Q1Labs®

Total Security Intelligence | An IBM Company

Q1Labs.com

Log management & SIEM:

QRadar Security Intelligence Platform

Tibor Bősze
Security Architect for CEE+RCIS
tibor.boesze@hu.ibm.com

The Security Intelligence Leader

Who is Q1Labs:

- Innovative Security Intelligence software company
- One of the largest and most successful SIEM vendors
- Leader in Gartner 2011, 2010, 2009 Magic Quadrant

Award-winning solutions:

- Family of next-generation Log Management, SIEM, Risk Management, Security Intelligence solutions

Proven and growing rapidly:

- Thousands of customers worldwide
- Five-year average annual revenue growth of 70%+

Now part of IBM Security Systems:

- Unmatched security expertise and breadth of integrated capabilities

Q1 Labs Solves Customer Problems with Total Security Intelligence

SRP

Detecting threats others miss

- Discovered 500 hosts with “Here You Have” virus, which all other security products missed

Chevron

Consolidating data silos

- 2 Billion log and events per day reduced to 25 high priority offenses

LIZ CLAIBORNE

Detecting insider fraud

- Caught an employee sending out proprietary designs

Cargill

Predicting risks against your business

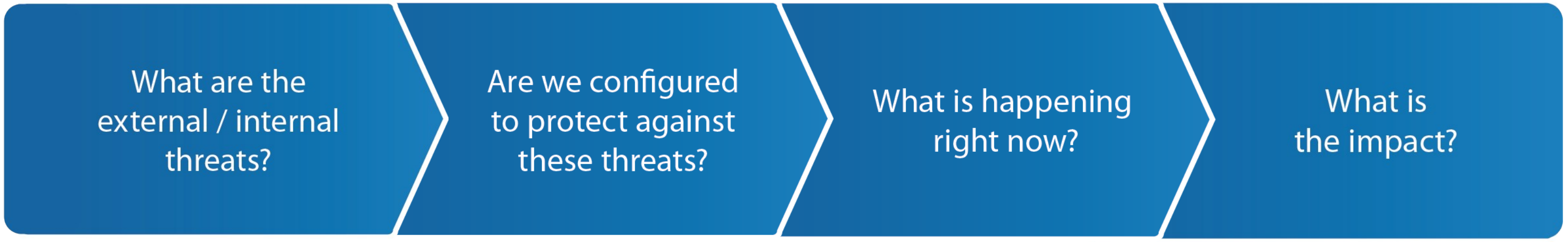
- Automating the policy monitoring and evaluation process for config. change in the infrastructure

