Enable	Source	Destination	Application	Action	Alert	Inspection	Schedule	Comment
☐	1	☑	Any	Any	Gambling and	Reject	Event Log	Default IPS		
☐	2	☑	Any	Any	Social Media Social Networ	Reject	Event Log	Default IPS		
☐	3	☑	Any	Any	Anonymous P	Reject	Event Log	Default IPS		Advanced Threat Protection Rule fo
☐	4	☑	Unauthenticat	Any	Auctions and	Authenticate (	Event Log	Default IPS		
☐	5	☐	Unauthenticat	Any	Any	Authenticate (		Default IPS		Example rule to redirect unauthenti
☐	6	☐	Any	Any	DHCP-DNS	Accept		Default IPS		Example rule to allow DHCP and D
☐	7	☐	Any	Any	Streaming Me Social Networ	Reject	Event Log	Default IPS	Business Hou	Example rule to block streaming m
☐	8	☐	Any	Any	Prohibited URI	Reject	Event Log	Default IPS		Example rule to block URLs prohib
☐	9	☐	Any	Any	Botnet Comm	Reject	Event Log	Default IPS		Advanced Threat Protection Rule fo
☐	10	☐	Any	Any	Spam and Phi	Reject	Event Log	Default IPS		Advanced Threat Protection Rule fo
☐	11	☐	Any	Any	Malware	Reject	Event Log	Default IPS		Advanced Threat Protection Rule fo
☐	12	☐	Any	Any	Unknown URL	Reject	Event Log	Default IPS		Advanced Threat Protection Rule fo
☐	13	☑	Any	Any	Any	Accept		Default IPS		Permit all traffic that is not blocked

2 X-Force URL reputation data incorporated by category



- Non-Web Applications
- URL Categories
  - Anonymous Proxies
  - Botnet Command and Control
  - E-Commerce
  - Gambling and Lottery
  - Hacking and Software Piracy
  - Job Search
  - Malware

3 Policy on XGS set to reject connections to malicious URLs



☐	Order	Enable	Source	Destination	Application	Action
☐	8	☐	Any	Any	Prohibited URI	Reject
☐	9	☐	Any	Any	Botnet Comm	Reject
☐	10	☐	Any	Any	Spam and Phi	Reject
☐	11	☐	Any	Any	Malware	Reject
☐	12	☐	Any	Any	Unknown URL	Reject
☐	13	☑	Any	Any	Any	Accept

1 - 13 of 13 items

Integrate to prevent web application exploits at the network level

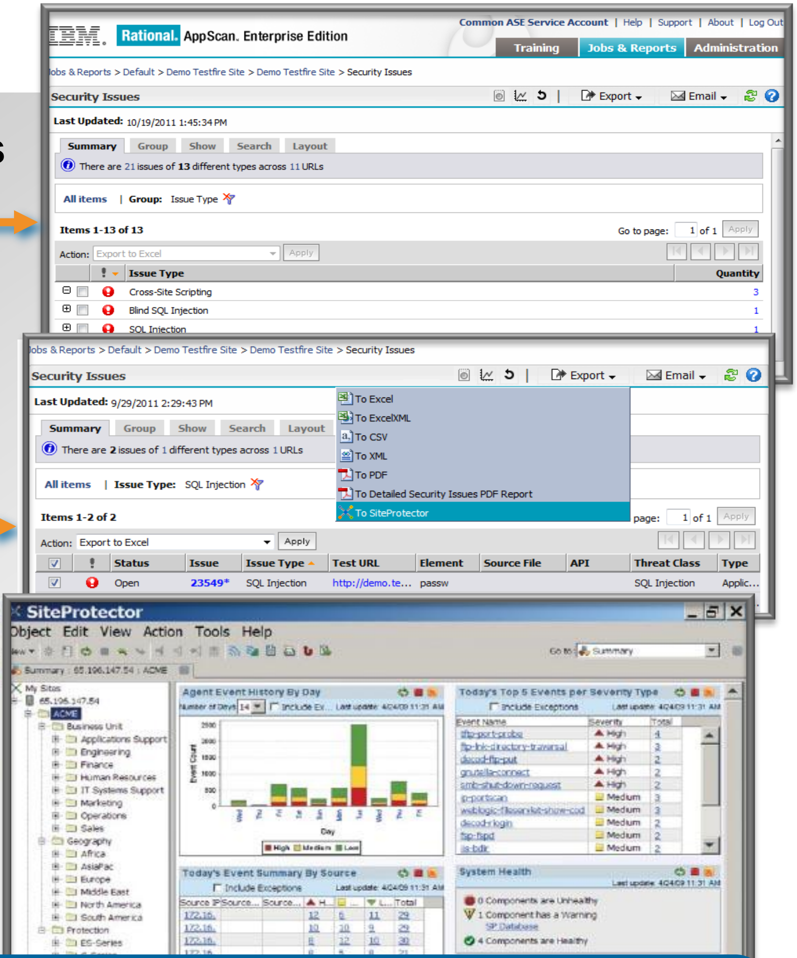
Access Manager flags a SQL injection, alerts QRadar and then…

