IBMSecuritySymposium

Intelligence | Integration | Expertise

Compliance and Audit: Cornerstones of a Secure Organization

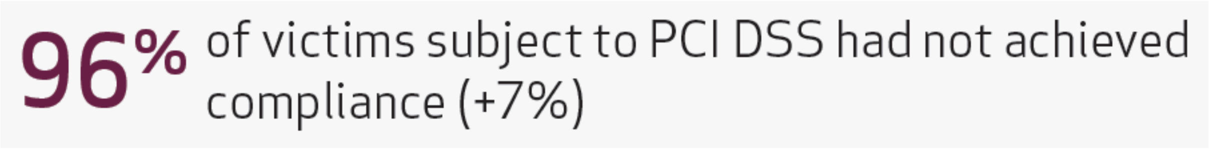
Jon Fraleigh, Senior Vice President of Worldwide Sales for Q1 Labs, an IBM Company

23 August 2012

Agenda

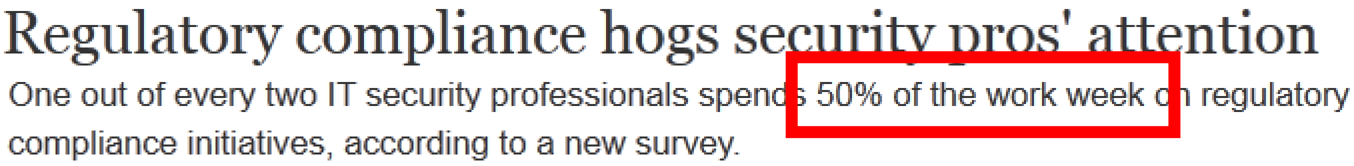
- The Challenges of Compliance and Security Management
- Introducing Security Intelligence
- Solving Compliance and Security Challenges with QRadar
- Next Steps

Compliance Remains a Huge Challenge – and Risk



96% of victims subject to PCI DSS had not achieved compliance (+7%)

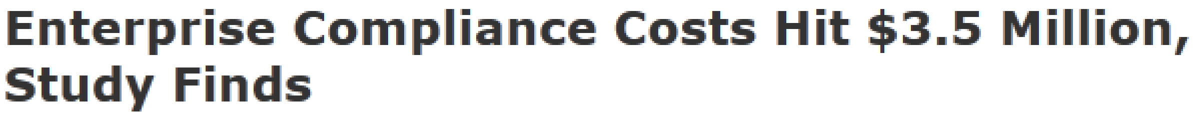
– Verizon 2012 Data Breach Investigations Report



Regulatory compliance hogs security pros' attention

One out of every two IT security professionals spends 50% of the work week on regulatory compliance initiatives, according to a new survey.

– Network World, December 2010



Enterprise Compliance Costs Hit $3.5 Million, Study Finds

– eWeek, January 2011

Key Business Drivers for Information Security and Compliance

Protect sensitive customer data, financial data and intellectual property from unauthorized access by:

- Outsiders such as cyber-criminals, hackers and foreign nations
- Insiders such as administrators, contractors and end users

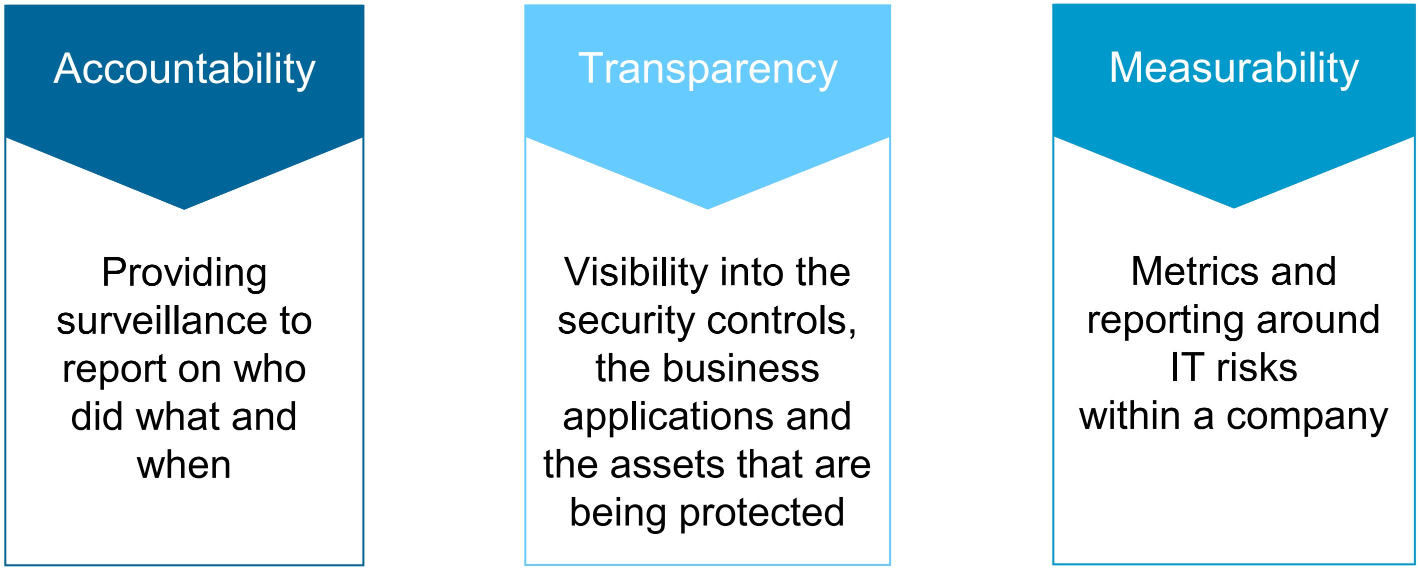
Reduce compliance cost and effort

- Manual processes to collect and analyze data
- Too much data to analyze effectively
- Siloed data sets that don’t provide unified view

Support new IT and business initiatives such as virtualization, cloud computing, mobile computing and more

The Compliance Imperative

- Companies today are under growing pressure to comply with regulations such as SOX, PCI and many more
- *Compliance is more than simply generating reports*
- 3 key factors need to be fulfilled:



Accountability

Providing surveillance to report on who did what and when

Transparency

Visibility into the security controls, the business applications and the assets that are being protected

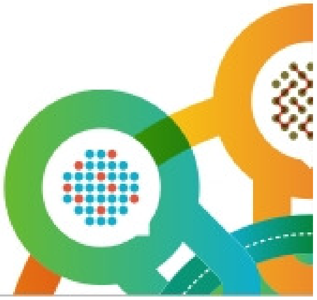
Measurability

Metrics and reporting around IT risks within a company

Challenge: How to Effectively Assess Risk

Assessing information risk spans many areas:

