



SIEM - Security Intelligence

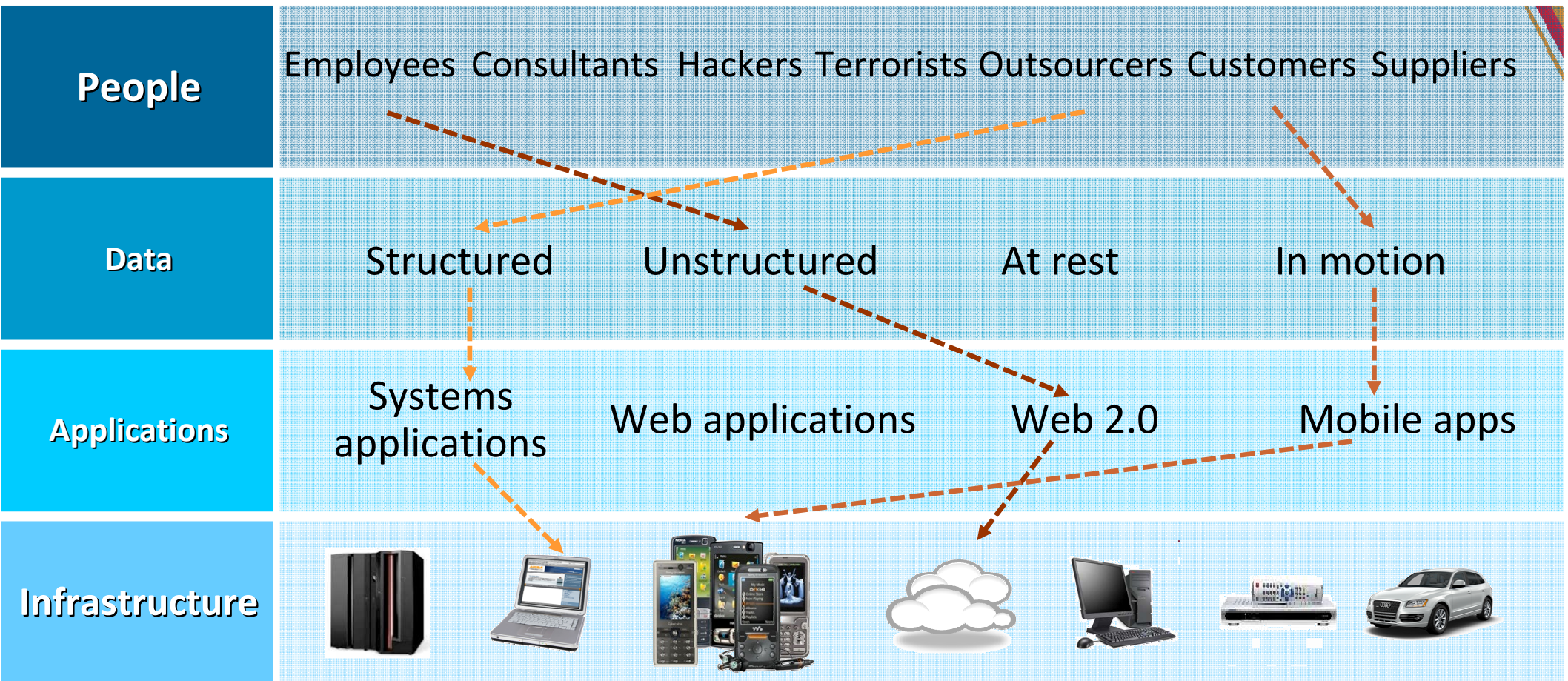
Alfonso Ponticelli
IBM Security Systems

PCTY2012 

Pulse Comes to You

Optimizing the World's Infrastructure
[May, 15° Rome]

Security: A complex, four- dimensional puzzle



Total Visibility: Product Portfolio, Services and Research

Enterprise Governance, Risk and Compliance Management

GRC Platform (OpenPages) Risk Analytics (Algorithmics) Investigation Management (i2)

IBM Security Portfolio

IT Security / Compliance Analytics & Reporting

QRadar SIEM QRadar Log Manager QRadar Risk Manager IBM Privacy, Audit and Compliance Assessment Services

IT Infrastructure – Operational Security Domains

People	Data	Applications	Infrastructure	
			Network	Endpoint
Identity & Access Management Suite	Guardium Database Security	AppScan Source Edition	Network Intrusion Prevention	Endpoint Manager (BigFix)
Federated Identity Manager	Optim Data Masking	AppScan Standard Edition	DataPower Security Gateway	zSecure, Server and Virtualization Security
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Anomaly Detection / QFlow	Native Server Security (RACF, IBM Systems)
Identity Assessment, Deployment and Hosting Services	Data Security Assessment Service	Application Assessment Service	Managed Firewall, Unified Threat and Intrusion Prevention Services	Penetration Testing Services
	Encryption and DLP Deployment	AppScan OnDemand Software as a Service		

Security Consulting

Managed Services

X-Force and IBM Research

Products Services



Q1Labs

✓ Who they are:

- Innovative Security Intelligence software company
- Largest independent SIEM vendor
- Leader in Gartner 2010 and 2009 Magic Quadrants

✓ Award winning solutions:

- Family of next-generation Risk Management, Log Management, SIEM, security intelligence solutions

✓ Executing, growing rapidly:

- +1600 customers worldwide
- Five-year average revenue growth +70%
- North America, EMEA and Asia Pacific