WEBB

Exceeding regulation mandates

- Real-time monitoring of all network activity, in addition to PCI mandates

Solutions for the Full Compliance and Security Intelligence Timeline

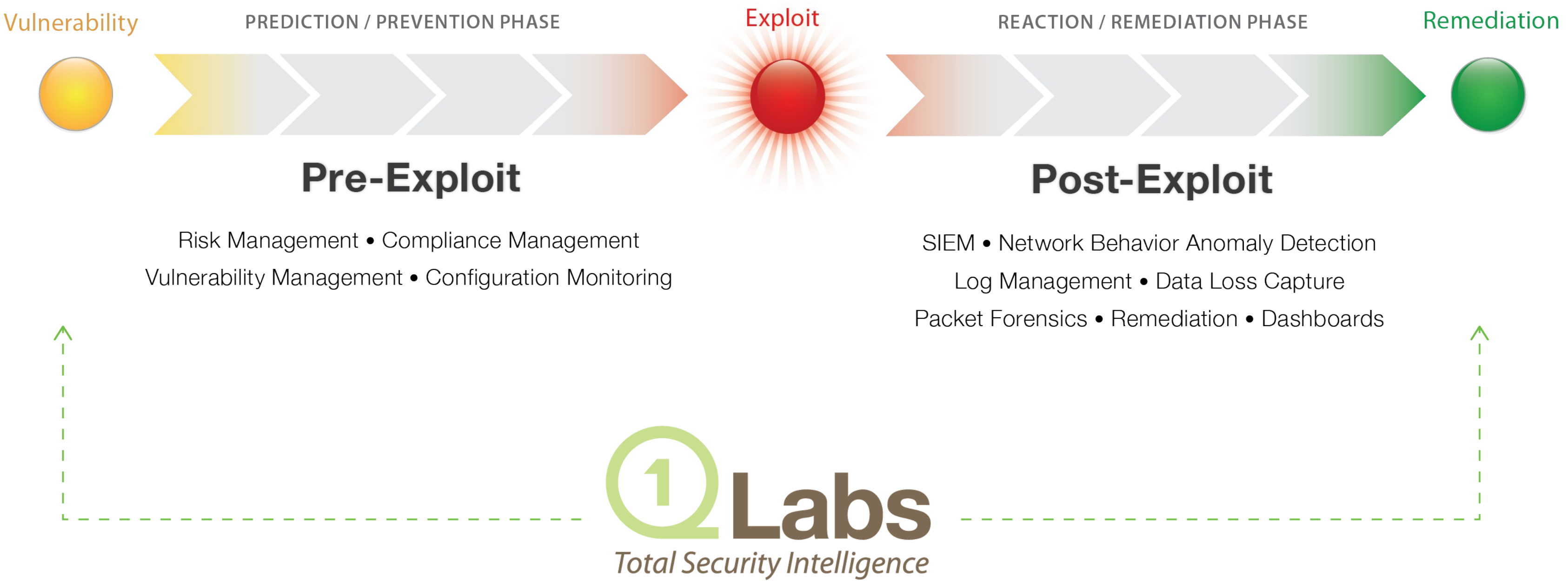


What are the external / internal threats?

Are we configured to protect against these threats?

What is happening right now?

What is the impact?



Vulnerability
PREDICTION / PREVENTION PHASE
Exploit
REACTION / REMEDIATION PHASE
Remediation