1 Analyst runs AppScan and finds the SQL injection vulnerabilities

2 AppScan sends vulnerability details to SiteProtector

3 SiteProtector creates virtual patch to block the SQL injection at the network level while the vulnerabilities are patched

4 Policy deploys to Network Protection XGS devices



IBM. Rational. AppScan. Enterprise Edition

Common ASE Service Account | Help | Support | About | Log Out

Training | Jobs & Reports | Administration

Jobs & Reports > Default > Demo Testfire Site > Demo Testfire Site > Security Issues

Security Issues Export ▾ Email ▾

Last Updated: 10/19/2011 1:45:34 PM

Summary | Group | Show | Search | Layout

There are 21 issues of **13** different types across 11 URLs

All items | **Group:** Issue Type

Items 1-13 of 13 Go to page: 1 of 1 Apply

Action: Export to Excel Apply

	!	Issue Type	Quantity
⊟ ☐	●	Cross-Site Scripting	3
⊞ ☐	●	Blind SQL Injection	1
⊞ ☐	●	SQL Injection	1

Jobs & Reports > Default > Demo Testfire Site > Demo Testfire Site > Security Issues

Security Issues Export ▾ Email ▾

Last Updated: 9/29/2011 2:29:43 PM

Summary | Group | Show | Search | Layout

There are **2** issues of 1 different types across 1 URLs

All items | **Issue Type:** SQL Injection

Items 1-2 of 2 page: 1 of 1 Apply

Action: Export to Excel Apply

☑	!	Status	Issue	Issue Type	Test URL	Element	Source File	API	Threat Class	Type
☑	●	Open	23549*	SQL Injection	http://demo.te…	passw			SQL Injection	Applic…

SiteProtector

Event Name	Severity	Total
tftp-port-probe	High	4
ftp-link-directory-traversal	High	3
decod-ftp-put	High	2
gnutella-connect	High	2
smb-shut-down-request	High	2
ip-portscan	Medium	3
weblogic-fileservlet-show-code	Medium	3
decod-rlogin	Medium	2
ftp-ftpd	Medium	2
is-bdir	Medium	2

Source IP	Source…	Source…	H…	…	L…	Total
172.16.			12	6	11	29
172.16.			10	10	9	29
172.16.			8	12	10	30

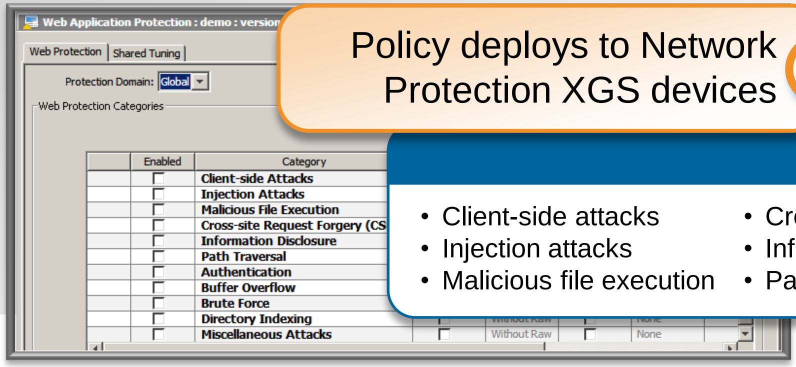
Last update: 4/24/09 11:31 AM

0 Components are Unhealthy

1 Component has a Warning

SP Database

4 Components are Healthy



Web Application Protection : demo : version

Web Protection | Shared Tuning

Protection Domain: Global

Web Protection Categories

	Enabled	Category				
	☐	Client-side Attacks				
	☐	Injection Attacks				
	☐	Malicious File Execution				
	☐	Cross-site Request Forgery (CS				
	☐	Information Disclosure				
	☐	Path Traversal				
	☐	Authentication				
	☐	Buffer Overflow				
	☐	Brute Force				
	☐	Directory Indexing	☐	Without Raw	☐	None
	☐	Miscellaneous Attacks	☐	Without Raw	☐	None