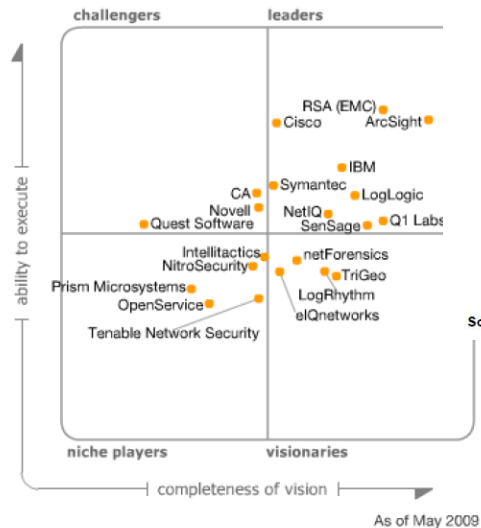
Gartner
Magic Quadrant



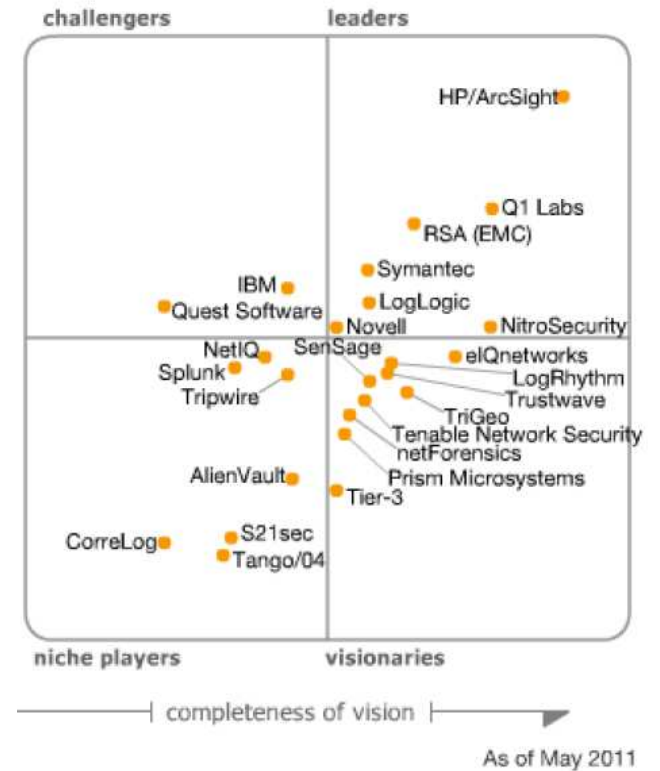
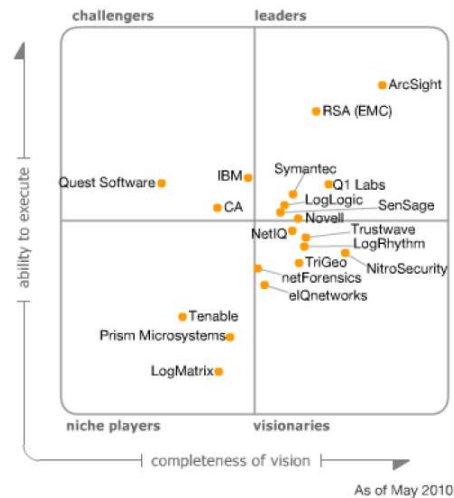
Consistent Leadership Progress



Source: Gartner (May 2009)



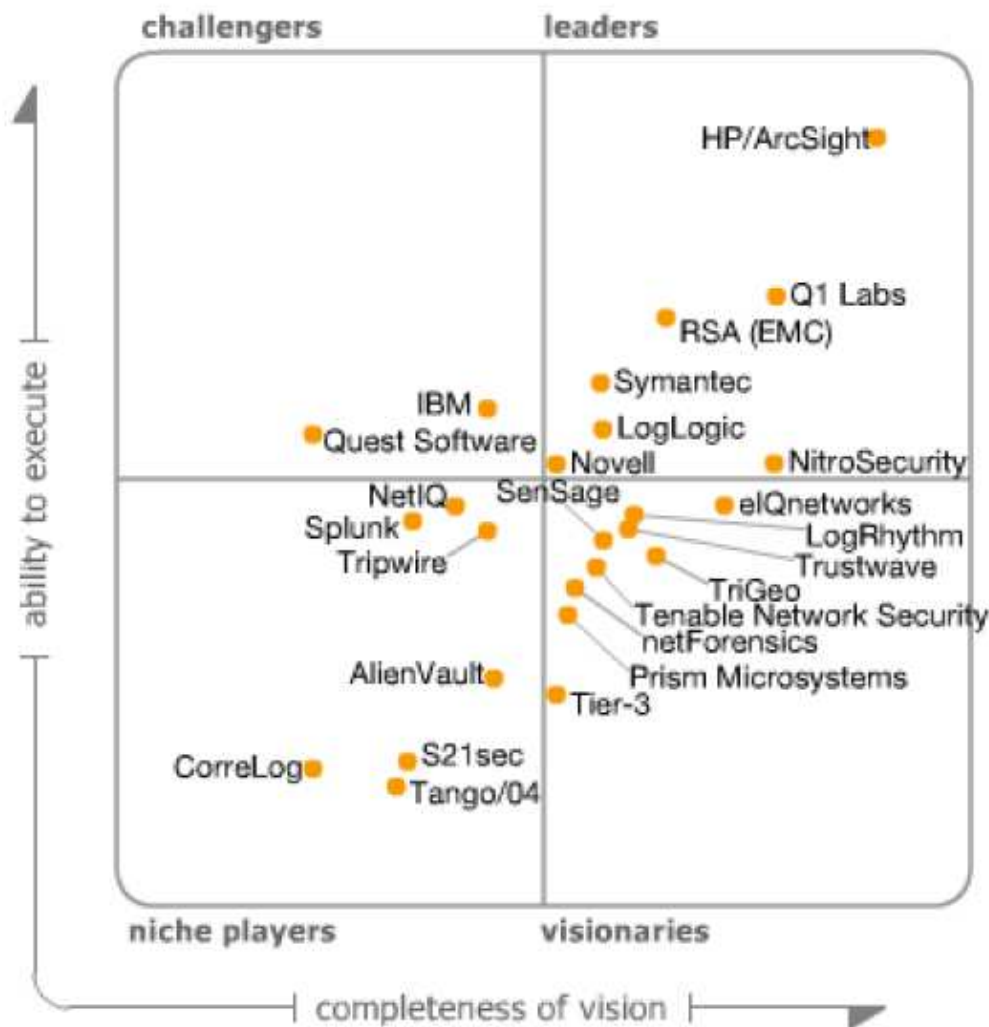
Source: Gartner (May 2010)



Source: Gartner (May 2008)