Pre-Exploit

Risk Management • Compliance Management

Vulnerability Management • Configuration Monitoring

Post-Exploit

SIEM • Network Behavior Anomaly Detection

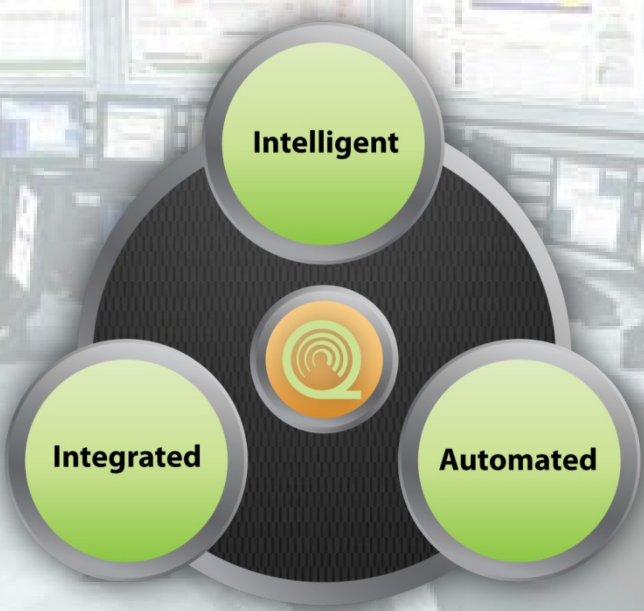
Log Management • Data Loss Capture

Packet Forensics • Remediation • Dashboards

Q1 Labs
Total Security Intelligence

QRadar: Intelligent, Integrated and Automated Security Intelligence Platform

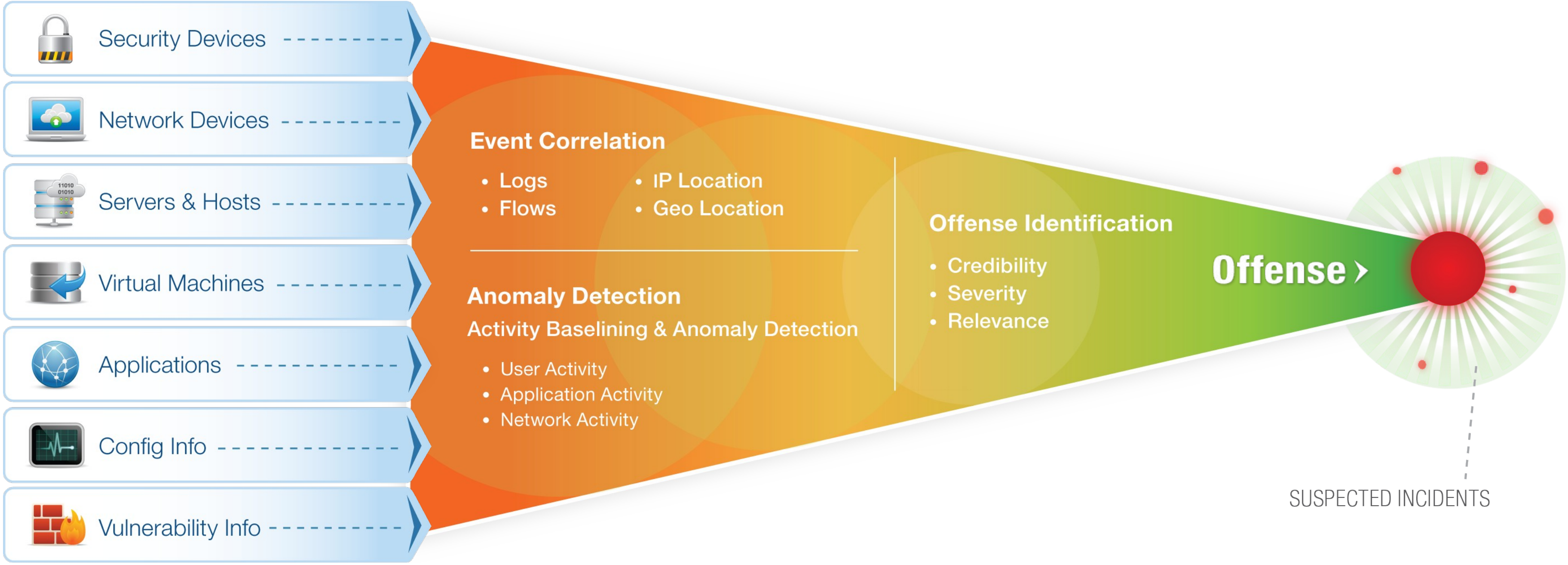
- Proactive threat management
- Massive data reduction
- Rapid, complete impact analysis



- Eliminates silos
- Highly scalable
- Flexible, future-proof

- Operational efficiency
- Simple deployment
- Rapid time to value

Intelligent:
Context & Correlation Drive Deepest Insight



- Security Devices
- Network Devices
- Servers & Hosts
- Virtual Machines
- Applications
- Config Info
- Vulnerability Info

Event Correlation

- Logs
- Flows
- IP Location
- Geo Location

Anomaly Detection

Activity Baselining & Anomaly Detection

- User Activity
- Application Activity
- Network Activity

Offense Identification

- Credibility
- Severity
- Relevance

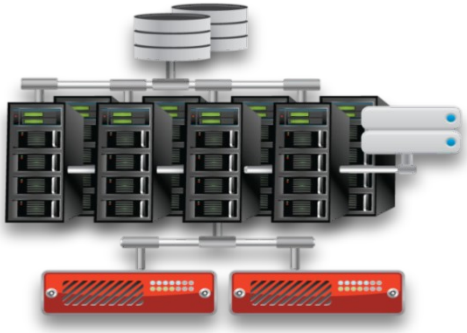
Offense ›

SUSPECTED INCIDENTS

Most Sources + Most Intelligence = Most Accurate & Actionable Insight

Integrated: Unified Platform for Scale & Ease of Use

Bolted Together Solution



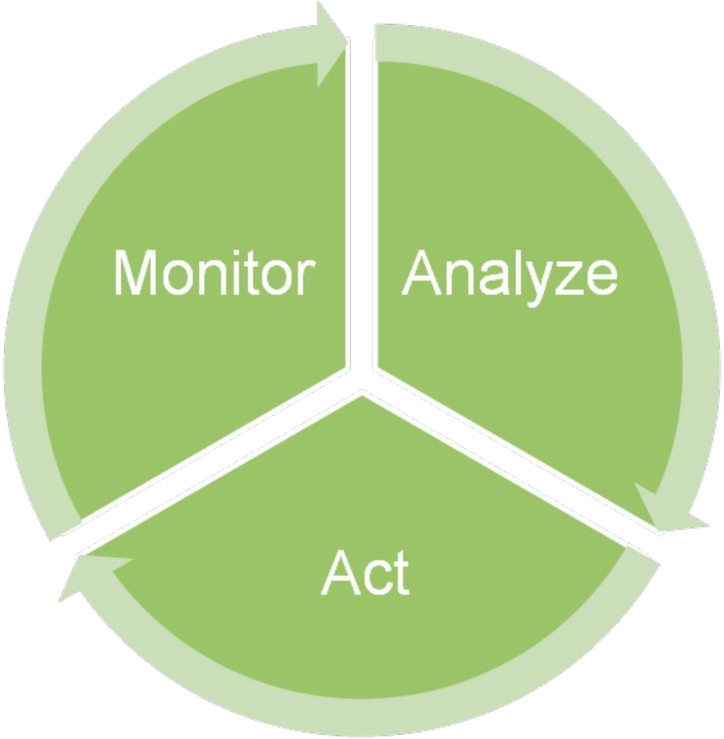
- Scale problems
- Non-integrated reporting & searching
- Only local decisions
- Multi-product administration
- Redundant log repositories
  - ➢ ***Operational bottlenecks***