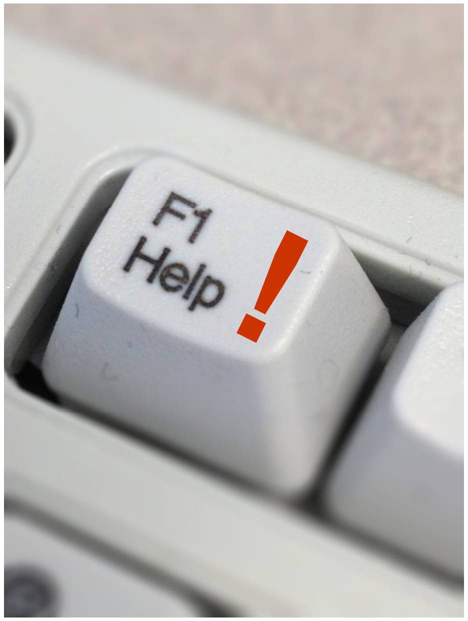
- Log management, SIEM, network analytics, anomaly detection, data management, etc.
- Configuration management
  - Many successful attacks are a result of poor configuration
  - Configuration audits are labor intensive and time consuming
  - Configuration files are inconsistent across vendor and product type
  - Required by most regulations
- Vulnerability Assessment
  - VA scanners lack full network context, leading to poor prioritization
  - Required by most regulations



Most home-built and older solutions are costly and ineffective

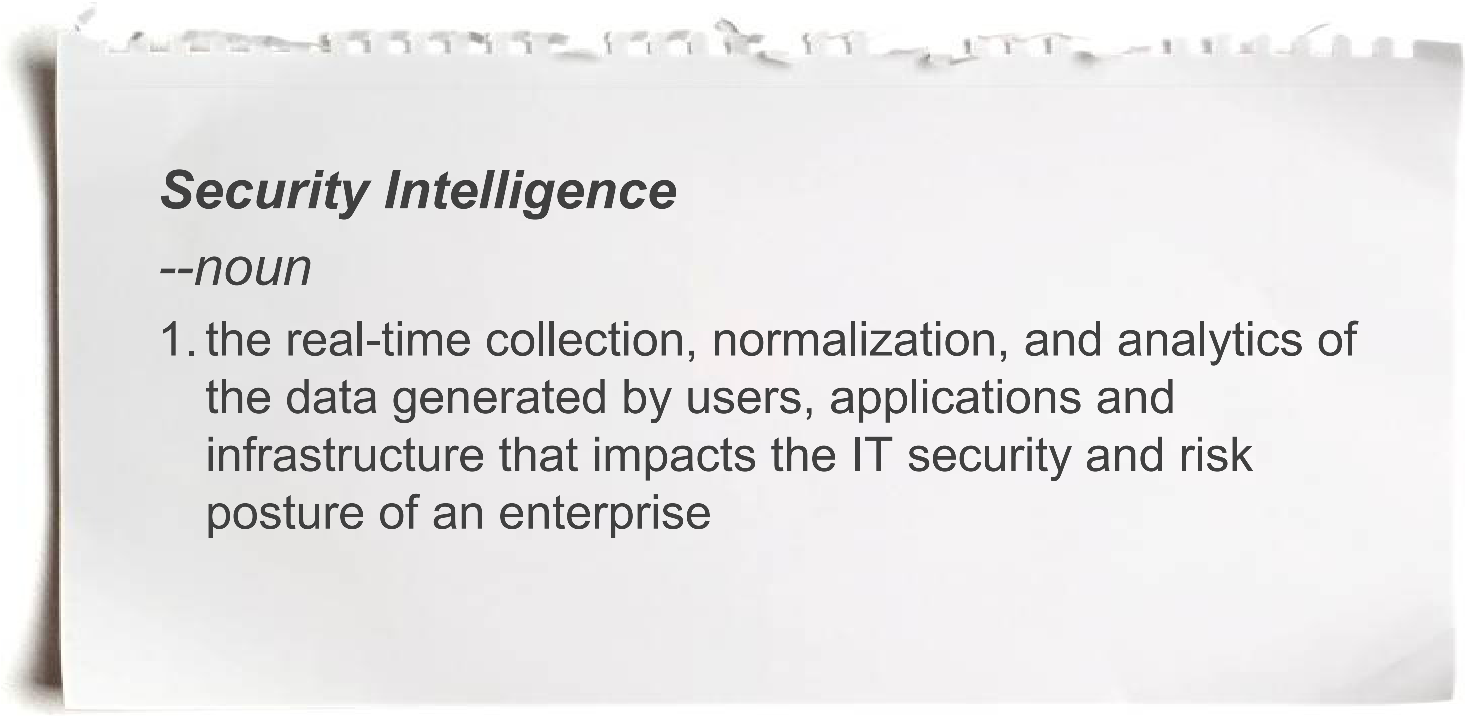
Disadvantages of Outdated Solutions:

- Significant cost to collect data, integrate systems, create and update reports, and monitor risks
- Cost and effort to manage massive amounts of data for reporting and monitoring
- No real time visibility
- No proactive intelligence or alerting
- Audit trail not secure since logging can sometimes be disabled



Introducing Security Intelligence

What is Security Intelligence?