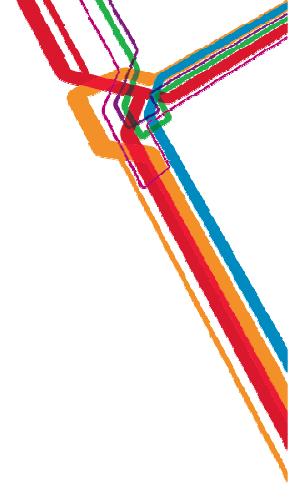
Clear Leadership 2011 SIEM MQ

Figure 1. Magic Quadrant for Security Information and Event Management



As of May 2011

Solving Customer Business Pains that Point Products Can't Address



Detecting threats others miss

- Arm yourself with total security intelligence



Consolidating data silos

- Collect, correlate and report on data in one integrated solution



Detecting insider fraud

- Next generation SIEM with identity correlation



Predicting risks to your business

- Full life cycle of compliance and risk management for network and security infrastructures



Exceeding regulation mandates

- Automated data collection and configuration audits

QRadar – SIEM 2nd Generation

Evolution of the **MODERN SIEM**

First Generation SIEM Matures to Anchor Security Intelligence

Security Information Management (SIM)

Log Management
Reporting
Analysis
Compliance reporting

1st Gen SIEM

Monitor traditional security telemetry
Visibility into servers and security systems

Security Event Management (SEM)

Real-time monitoring of events
Security and network devices
Applications
Event correlation
Incident response

Next Generation SIEM

Threat and anomaly detection
Policy-aware compliance
User behavior & context
Analysis before, during, after attack

Risk Management

Device configuration & topology
Pre-exploit analysis & simulation
Prioritized vulnerabilities

Network Behavior Anomaly Detection

Network activity monitoring; virtual, physical
Full packet capture

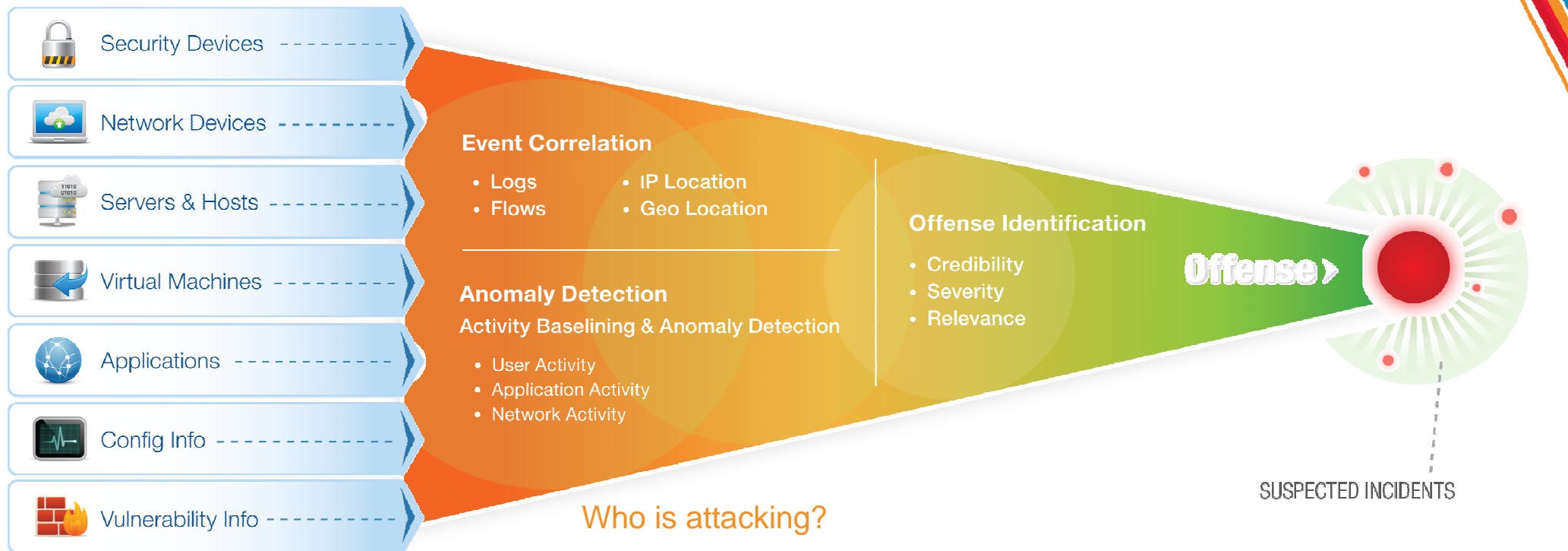
Future

Open Systems & SDKs
Increasing levels of context
Full integration of security process & workflow
Greater predictive ability

Integrated Architecture | Database Rapid Search & Query | Correlation, Analysis, Normalization | One-console Security

Security Intelligence Platform

QRadar Security Intelligence Platform: helps provide security teams with the intelligence they need to act



Who is attacking?

What is being attacked?

What is the business impact?

Where do I investigate?

Most Sources

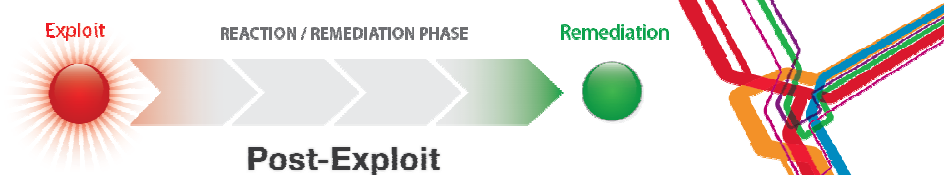


Most Intelligence



Most Accurate &
Actionable Insight

Offenses are Real-Time



Event Correlation

- Logs
- IP Location
- Flows
- Geo Location

Anomaly Detection

Activity Baseline & Anomaly Detection

- User Activity
- Application Activity
- Network Activity

Rules Engine



Rule Action
Choose the action(s) to take when an event occurs that triggers this rule

Severity Set to: C

Credibility Set to: C

Relevance Set to: C

Ensure the detected event is part of an offense

Index offense based on: Source IP

Annotate this offense:

Include detected events by Source IP from this point forward, for _____ second(s), in the offense