QRadar Integrated Solution

- Highly scalable
- Common reporting & searching
- Distributed correlation
- Unified administration
- Logs stored once
  - ➢ ***Total visibility***

Automated: No need for additional staff

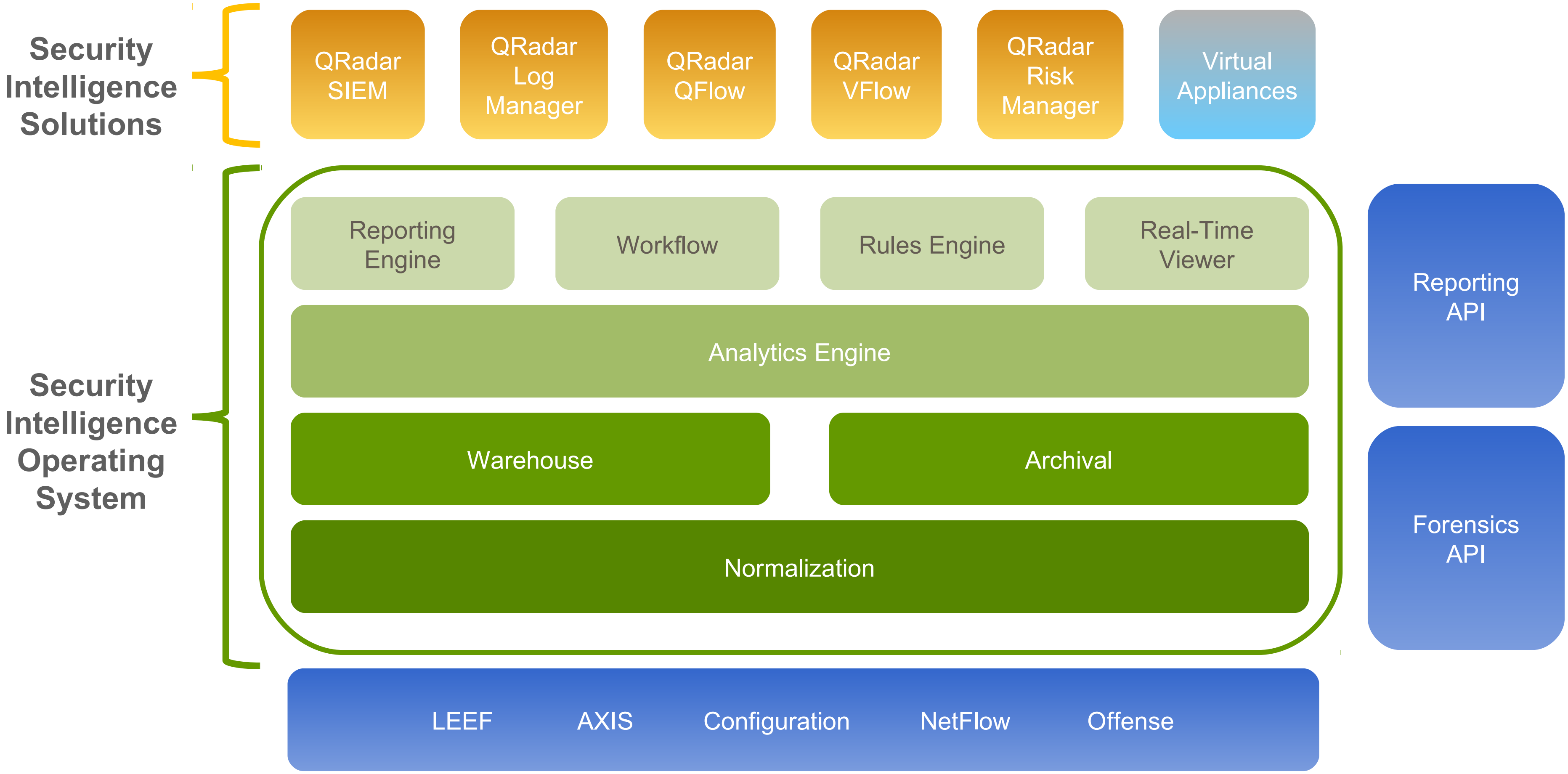
- Auto-discovery of log sources, applications and assets
- Asset auto-grouping
- Centralized log mgmt
- Automated configuration audits