Security Intelligence

--noun

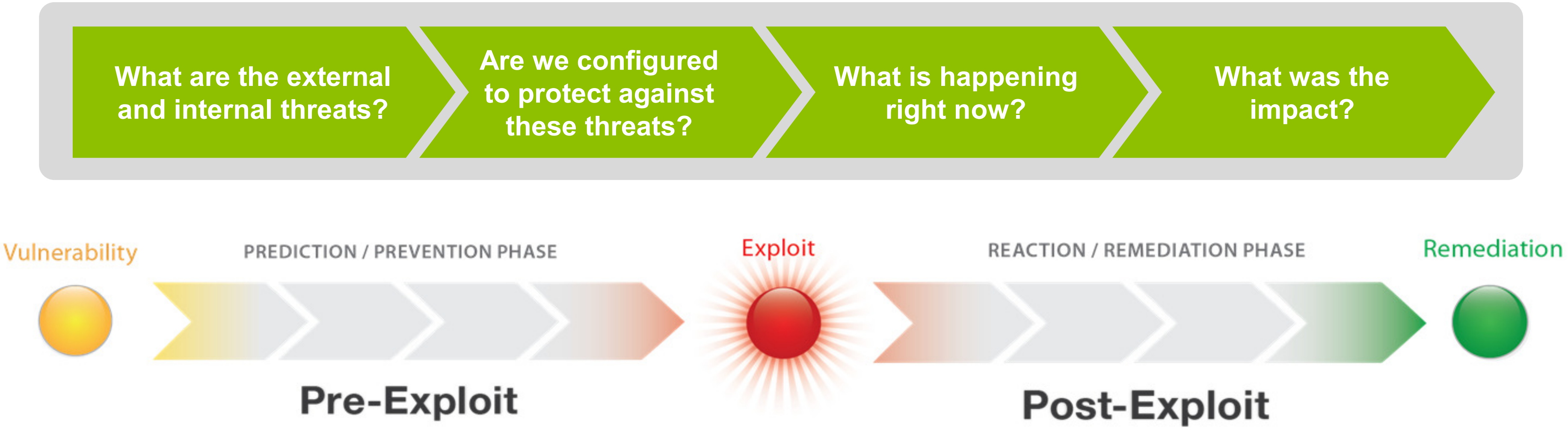
1. the real-time collection, normalization, and analytics of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise

Security Intelligence provides actionable insight for managing compliance and security, from detection to investigation and reporting

How Security Intelligence Can Help

- Continuously monitor all activity and identify risks in real-time
- Gain *visibility and insight* into unauthorized or anomalous activities
  - Unusual access of PCI or SOX servers – compliance violation?
  - Unusual Windows service – backdoor or spyware program?
  - Spike in download volume from SharePoint server – suspicious access?
  - High number of failed logins to key servers – brute-force password attack?
  - Unexpected configuration change – enabling data exfiltration?

Compliance and Security Intelligence Timeline



What are the external and internal threats?

Are we configured to protect against these threats?

What is happening right now?

What was the impact?

Vulnerability

PREDICTION / PREVENTION PHASE

Exploit

REACTION / REMEDIATION PHASE

Remediation

Pre-Exploit

Post-Exploit

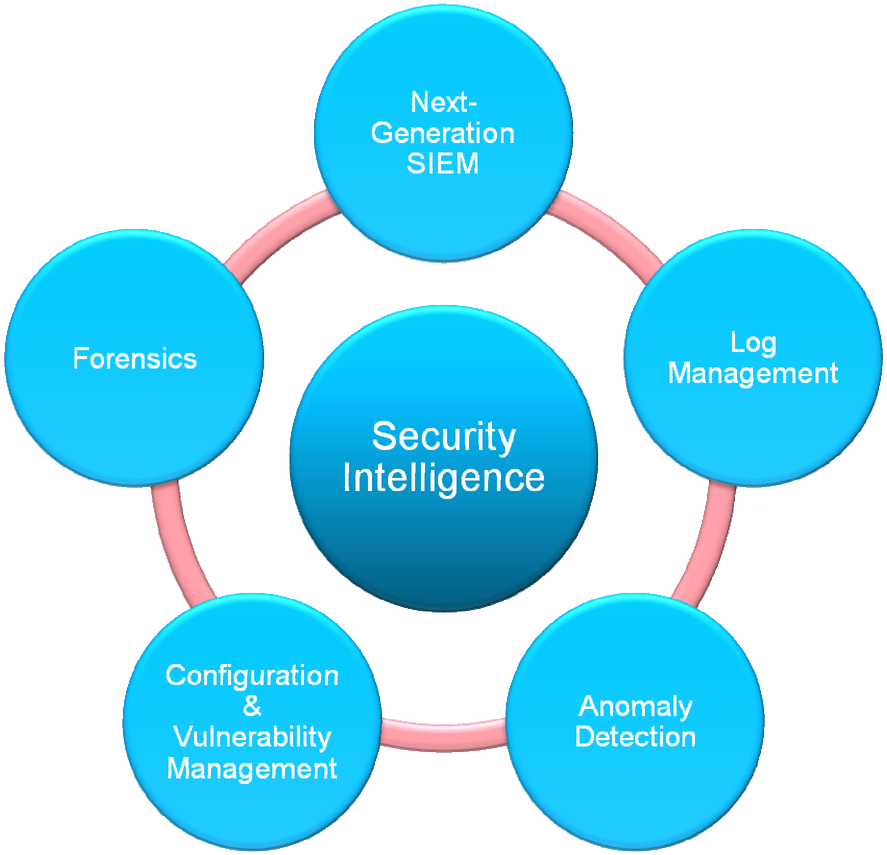
Prediction & Prevention

Risk Management. Vulnerability Management.
Configuration Monitoring. Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

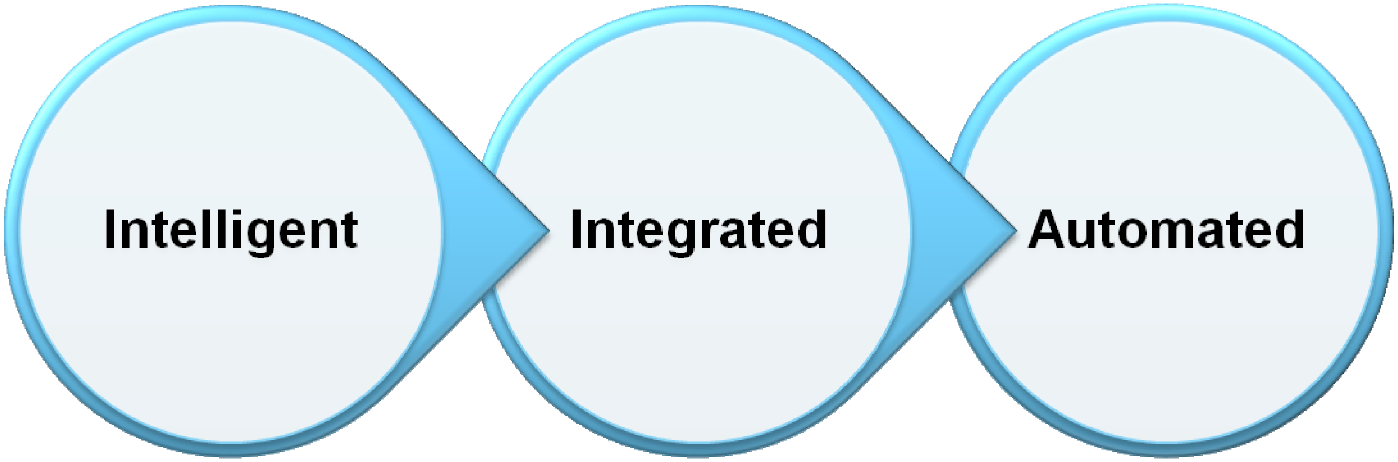
Reaction & Remediation

SIEM. Log Management. Incident Response.
Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Loss Prevention.