Annotate event

Drop the detected event

Offenses

ID	Description	Attacker(s)/Src	Magnitude	Target(s)/Dest
001	Remote FTP Scanner detected, Excessive Firewall Denies	217.64.100.162	8	Multiple (99)
002	Excessive Login Faliures, Login Success	81.240.89.210	9	10.100.50.81

The Key to Data Management:

System Summary

Flows (Past 24 Hours)	1.3M
New Events (Past 24 Hours)	677M
Updated Offenses (Past 24 Hours)	588
Data Reduction Ratio	10833 : 1

Most Recent Offenses

Offense Name	Magnitude
Local Web Scanner Detected containing Web.Image.GIF	██████
Potential P2P Traffic or VoIP Detected preceded by Local TCP Scanner Detected containing unknown	██████
Local Web Scanner Detected containing Web.Image.JPG	██████
MS SMB2 Validate Provider Callback RCE	███████
Local Web Scanner Detected containing Web-HTTPWeb	██████

Reduction and Prioritization

QRadar Offense Management

QRadar - Offense Manager - Mozilla Firefox

File Edit View History Bookmarks Tools Help

192.168.202.128 https://192.168.202.128/console/qradar/jsp/QRadar.jsp

QRadar7 QRadar-LM Q-Zone Qmmunity Partner Portal

QRadar - Offense Manager

Welcome, admin [logout]

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Admin

My Offenses
All Offenses
By Category
By Source IP
By Destination IP
By Network
Rules

Search... Save Criteria Actions Print

All Offenses: View Offenses: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Events	Flows	Start Date	Last Event/Flov
160	Destination Vulnerable to Detected Exploit preced					19984	355	2010-10-01 07:51:00	28d 4h ...
148	Sensitive Data in Transit containing Web.Facebo					1	1	2010-10-01 05:31:30	28d 6h ...
154	Policy: Chat or IM Traffic Detected containing Chat					1	5	2010-10-01 01:04:09	28d 11h...
236	Communication to a know Bot Command and Control containing					1	4	2010-10-01 03:16:00	28d 8h ...
125	Policy: Local: Clear Text Application Usage	Source IP	10.0.100.104		10.0.100.104	1	4	2010-10-01 00:04:00	28d 12h...
155	DLP - Potential Data Loss containing Web.MSNLive.Text	Source IP	10.0.240.251		dhcp-251-users-1.a	8	N/A	2010-10-01 04:00:19	28d 8h ...
150	Login Failures Followed By Success from the same Username	Username	roberta_hite		10.0.5.226	2	140	2010-10-01 06:26:16	28d 5h ...
146	Login Failures Followed By Success to the same Destination IP pri	Source IP	80.96.34.22		80.96.34.22	45	2338	2010-10-01 02:23:01	28d 9h ...

Displaying 1 to 8 of 8 items (Elapsed time: 0:00:00.158)
Copyright © 2010 Q1 Labs Inc. All rights reserved.

Done

Q1 Labs

Specifies the number of flows and events for this offense

Specifies the elapsed time since the last event or flow associated with this offense

Specifies the log sources associated with this offense. If more than one log source is associated with the offense, this field indicates Multiple and the number.

Specifies that component

Specifies The represent events include

Specifies offense. Source example Offense

QRadar Offense Management



Offense 3063		Summary	Attackers	Targets	Categories	Annotations	Networks	Events	Flows	Rules	Actions	Print	?
Magnitude		Relevance	0	Severity	8	Credibility	3						
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Preceded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan			Event count	1428 events in 3 categories								
Attacker/Src	202.153.48.66			Start	2009-09-29 16:05:01								
Target(s)/Dest	Local (717)			Duration	1m 32s								
Network(s)	Multiple (3)			Assigned to	Not assigned								
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving... data with IDS alerts An attacker originating from China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250). The first sys...												

What was the attack?

Was it successful?

Who was responsible?

Attacker Summary		Details
Magnitude		User
Description		Asset Name
Vulnerabilities		MAC
Location		Asset Weight

Top 5 Categories					Categories
Name	Magnitude	Local Target Count	Events	Last Event	
Buffer Overflow		8		09-29 16:06:33	
Misc Exploit		3		09-29 16:06:33	
Network Sweep		716			

Where do I find them?

How valuable are they to the business?

Top 5 Local Targets							Targets
IP/DNS Name	Chained	User	MAC	Weight			
Windows AD Server	No	Unknown	Unknown	8			
10.101.3.3	No	Unknown	Unknown	0			
10.101.3.4	No	Unknown	Unknown	0			
DC106	Yes	Administrator	00:15:c5:56:3e:a7	10			
10.101.3.11	Unknown	No	DCAdmin	00:15:c5:5a:3e:a7	main	0	

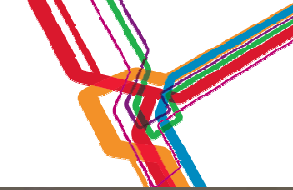
How many targets involved?

Top 10 Events								Events
Event Name	Magnitude	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 @	Buffer Overflow	10.101.3.10	445	09-29 16:06:28		
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @	Buffer Overflow	10.101.3.15	445	09-29 16:06:33		
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm	Misc Exploit	10.101.3.13	445	09-29 16:06:31		
Network Sweep - QRadar Classify Flow		Flow Classification Engine-8 :: qradar-vm	Network Sweep	10.101.3.10	445	09-29 16:05:01		
Network Sweep - QRadar Classify Flow		Flow Classification Engine-8 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01		
Network Sweep - QRadar Classify Flow		Flow Classification Engine-8 :: qradar-vm	Network Sweep	10.101.3.10	445	09-29 16:05:01		
Network Sweep - QRadar Classify Flow		Flow Classification Engine-8 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01		

Are any of them vulnerable?

Where is all the evidence?

Rule Modification - Editor



Welcome, admin [logout]

Dashboard Offenses

- My Offenses
- All Offenses
- By Category
- By Source IP
- By Destination IP
- By Network
- Rules

Rule Wizard - Rule Test Stack Editor

Which tests do you wish to perform on incoming flows and events?