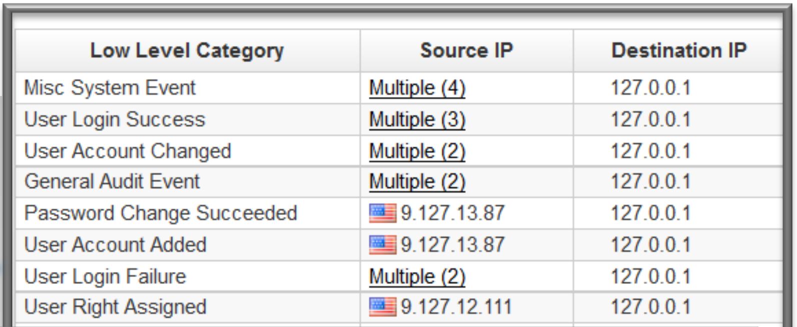
Types of Protection

- Client-side attacks
- Injection attacks
- Malicious file execution
- Cross-site request forgery
- Information disclosure
- Path traversal
- Authentication
- Buffer overflow
- Brute force
- Directory indexing
- Miscellaneous attacks

Monitor privileged users to detect malicious activity

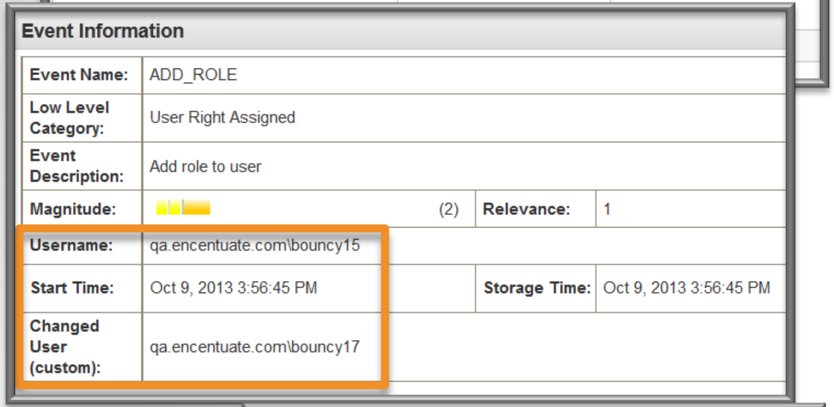
An attacker steals system administrator login credentials then grants increased permissions to invalid user

1 Privileged Identify Manager sends QRadar details of the privilege escalation



Low Level Category	Source IP	Destination IP
Misc System Event	Multiple (4)	127.0.0.1
User Login Success	Multiple (3)	127.0.0.1
User Account Changed	Multiple (2)	127.0.0.1
General Audit Event	Multiple (2)	127.0.0.1
Password Change Succeeded	9.127.13.87	127.0.0.1
User Account Added	9.127.13.87	127.0.0.1
User Login Failure	Multiple (2)	127.0.0.1
User Right Assigned	9.127.12.111	127.0.0.1

2 QRadar notifies a security analyst



Event Information

Event Name:	ADD_ROLE		
Low Level Category:	User Right Assigned		
Event Description:	Add role to user		
Magnitude:	▨ (2)	Relevance:	1
Username:	qa.encentuate.com\bouncy15		
Start Time:	Oct 9, 2013 3:56:45 PM	Storage Time:	Oct 9, 2013 3:56:45 PM
Changed User (custom):	qa.encentuate.com\bouncy17		

3 Security analyst views a recording that shows compromised administrator granting a user rights outside of the formal process