- Asset-based prioritization
- Auto-update of threats
- Auto-response
- Directed remediation

- Auto-tuning
- Auto-detect threats
- Thousands of pre-defined rules and role based reports
- Easy-to-use event filtering
- Advanced security analytics

QRadar Family: Built On a Common Foundation

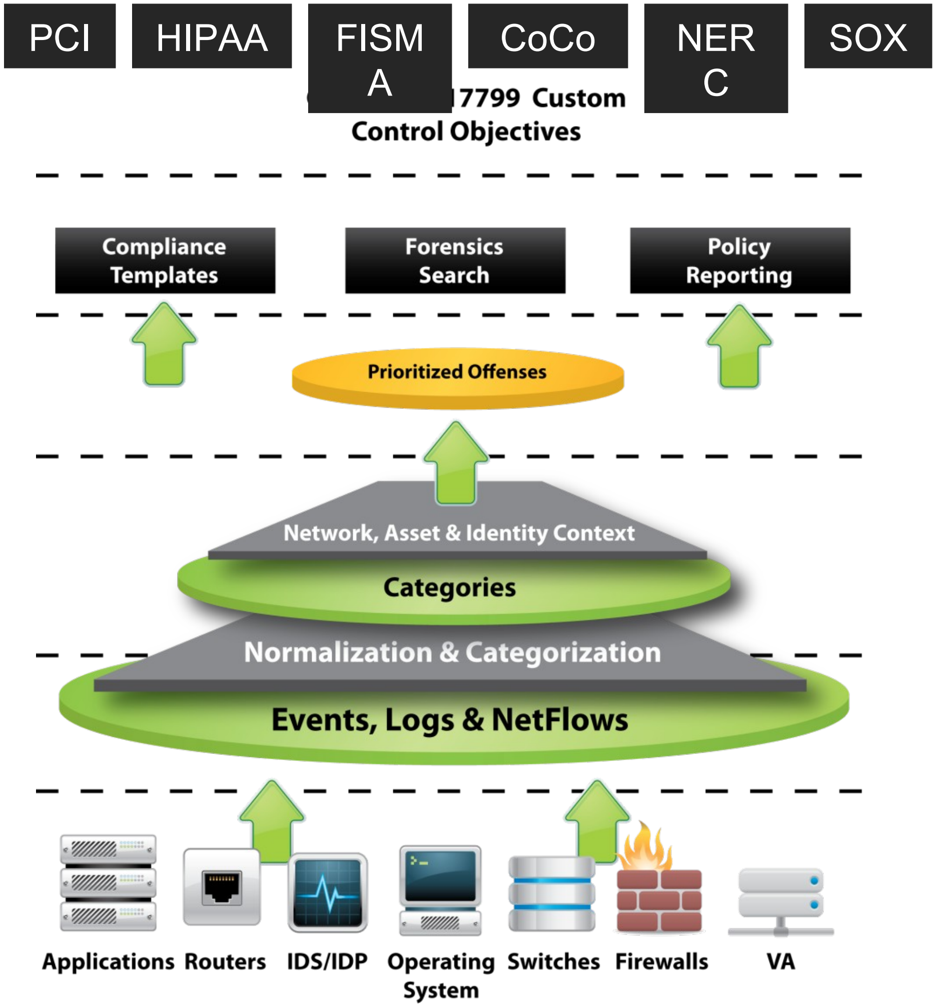


Intelligent, Integrated, Automated – One Console Security

Fully Integrated Security Intelligence

Log Management	QRadar® Log Manager QRadar® Log Manager Free Edition	• Turnkey log management • SME to Enterprise • Upgradeable to enterprise SIEM
SIEM	QRadar® SIEM	• Integrated log, threat, risk & compliance mgmt. • Sophisticated event analytics • Asset profiling and flow analytics • Offense management and workflow
Risk Management	QRadar® Risk Manager	• Predictive threat modeling & simulation • Scalable configuration monitoring and audit • Advanced threat visualization and impact analysis
Network Activity & Anomaly Detection	QRadar® SIEM QRadar QFlow	• Network analytics • Behavior and anomaly detection • Fully integrated with SIEM
Network and Application Visibility	QRadar QFlow QRadar VFlow	• Layer 7 application monitoring • Content capture • Physical and virtual environments