Test Group: All Export as Building Block

- when the local network is **one of the following networks**
- when the destination network is **one of the following networks**
- when the IP protocol is one of the following **protocols**
- when the Flow Source or Destination Payload contains **this string**
- when the source port is one of the following **ports**
- when the destination port is one of the following **ports**
- when the local port is one of the following **ports**
- when the remote port is one of the following **ports**
- when the source IP is one of the following **IP addresses**
- when the destination IP is one of the following **IP addresses**
- when the local IP is one of the following **IP addresses**
- when the remote IP is one of the following **IP addresses**
- when either the source or destination IP is one of the following **IP addresses**

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Recon: Local Web Server Scanner on events or flows which are detected by the Local system

- and when the context is Local to Local, Local to Remote
- and when a flow or an event matches any of the following BB:PortDefinition: Web Ports
- and when any of these BB:CategoryDefinition: Recon Events, BB:CategoryDefinition: Suspicious Events with the same source IP more than 5 times, across more than 59 destination IP within 10 minutes

Please select any groups you would like this rule to be a member of:

- Anomaly
- Authentication

<< Back Next >> Finish Cancel

Radar

Path	Actions	Print
3	Credibility	3

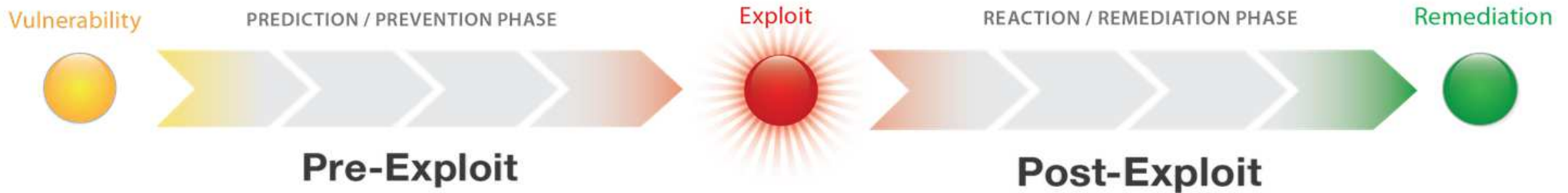
Last Event/Flow

S

Done

Attack Sophistication

IBM is helping clients combat advanced threats with pre- and post-exploit intelligence and action



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.



The QRadar Security Intelligence Solutions Deploy, Expand at Your Pace



One Console Security

Log Management

SIEM/SEM

Risk Management

Scale

Visibility/
Network Activity

The screenshot shows the QRadar dashboard with several key sections:

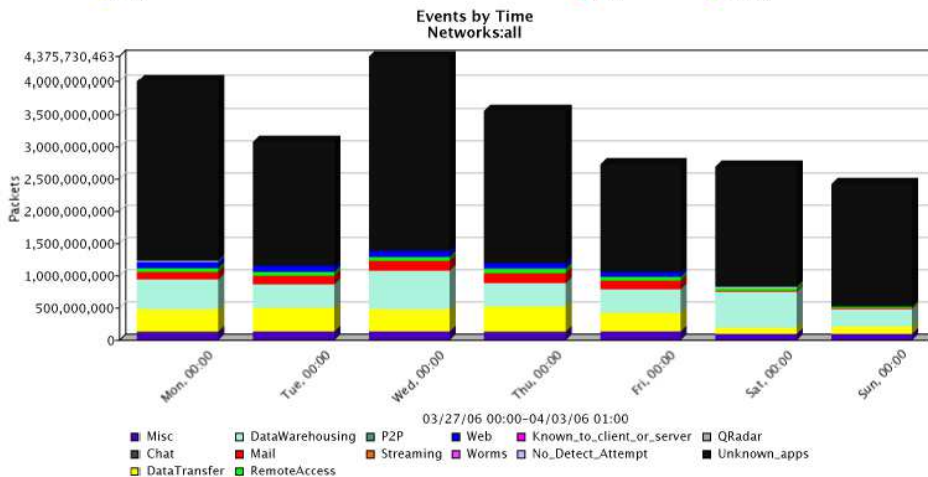
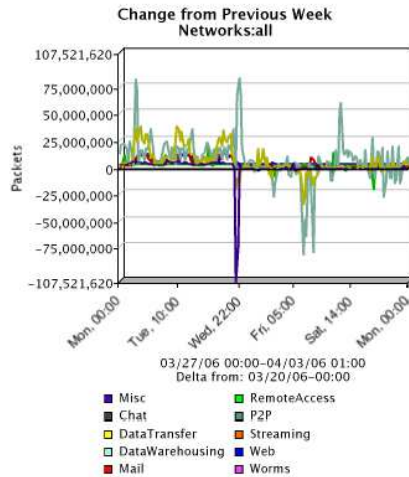
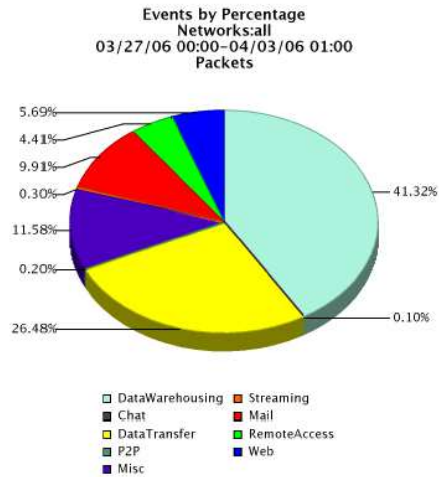
- Top Systems:** A bar chart showing system activity with a zoom level of 'max' and a sum of 8.5.
- Most Severe Offenses:** A table listing offenses such as 'MS SMB2 Validate Provider Callback RCE' and 'Remote Desktop Access from the Internet containing RemoteAccess.MSTerminalServices'.
- Most Recent Offenses:** A table listing recent offenses like 'Possible Tunneling containing unknown' and 'IRC Connections preceded by IM/Chat Policy Violation'.
- Flow Bias (Total Bytes):** A line chart showing network activity flow bias for the period 2010-Oct-07, 07:31 - 13:31.
- Top Category Types:** A table showing the number of offenses for categories like 'Unknown' (13), 'Firewall Permit' (10), and 'TCP Reconnaissance' (9).