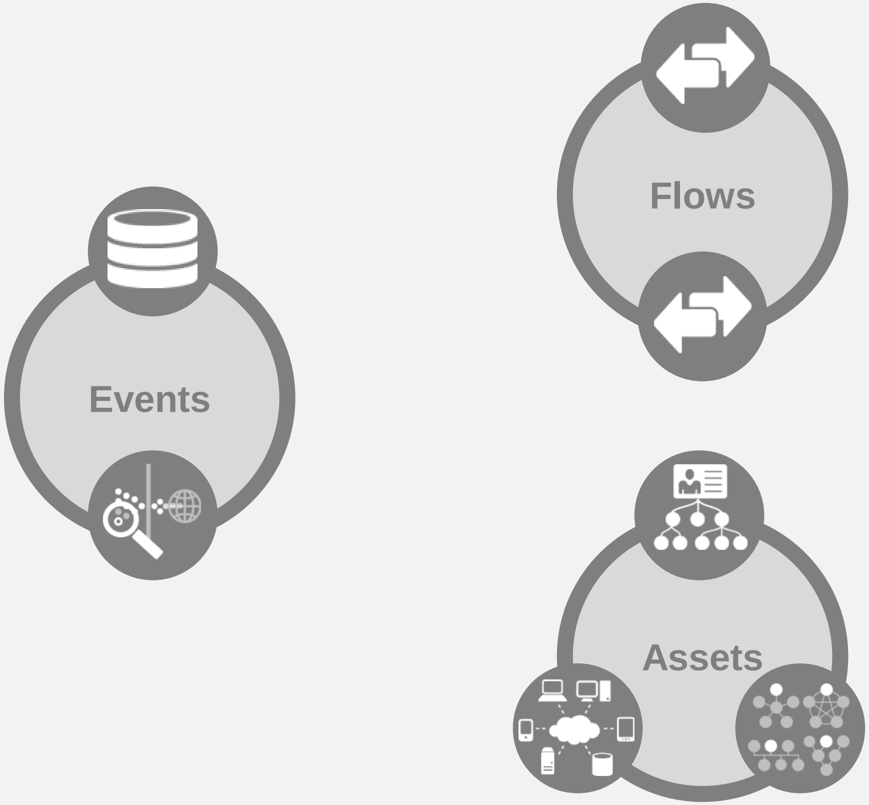
Security analyst revokes compromised account access to prevent further malicious action

Security analysis is a big data problem

Security analysts are overwhelmed by a variety of data and lack of visibility

Integrated Defense Strategy

HARDEN › DETECT › ANALYZE



Analyze challenges:

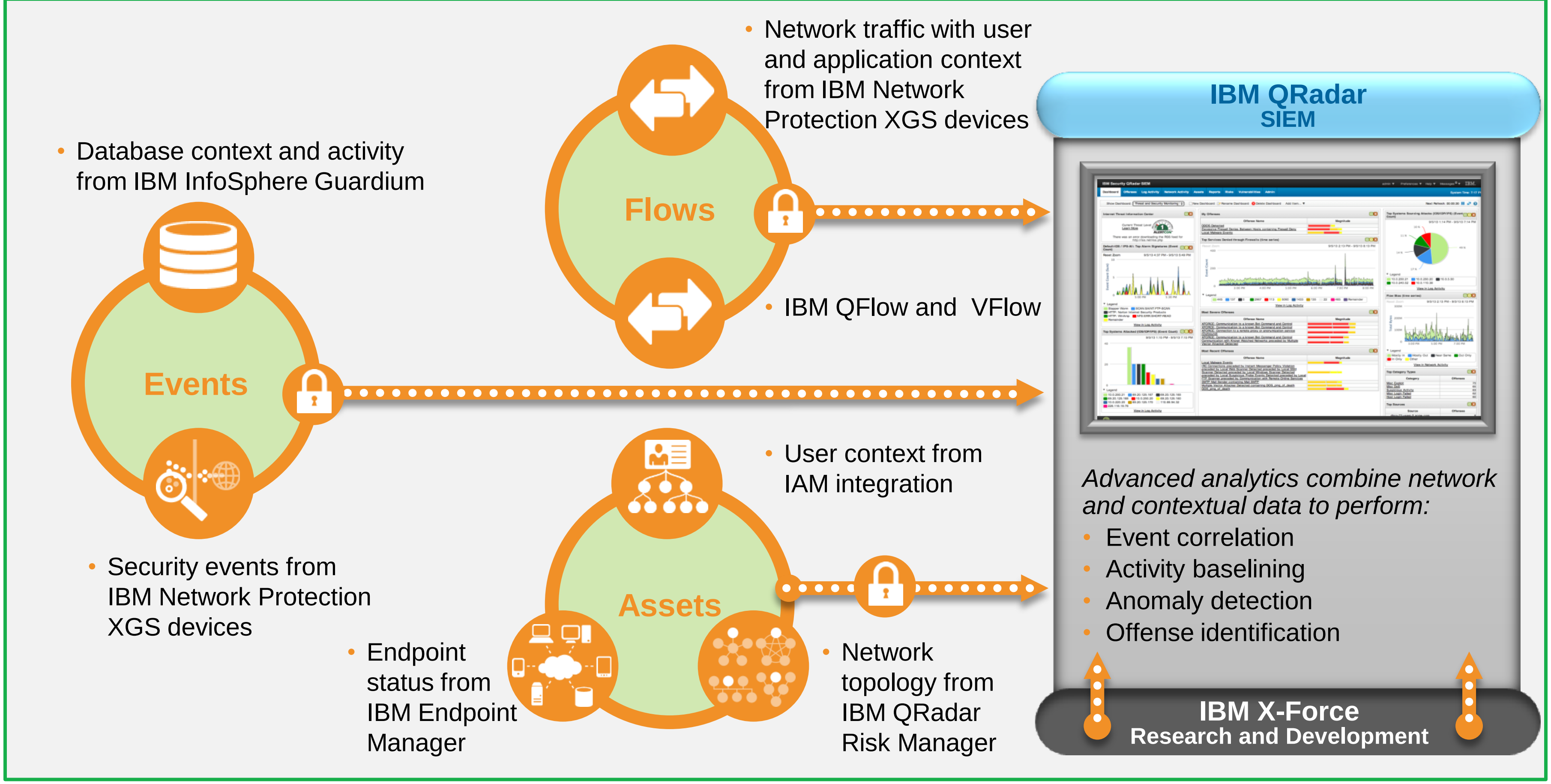
- Rapid growth in the volume of security data
- Incompatible information from diverse data sources
- Multiple, siloed security systems each with its own dashboard
- Lack of application, configuration and user context