Security Intelligence Integrates Familiar Approaches

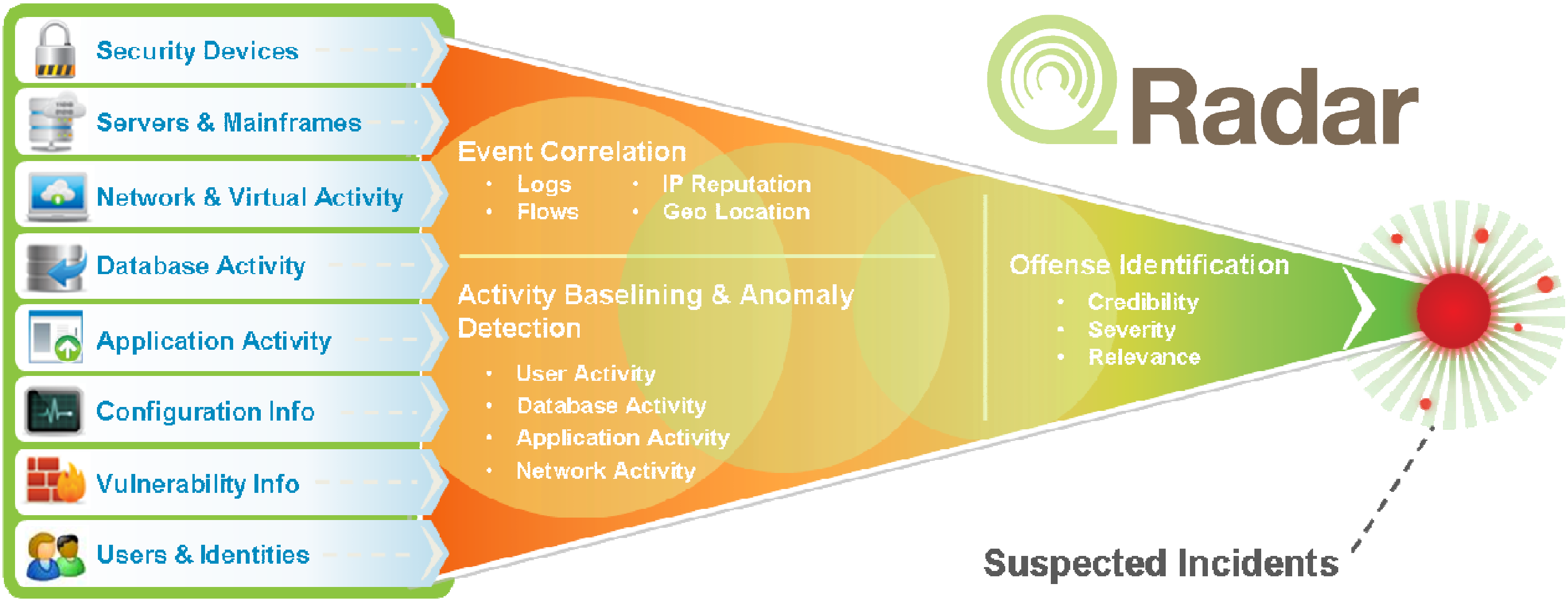


The Three Principles of Security Intelligence



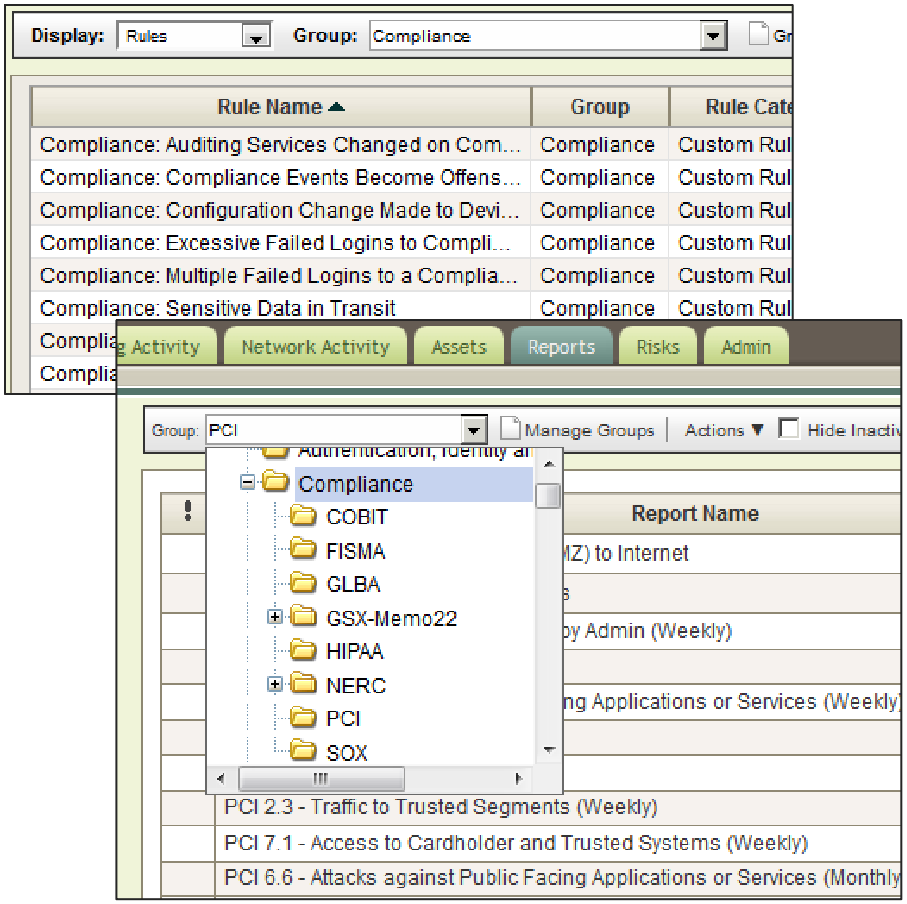
Solving Compliance and Security Challenges with QRadar