The dashboard also includes navigation tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, and Admin. The system time is 14:35.

Reporting

Weekly Events Summary

Generated: Apr 3, 2006 3:47:51 PM



- ✓ All information collected is available for reports
- ✓ Thousands out-of-the-box report templates for compliance and device reporting
- ✓ Fully customizable reporting engine: creating, branding and scheduling delivery of reports
- ✓ Compliance reporting packages for PCI, SOX, FISMA, GLBA, and HIPAA
- ✓ Reports based on control frameworks: NIST, ISO, and CoBIT

Manage User Roles Function



- ✓ Best Practice: Create roles before users
- ✓ Roles must be created for user accounts that will not have full administrative access
- ✓ To create a role, use the Manage User Roles function in the Administration Console
- ✓ Select the check boxes for the functionality you want
- ✓ You can have an unlimited number of roles

Manage Role Permissions

Role Name

Select the permissions to be associated with this role.

<input type="checkbox"/> Admin <ul style="list-style-type: none"><input type="checkbox"/> Administrator Manager<input type="checkbox"/> System Administrator<input type="checkbox"/> Remote Networks and Services Configuration	<input type="checkbox"/> Offenses <ul style="list-style-type: none"><input type="checkbox"/> Customized Rule Creation<input type="checkbox"/> Assign Offenses to Users
<input type="checkbox"/> Log Activity <ul style="list-style-type: none"><input type="checkbox"/> Customized Rule Creation<input type="checkbox"/> User Defined Event Properties<input type="checkbox"/> Manage Time Series	<input type="checkbox"/> Assets <ul style="list-style-type: none"><input type="checkbox"/> Remove Vulnerabilities<input type="checkbox"/> Server Discovery<input type="checkbox"/> View VAData<input type="checkbox"/> Perform VA Scans
<input type="checkbox"/> Network Activity <ul style="list-style-type: none"><input type="checkbox"/> View Flow Content<input type="checkbox"/> Manage Time Series<input type="checkbox"/> Customized Rule Creation<input type="checkbox"/> User Defined Flow Properties	<input type="checkbox"/> Reports <ul style="list-style-type: none"><input type="checkbox"/> Maintain Templates<input type="checkbox"/> Distribute Reports via Email
<input type="checkbox"/> IP Right Click Menu Extensions	<input type="checkbox"/> Risk Manager

QRadar Architecture – “All In One”

or
 QRadar LM All-In-One Appliance  QRadar SIEM All-In-One Appliance

QRadar License	LM	SIEM
Events	✓	✓
Network Flows	-	✓
QFlow or VFlow	-	✓
Vulnerability Data	-	✓
Log Management	✓	✓
Correlation Engine	✓	✓
Offenses	-	✓
Risk Manager Option	-	✓
Upgradable to SIEM	✓	N/A
Migration to Distributed Architecture	✓	✓
Max EPS	5,000	5,000
Max FPI	N/A	200,000