Integrated IBM solutions provide actionable security intelligence

QRadar SIEM correlates and analyzes millions of events with contextual data to produce a detailed view of key offenses

Integrated Defense Strategy

HARDEN → DETECT → **ANALYZE**



- Network traffic with user and application context from IBM Network Protection XGS devices
- IBM QFlow and VFlow
- Database context and activity from IBM InfoSphere Guardium
- Security events from IBM Network Protection XGS devices
- User context from IAM integration
- Endpoint status from IBM Endpoint Manager
- Network topology from IBM QRadar Risk Manager

Advanced analytics combine network and contextual data to perform:

- Event correlation
- Activity baselining
- Anomaly detection
- Offense identification

Correlate events across security domains to gain visibility

Security Event	User connects from country where company does not do business	IAM
Security Event	User accesses database outside normal business hours	Guardium
Security Event	Unusual network traffic identified	XGS

1 → **IBM QRadar SIEM**

QRadar correlates 3 security events and triggers an offense

2

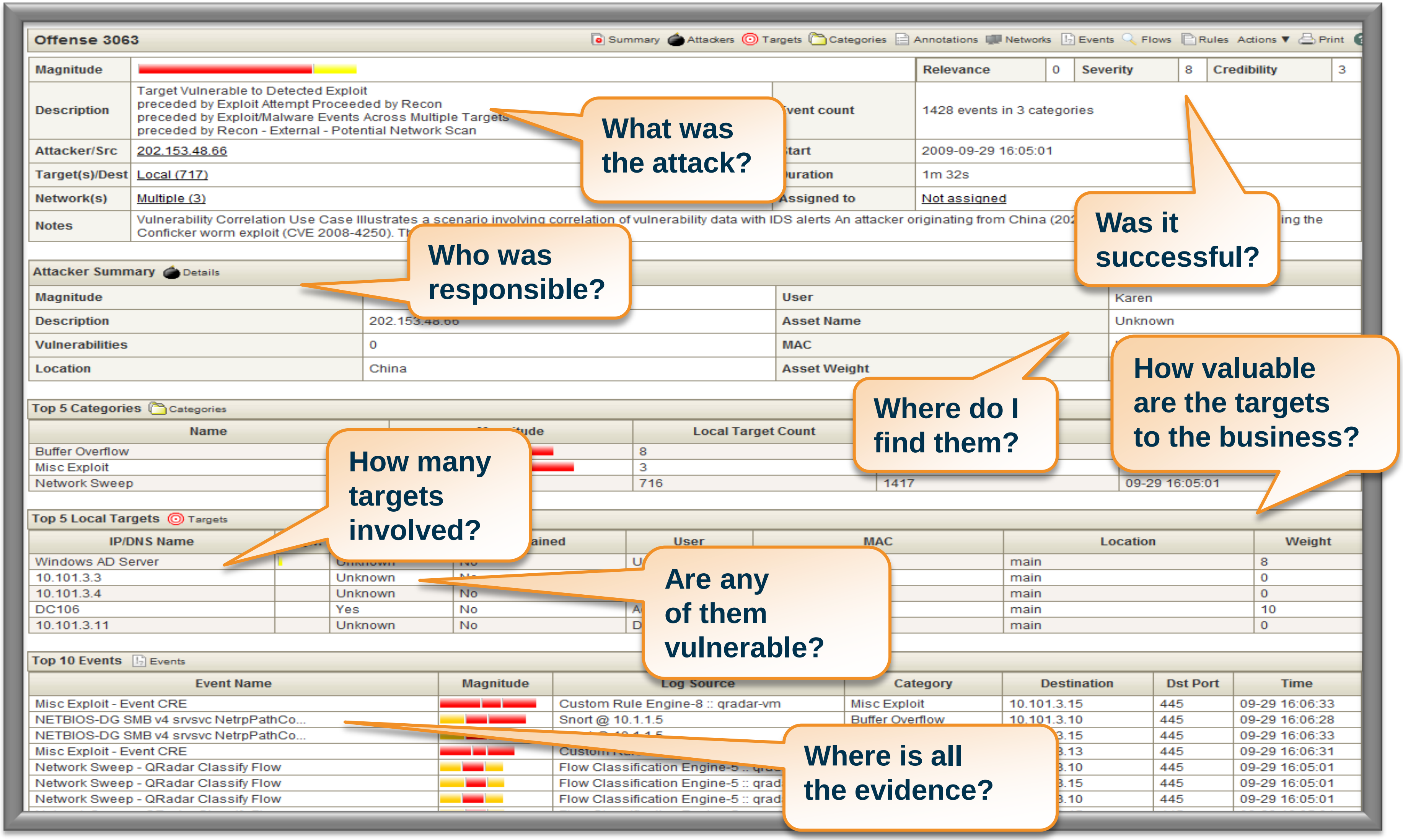
	Investigations…	***Results…***
IAM	Look for recent changes in the user's permissions	User requested access to sensitive DB
XGS	Lookup all activity from user's IP address	6 days ago, the user connected to an unknown IP located in a suspicious region 5 days ago, the user's machine began opening suspicious connections
QFlow	Find other users who connected to the same suspicious IP	3 other users have connected with similar suspicious traffic
Guardium	Determine which DBs and records these users accessed in last 6 days	Users accessed unannounced quarterly financial results
Endpoint Manager	Check patch status of compromised machines	All compromised users have latest browser patches

3

Remediation

- Update XGS to block malware command and control