Context and Correlation Lead to Deep Insight



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

Automating Compliance Operations



Display: Rules Group: Compliance Gr

Rule Name ▲	Group	Rule Cate
Compliance: Auditing Services Changed on Com...	Compliance	Custom Rul
Compliance: Compliance Events Become Offens...	Compliance	Custom Rul
Compliance: Configuration Change Made to Devi...	Compliance	Custom Rul
Compliance: Excessive Failed Logins to Compli...	Compliance	Custom Rul
Compliance: Multiple Failed Logins to a Complia...	Compliance	Custom Rul
Compliance: Sensitive Data in Transit	Compliance	Custom Rul
Complia		
Complia		

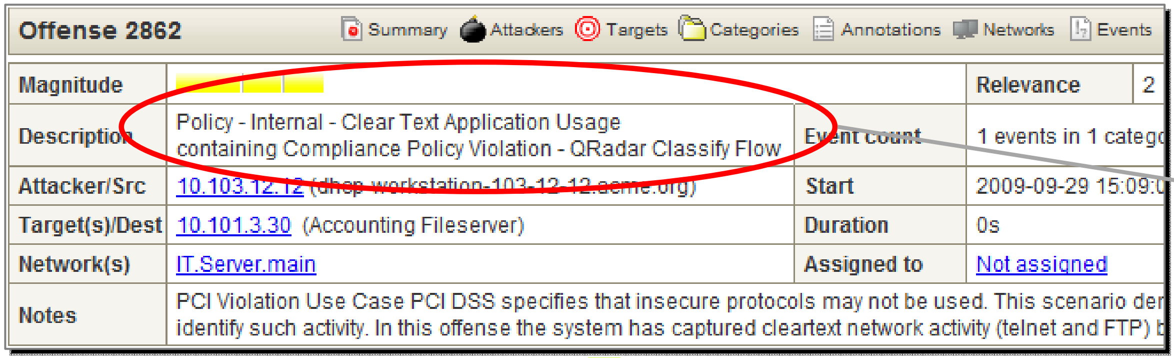
Group: PCI

- Authentication, Identity an
- Compliance
  - COBIT
  - FISMA
  - GLBA
  - GSX-Memo22
  - HIPAA
  - NERC
  - PCI
  - SOX

!	Report Name
	IZ) to Internet
	s
	by Admin (Weekly)
	ng Applications or Services (Weekly)
	PCI 2.3 - Traffic to Trusted Segments (Weekly)
	PCI 7.1 - Access to Cardholder and Trusted Systems (Weekly)
	PCI 6.6 - Attacks against Public Facing Applications or Services (Monthly

- Out-of-the-box templates for specific regulations and best practices:
  - PCI, COBIT, SOX and more
- Easily modified to include new definitions
- Extensible to include new regulations and best practices
- Leverage existing correlation rules

Proactive Compliance Monitoring
Compliance is not just reporting

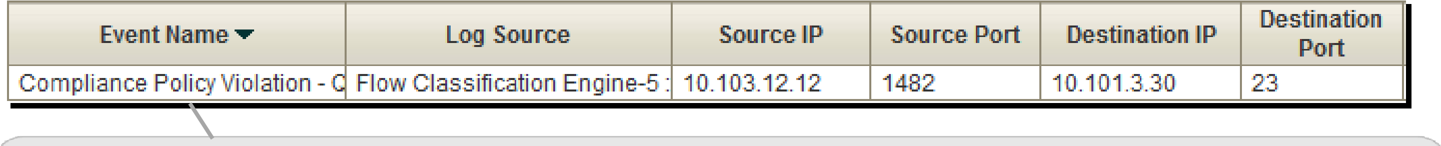


Offense 2862

Magnitude		Relevance	2
Description	Policy - Internal - Clear Text Application Usage containing Compliance Policy Violation - QRadar Classify Flow	Event count	1 events in 1 catego
Attacker/Src	10.103.12.12 (dhcp-workstation-103-12-12.acme.org)	Start	2009-09-29 15:09:0
Target(s)/Dest	10.101.3.30 (Accounting Fileserver)	Duration	0s
Network(s)	IT.Server.main	Assigned to	Not assigned
Notes	PCI Violation Use Case PCI DSS specifies that insecure protocols may not be used. This scenario der identify such activity. In this offense the system has captured cleartext network activity (telnet and FTP) b		

PCI compliance at risk?

Real-time detection of possible violation



Event Name	Log Source	Source IP	Source Port	Destination IP	Destination Port
Compliance Policy Violation - C	Flow Classification Engine-5 :	10.103.12.12	1482	10.101.3.30	23

Unencrypted Traffic

QRadar QFlow saw a cleartext service running on the Accounting server

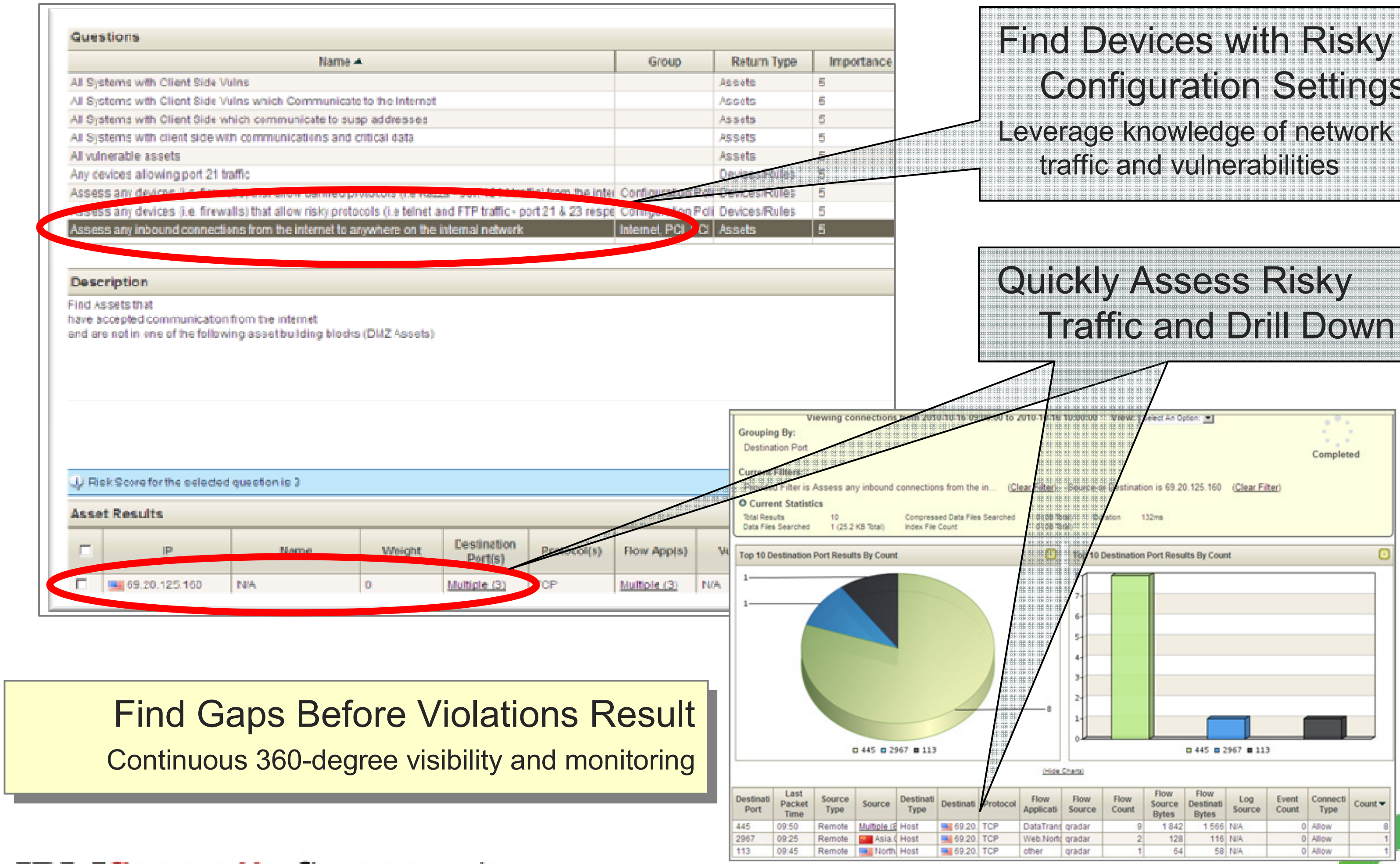
PCI Requirement 4 states: Encrypt transmission of cardholder data across open, public networks