QRadar Architecture – Distributed Architecture

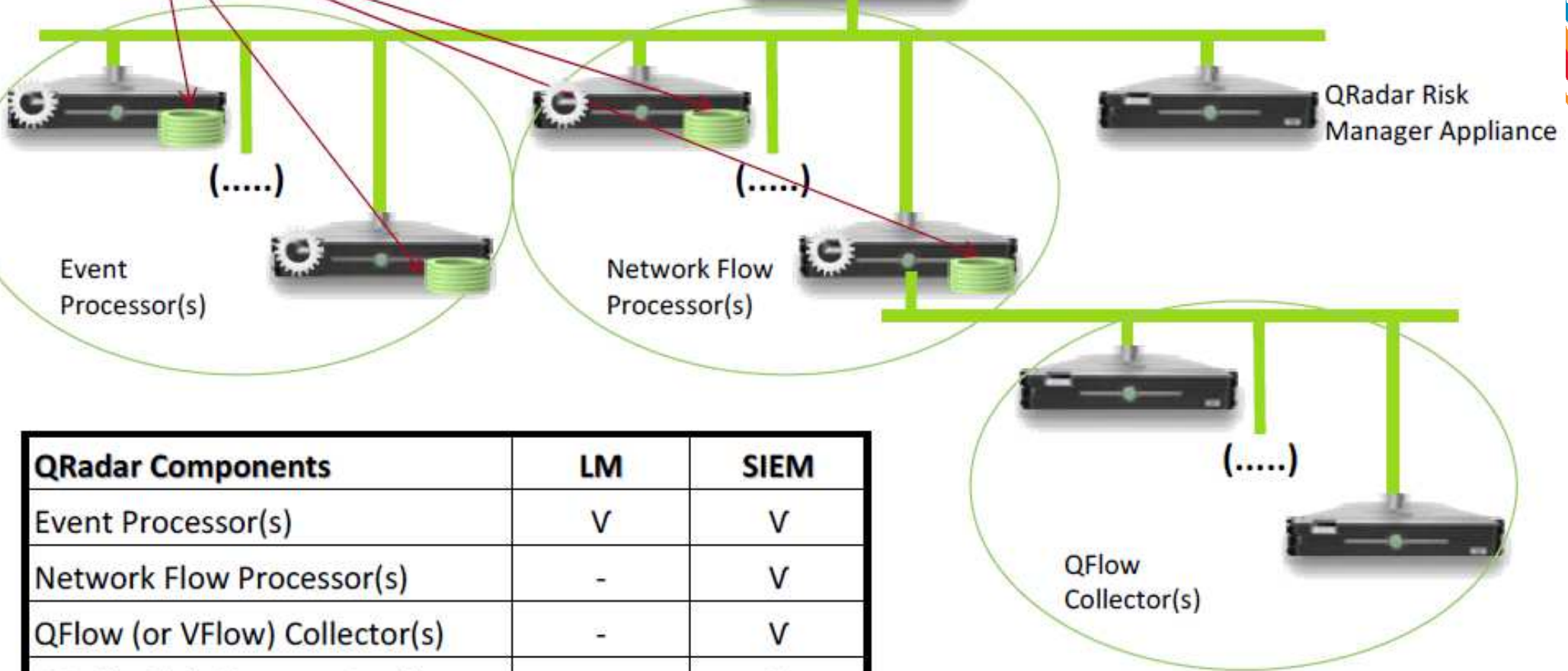


Embedded, real-time distributed database

QRadar LM Console

or

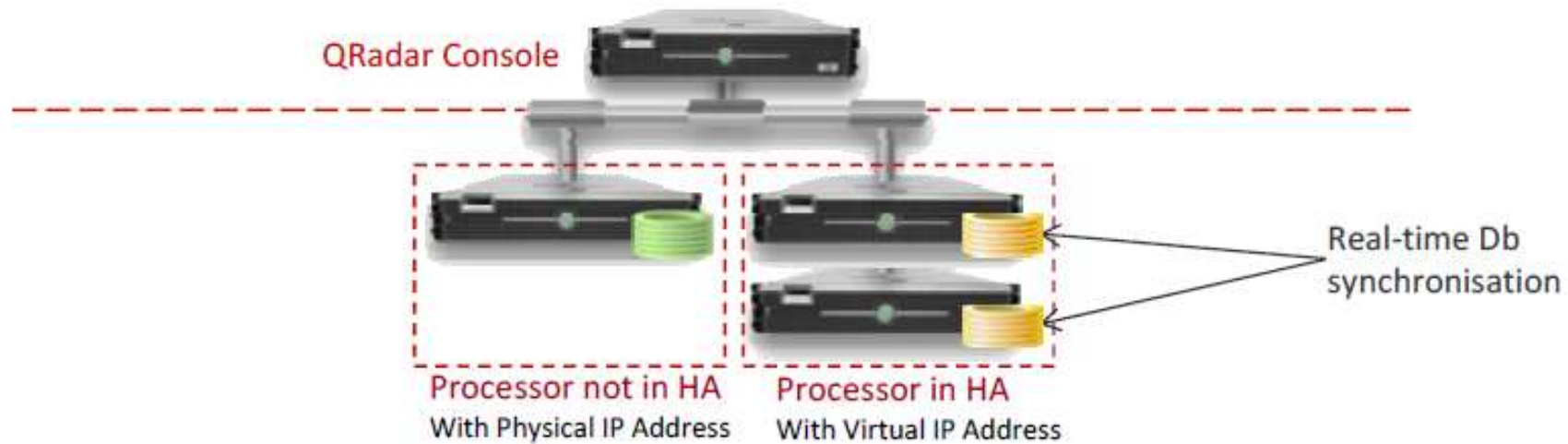
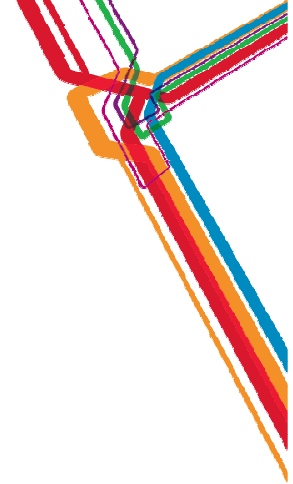
QRadar SIEM Console



QRadar Components	LM	SIEM
Event Processor(s)	✓	✓
Network Flow Processor(s)	-	✓
QFlow (or VFlow) Collector(s)	-	✓
QRadar Risk Manager Appliance	-	✓
Max EPS	Unlimited*	Unlimited*
Max FPI	N/A	Unlimited*

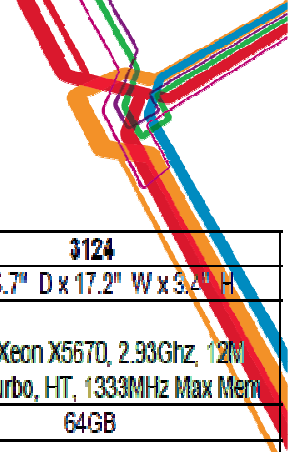
* Unlimited as long as enough processors are deployed to support the required volume of events/flows.