- Alert security team to remove the endpoint malware
- Produce sensitive data access report

QRadar integrates data to answer the important questions



Offense 3063

Magnitude			Relevance	0	Severity	8	Credibility 3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan	vent count	1428 events in 3 categories				
Attacker/Src	202.153.48.66	tart	2009-09-29 16:05:01				
Target(s)/Dest	Local (717)	uration	1m 32s				
Network(s)	Multiple (3)	Assigned to	Not assigned				
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with IDS alerts An attacker originating from China (202 … ing the Conficker worm exploit (CVE 2008-4250). Th						

Attacker Summary Details

Magnitude		User	Karen
Description	202.153.48.66	Asset Name	Unknown
Vulnerabilities	0	MAC	
Location	China	Asset Weight	

Top 5 Categories Categories

Name	Magnitude	Local Target Count		
Buffer Overflow		8		
Misc Exploit		3		
Network Sweep		716	1417	09-29 16:05:01

Top 5 Local Targets Targets

IP/DNS Name			ained	User	MAC	Location	Weight
Windows AD Server		Unknown	No	U		main	8
10.101.3.3		Unknown	No			main	0
10.101.3.4		Unknown	No			main	0
DC106		Yes	No	A		main	10
10.101.3.11		Unknown	No	D		main	0

Top 10 Events Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm	Misc Exploit	10.101.3.15	445	09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5	Buffer Overflow	10.101.3.10	445	09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...				3.15	445	09-29 16:06:33
Misc Exploit - Event CRE		Custom		3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qra		3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qrad		3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qrad		3.10	445	09-29 16:05:01

What was the attack?

Was it successful?

Who was responsible?

How valuable are the targets to the business?

Where do I find them?

How many targets involved?

Are any of them vulnerable?

Where is all the evidence?