Compliance Simplified

Out-of-the-box support for major compliance and regulatory standards

Automated reports, pre-defined correlation rules and dashboards

Configuration and Vulnerability Monitoring for Compliance



Questions

Name ▲	Group	Return Type	Importance
All Systems with Client Side Vulns		Assets	5
All Systems with Client Side Vulns which Communicate to the Internet		Assets	5
All Systems with Client Side which communicate to susp addresses		Assets	5
All Systems with client side with communications and critical data		Assets	5
All vulnerable assets		Assets	5
Any devices allowing port 21 traffic		Devices/Rules	5
Assess any devices (i.e. firewalls) that allow banned protocols (i.e Kazaa - port 1214 traffic) from the inte	Configuration Poli	Devices/Rules	5
Assess any devices (i.e. firewalls) that allow risky protocols (i.e telnet and FTP traffic - port 21 & 23 respe	Configuration Poli	Devices/Rules	5
Assess any inbound connections from the internet to anywhere on the internal network	Internet, PCI, PCI	Assets	5

Description

Find Assets that
have accepted communication from the internet
and are not in one of the following asset building blocks (DMZ Assets)

Risk Score for the selected question is 3

Asset Results

□	IP	Name	Weight	Destination Port(s)	Protocol(s)	Flow App(s)	Vu
□	69.20.125.160	N/A	0	Multiple (3)	TCP	Multiple (3)	N/A

Viewing connections from 2010-10-16 09:00:00 to 2010-10-16 10:00:00 View: Select An Option:

Grouping By:
Destination Port

Completed

Current Filters:
Provided Filter is Assess any inbound connections from the in... (Clear Filter) Source or Destination is 69.20.125.160 (Clear Filter)

Current Statistics

Total Results	10	Compressed Data Files Searched	0 (0B Total)	Duration	132ms
Data Files Searched	1 (25.2 KB Total)	Index File Count	0 (0B Total)		

Top 10 Destination Port Results By Count
1
1
8
445
2967
113
Top 10 Destination Port Results By Count
0
1
2
3
4
5
6
7
445
2967
113
(Hide Charts)

Destinati Port	Last Packet Time	Source Type	Source	Destinati Type	Destinati	Protocol	Flow Applicati	Flow Source	Flow Count	Flow Source Bytes	Flow Destinati Bytes	Log Source	Event Count	Connecti Type	Count ▾
445	09:50	Remote	Multiple (8	Host	69.20.	TCP	DataTrans	qradar	9	1 842	1 566	N/A	0	Allow	8
2967	09:25	Remote	Asia.(	Host	69.20.	TCP	Web.Nortc	qradar	2	128	116	N/A	0	Allow	1
113	09:45	Remote	North.	Host	69.20.	TCP	other	qradar	1	64	58	N/A	0	Allow	1