Complete Security and Compliance Management


PCI
HIPAA
FISMA
CoCo
NERC
SOX
17799 Custom
Control Objectives
Compliance Templates
Forensics Search
Policy Reporting
Prioritized Offenses
Network, Asset & Identity Context
Categories
Normalization & Categorization
Events, Logs & NetFlows
Applications
Routers
IDS/IDP
Operating System
Switches
Firewalls
VA

- Compliance validation and security response improvement in the same solution
- Out of the box content to swiftly meet PCI, NERC, SOX, HIPAA, GLBA, CoCo, etc.
- Flexibility to meet new compliance standards as they evolve

Fully Integrated Security Intelligence

Log Management

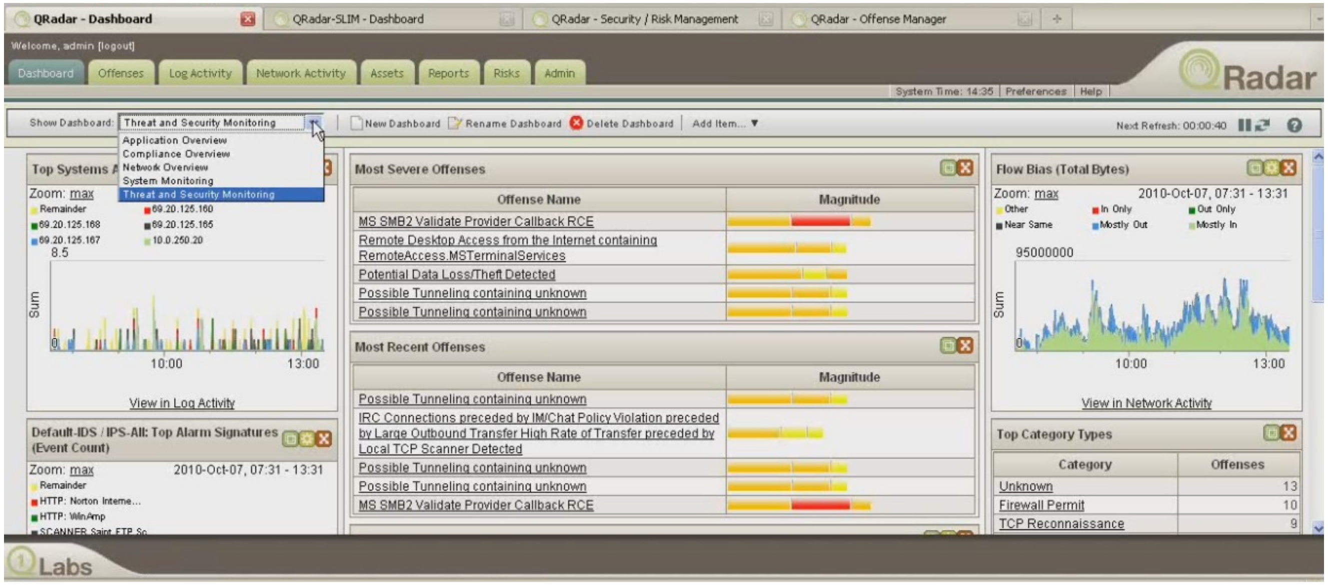
SIEM

Risk Management

Network Activity & Anomaly Detection

Network and Application Visibility

One Console Security



Most Severe Offenses

Offense Name	Magnitude
MS SMB2 Validate Provider Callback RCE	▬
Remote Desktop Access from the Internet containing RemoteAccess.MSTerminalServices	▬
Potential Data Loss/Theft Detected	▬
Possible Tunneling containing unknown	▬
Possible Tunneling containing unknown	▬

Most Recent Offenses

Offense Name	Magnitude
Possible Tunneling containing unknown	▬
IRC Connections preceded by IM/Chat Policy Violation preceded by Large Outbound Transfer High Rate of Transfer preceded by Local TCP Scanner Detected	▬
Possible Tunneling containing unknown	▬
Possible Tunneling containing unknown	▬
MS SMB2 Validate Provider Callback RCE	▬

Top Category Types

Category	Offenses
Unknown	13
Firewall Permit	10
TCP Reconnaissance	9

Built on a Single Data Architecture

Thank You

Questions and Answers