QRadar Architecture – High Availability



Example : Distributed Architecture
with 1 Processor and 2 Processors in HA

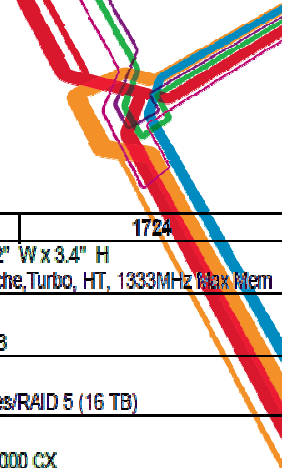
Appliance Specifications Matrix



All in One and Console Appliances

	2000	2100	3100/Console	LM/Console	3105	3124
Dimensions	1U:30.4" D x 16.7" W x		2U:26.8" D x 17.44" W x 3.4" H		2U:26.7" D x 17.2" W x 3.4" H	2U:26.7" D x 17.2" W x 3.4" H
CPU	Quad Core Xeon with 8MB Cache, 2.4GHz, 5.86 GT/s QPI, TurboHT		2 Quad Core Xeon 2.4GHz 8M Cache, Turbo, HT, 1066MHz Max Mem		2 Quad Core Xeon with 2.4GHz 8M Cache, Turbo, HT, 1056MHz Max Mem	2 Intel Xeon X5670, 2.93Ghz, 12M Cache, Turbo, HT, 1333MHz Max Mem
Memory	12GB	24GB	24GB		24GB	64GB
Storage	2x500GB SATA II Drives/RAID 1 (500GB)	6x500GB SATA II Drives/RAID10 (1.5TB)	6x1 TB SATA II Drives/RAID10 (3 TB)		8x1TB SATA II Drives/RAID 5 (6.2 TB)	12x2TB SATA II Drives/RAID 5 (16 TB)
Network Interfaces	4x10/100/1000 CX				2x10/100/1000 CX	2x10/100/1000 CX
Power	Dual Redundant Auto Sensing 110/220 Volt Power Supply (670 Watt)		Dual Redundant Auto Sensing 110/220 Volt Power Supply (750 Watt)		Dual Redundant Auto Sensing 110/220 Volt Power Supply (750 Watt)	Dual Redundant Auto Sensing 110/220 Volt Power Supply (750 Watt)
	Configuration Totals for 110 AC Input Voltage and 77°F Total Input Power: 175.5 watts 598.9 btu/h Total Input Current: 1.6 amps Sound Power Level: 6.2 bels * Airflow Rate: 11.2 l/s 23.7 CFM Total Weight: 17.7 kg 39.0 lbs		Configuration Totals for 110 AC Input Voltage and 77°F Total Input Power: 377.6 watts 1288.4 btu/h Total Input Current: 3.5 amps Sound Power Level: 6.1 bels * Airflow Rate: 17.6 l/s 37.4 CFM Total Weight: 26.1 kg 57.5 lbs		Configuration Totals for 110 AC Input Voltage and 77°F Total Input Power: 354.8 watts 1210.7 btu/h Total Input Current: 3.3 amps Sound Power Level: 0.0 bels * Total Weight: 34.5 kg 76.1 lbs	Configuration Totals for 110 AC Input Voltage and 77°F, Total Input Power: 477 watts 1627.6 btu/h, Total Input Current: 4.4 amps, Sound Power Level: 4.4 bels * Total Weight: 34.5 kg 76.1 lbs
QFlow Traffic Rate	50Mbps	50Mbps	NA	NA	NA	NA
EPS Sustained	200	1000	5000/NA	5000/NA	5000	5000
EPS Burst	50,000		50,000		50,000	50,000
Flows Per Interval	15,000	up to 50,000	up to 200,000	NA	up to 200,000	up to 200,000
Event Storage	*3 Weeks	*5 Weeks	*6 Weeks/NA	Up to 41 Wks @ 1000 Avg. EPS	*10 weeks	*10 weeks
Flow Storage	*7 Days		NA		*14 days	*14 days
Views Storage	*6 Weeks		NA		NA on 7.0	NA on 7.0
Network Objects	100	100	1000	1000	1000	1000

Appliance Specifications Matrix



Processor Appliances

	1701	1801/SLIM	1801	1802	1805	1824	1724
Dimensions	2U:26.8" D x 17.44" W x 3.4" H				2U:26.8" D x 17.44" W x 3.4" H		2U:26.7" D x 17.2" W x 3.4" H
CPU	2 Quad Core Xeon with 2.4GHz 8M Cache, Turbo, HT, 1066MHz Max Mem				2 Quad Core Xeon with 2.4GHz 8M Cache, Turbo, HT, 1066MHz Max Mem		2 Intel Xeon X5670, 2.93GHz, 12M Cache, Turbo, HT, 1333MHz Max Mem
Memory	12GB			24GB	12GB		64GB
Storage	6x1TB SATA II Drives/RAID10 (3 TB)		6x500GB SATA II Drives/RAID10 (1.5TB)	6x1 TB SATA II Drives/RAID10 (3 TB)	8x1TB SATA II Drives/RAID 5 (6.2 TB)		12x2TB SATA II Drives/RAID 5 (16 TB)
Network Interfaces	4x10/100/1000 CX				2x10/100/1000 CX		2x10/100/1000 CX
Power	Dual Redundant Auto Sensing 110/220 Volt Power Supply (750 Watt)						
	Configuration Totals for 110 AC Input Voltage and 77°F Total Input Power: 377.6 watts 1298.4 btu/h Total Input Current: 3.5 amps Sound Power Level: 6.1 bels * Total Weight: 26.1 kg 57.5 lbs				Configuration Totals for 110 AC Input Voltage and 77°F Total Input Power: 354.8 watts 1210.7 btu/h Total Input Current: 3.3 amps Sound Power Level: 0.0 bels * Total Weight: 34.5 kg 76.1 lbs		Configuration Totals for 110 AC Input Voltage and 77°F, Total Input Power: 477 watts 1627.6 btu/h, Total Input Current: 4.4 amps, Sound Power Level: 4.4 bels * Total Weight: 34.5 kg 76.1 lbs
EPS Sustained	NA	Up to 10000*	1000*	5,000	Up to 20,000*		Up to 20,000*
EPS Burst	NA	75000*	50000*	50000*	75000*		75000*
Flows Per Interval	Up to 600,000	NA	Up to 50,000	Up to 200,000	NA		NA
Event Storage	NA	Up to 16 Weeks @ 2500 EPS	*5 Weeks	10 Weeks @ 1000eps	Up to 90 days @ 10,000 sustained EPS*		Up to 260 days at 10,000 EPS*
Flow Storage	*3 Weeks	NA	*7 Days	14 Days @ 50,000fpi			Up to 130 days at 1.2M Flows*
Network Objects	NA	NA	NA	NA	NA		NA

QFlow Collector Appliances

	1101	1201	1202	1301	1302	1310
Dimensions	1U: Dimensions: 21.5" D x 17.6" W x 1.68" H			1U: Dimensions: 30.4" D x 16.7" W x 1.67" H		
CPU	Quad Core Xeon 2x1MB Cache, 2.40GHz, 1066MHz FSB			Quad Core Xeon with 8MB Cache, 2.4GHz, 5.86 GT/s QPI, TurboHT		
Memory	2GB			6GB		
Storage	NA	NA	NA	NA	NA	NA
Network Interfaces	2x10/100/1000 CX	4x10/100/1000 CX	1x10/100/1000 CX Mngt 4x1000 CX Monitor (Napatech NIC)	1x10/100/1000 CX Mngt 4x1000 SX Monitor (Napatech NIC)	1x10/100/1000 CX Mngt 2x1000 SX Monitor	1x10/100/1000 CX Mngt 2x10GB SR - 850nm or LR - 1310nm (Napatech)
Power	Single power supply (345W)	Dual Redundant Auto Sensing 110/220 Volt Power Supply (670 Watt)				
	Configuration Totals for 110 AC Input Voltage and 77°F Total Input Power: 185.8 watts 633.9 btu/h Total Input Current: 1.7 amps Sound Power Level: 6.2 bels * Airflow Rate: 11.2 l/s 23.7 CFM Total Weight: 17.7 kg 39.0 lbs					
Traffic Rate	50Mbps	200Mbps	2Gbps*	2Gbps*	200Mbps	2Gbps*

questions?