Find Devices with Risky Configuration Settings

Leverage knowledge of network traffic and vulnerabilities

Quickly Assess Risky Traffic and Drill Down

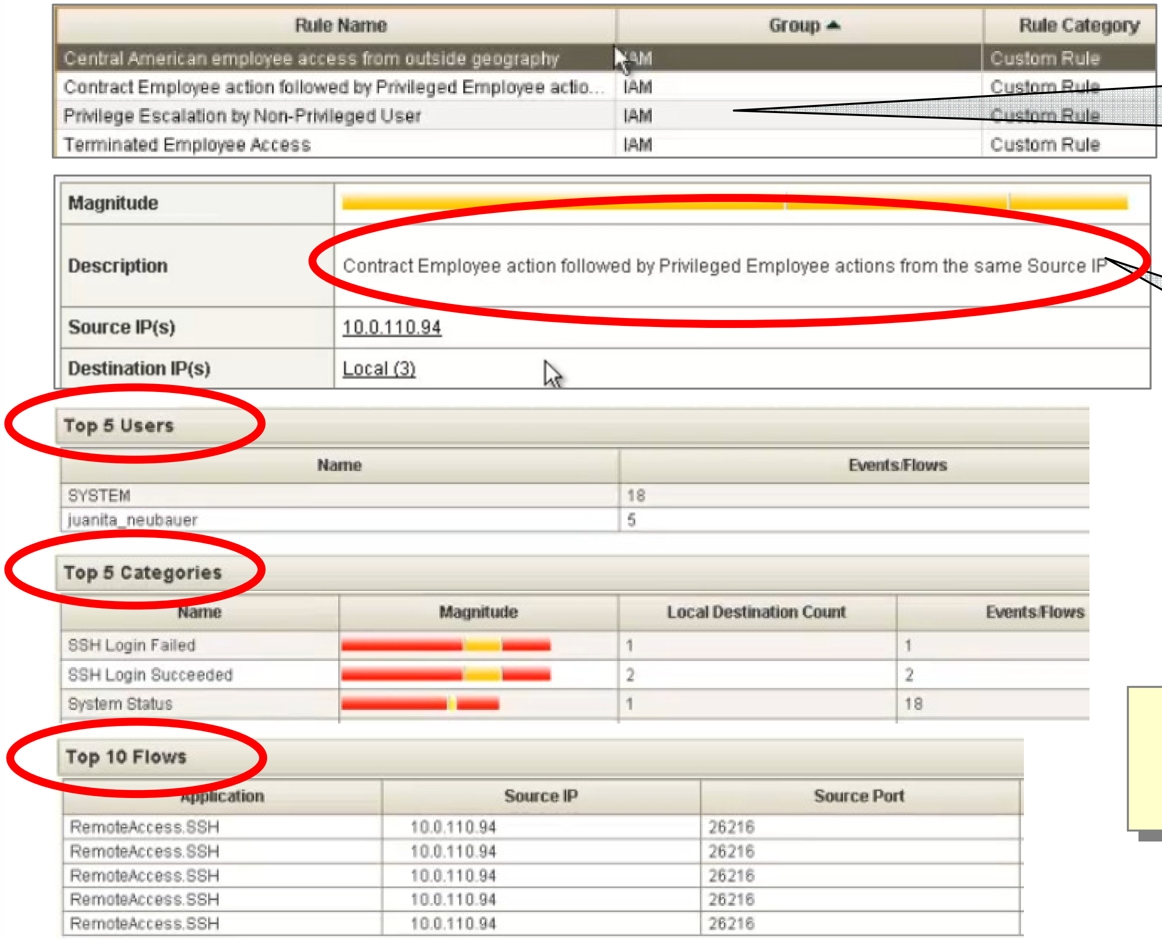
Find Gaps Before Violations Result

Continuous 360-degree visibility and monitoring

IBMSecuritySymposium

Intelligence | Integration | Expertise

User Activity Monitoring



Rule Name	Group ▲	Rule Category
Central American employee access from outside geography	IAM	Custom Rule
Contract Employee action followed by Privileged Employee actio...	IAM	Custom Rule
Privilege Escalation by Non-Privileged User	IAM	Custom Rule
Terminated Employee Access	IAM	Custom Rule

Magnitude	
Description	Contract Employee action followed by Privileged Employee actions from the same Source IP
Source IP(s)	10.0.110.94
Destination IP(s)	Local (3)

Top 5 Users

Name	Events/Flows
SYSTEM	18
juanita_neubauer	5

Top 5 Categories

Name	Magnitude	Local Destination Count	Events/Flows
SSH Login Failed		1	1
SSH Login Succeeded		2	2
System Status		1	18

Top 10 Flows

Application	Source IP	Source Port
RemoteAccess.SSH	10.0.110.94	26216
RemoteAccess.SSH	10.0.110.94	26216
RemoteAccess.SSH	10.0.110.94	26216
RemoteAccess.SSH	10.0.110.94	26216
RemoteAccess.SSH	10.0.110.94	26216

Integration with Identity & Access Management

Knowledge of user roles

Detect Suspicious Activity

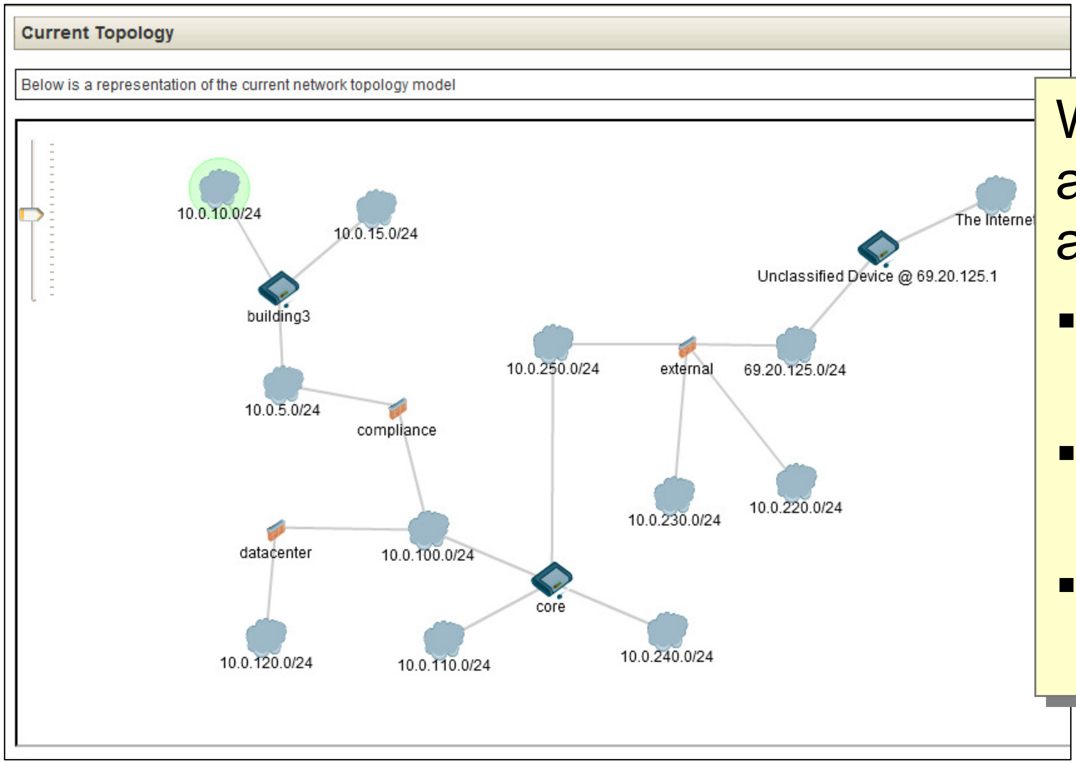
Why is a privileged user taking action from a contractor's system?

Full Visibility at Your Fingertips

All Information Readily Available

Managing Risk Efficiently with Automated Monitoring and Full Visibility

Know Your Environment ❖ Identify Your Risks ❖ Prioritize Your Actions



Current Topology

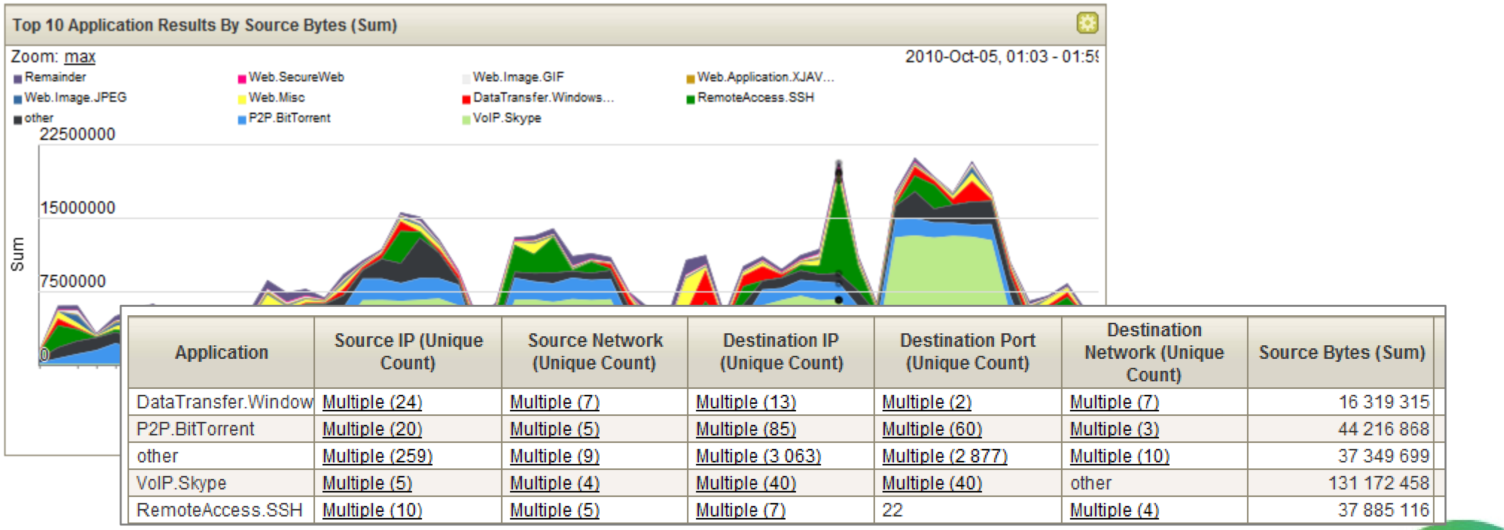
Below is a representation of the current network topology model

With full visibility and sophisticated analytics, you can:

- Focus on the risks that matter
- Enforce policies with automation
- Perform “what-if” scenarios

Network Analysis for Deep Intelligence

- **Network traffic doesn't lie.** Attackers can stop logging and erase their tracks, but can't cut off the network (flow data)
  - Deep packet inspection for Layer 7 flow data
  - Pivoting and data mining for advanced detection and forensics
- Helps detect anomalies that might otherwise get missed
- Enables visibility into attacker communications



Top 10 Application Results By Source Bytes (Sum)

Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116

European Payments Processor Achieves PCI Compliance in 4 Weeks

Value

- **Integrated solution protects critical data while supporting compliance with PCI, SOX and others**
- **Expert implementation services based on decades of financial industry experience**
- **Client passed PCI audit 4 weeks after purchase**

Business Challenge

- Protect client data at the heart of this business
- PCI compliance for processing of US$25 billion in annual transactions
- Rapidly implement proven solution; zero tolerance for delays or errors

Solution

QRadar SIEM, IBM Network IPS

- Integrated solution to provide visibility into PCI and data exposure risks
- Secure log archiving, intrusion detection, and file integrity monitoring
- Monitors products from McAfee, Cisco, Oracle, Microsoft & many others

QRadar Advantages

- Deployed quickly, using proven products and expert services
- Easy to customize, for future business needs and growth

IBMSecuritySymposium

Intelligence | Integration | Expertise

Fortune 100 Healthcare Organization Builds a Scalable Strategy for Threat Detection and Prevention

Value

- **SIEM solution helps pinpoint detection of security threats while ensuring compliance with PCI, SOX, HIPAA and FDA**
- **Integrate 100s of data sources and expand capacity as needed**
- **Deployed into production in 60 days, using only 37 professional services days and 2 weeks of training**

> *"Humans can't detect abnormal activity.*
>
> *QRadar can."*

Business Challenge

- Detect and remediate wide range of security threats and compliance & fraud risks
- Intelligently automate manual investigations
- Gain massive scalability for current and future needs; starting at 160,000 EPS today

Solution

QRadar SIEM, QRadar QFlow

- Real-time correlation of hundreds of data sources
- Hundreds of out-of-the-box reports and rules for compliance and security
- Automated data gathering and intelligent user interface

QRadar Advantages

- Deployed quickly, unlike alternative product which needed US$3M to implement
- Highly scalable architecture, able to perform very well in a large, distributed environment

Financial Information Provider Uses Anomaly Detection to Identify Fraud and Security Threats

IBM

Value

- **Next-generation SIEM uses advanced behavioral analysis to protect against fraud and network threats**
- **Automates and supports PCI compliance enterprise-wide**
- **Flexible monitoring capabilities yield revenue-producing business insights – in addition to security and compliance**

> *"Humans can't detect abnormal activity.*
>
> *QRadar can."*

Business Challenge

- Identify threats and risks in real-time, among massive data sets
- Reduce staffing requirements through intelligence & automation
- Gain flexibility of monitoring and reporting, to meet specific business needs

Solution

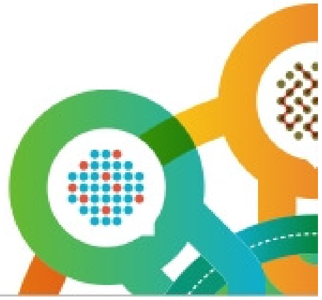
QRadar SIEM, QRadar QFlow

- Real-time correlation of activity across 18 data centers
- Anomaly detection of network and business activity
- Flexible taxonomy and reporting that anyone can use

QRadar Advantages

- Lower cost of ownership: Requires **83% to 92% less** professional services than other solutions, for this client
- Greater automation: Requires **50% to 80% less** staffing than other solutions, for this client

IBMSecuritySymposium
Intelligence | Integration | Expertise



Next Steps

Learn about Security and Compliance in Dark Reading tech center: bit.ly/Dark-Reading

Subscribe to Q1 Labs Newsletter: bit.ly/Q1-subscribe

Read the Q1 Labs Blog: blog.q1labs.com

Follow us on Twitter: @q1labs @ibmsecurity ibm.com/security

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products 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 SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.