

IBM SolutionsConnect 2013

Turning Opportunity into Outcomes.



IBM QRadar Security Intelligence

Nico de Smidt

NdS@nl.ibm.com



IBM Security Framework (ISF)



ISF recognises 6 security domains.

Software and appliances for each of these domains can either be of the security enablers or security controllers type.

Depending on the maturity of the security framework implementation one will find either of these types in the domains.

SLIDE VAN ERNO

Customer Challenges



Detecting threats

- Arm yourself with comprehensive security intelligence



Consolidating data silos

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



Detecting insider fraud

- Next-generation SIEM with identity correlation



Better predicting risks to your business

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

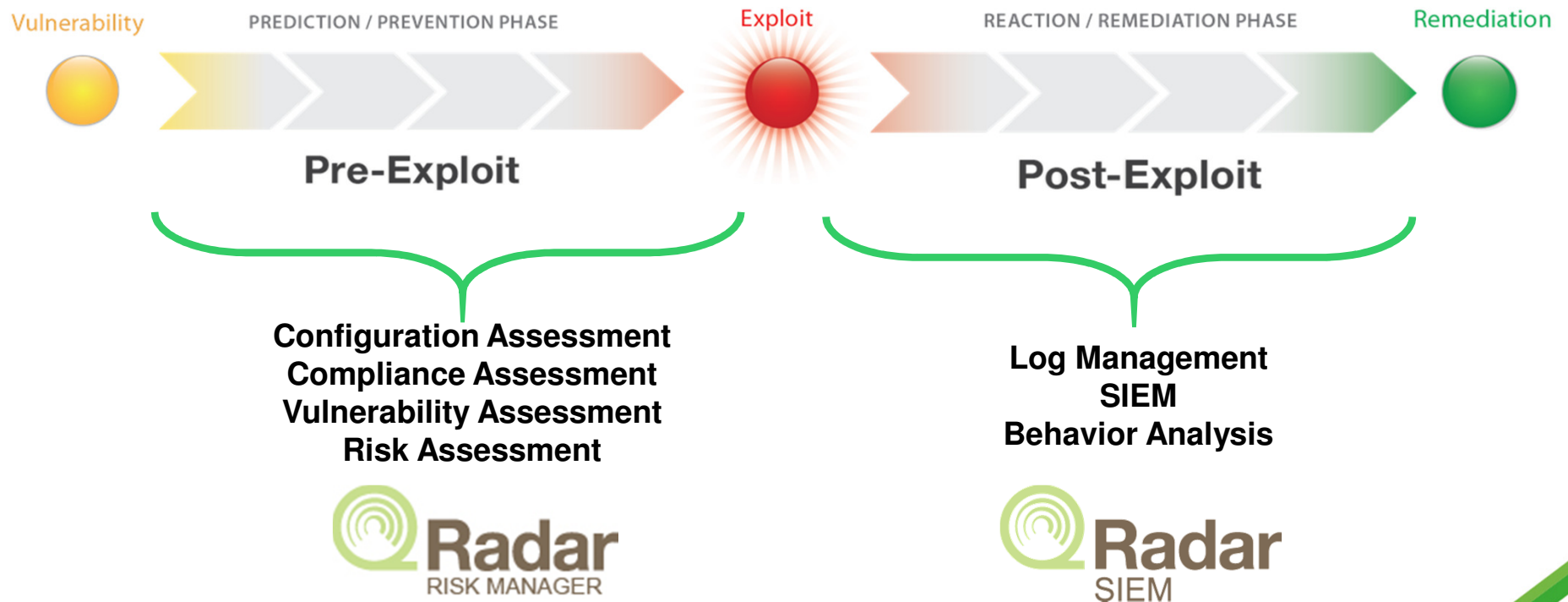


Addressing regulation mandates

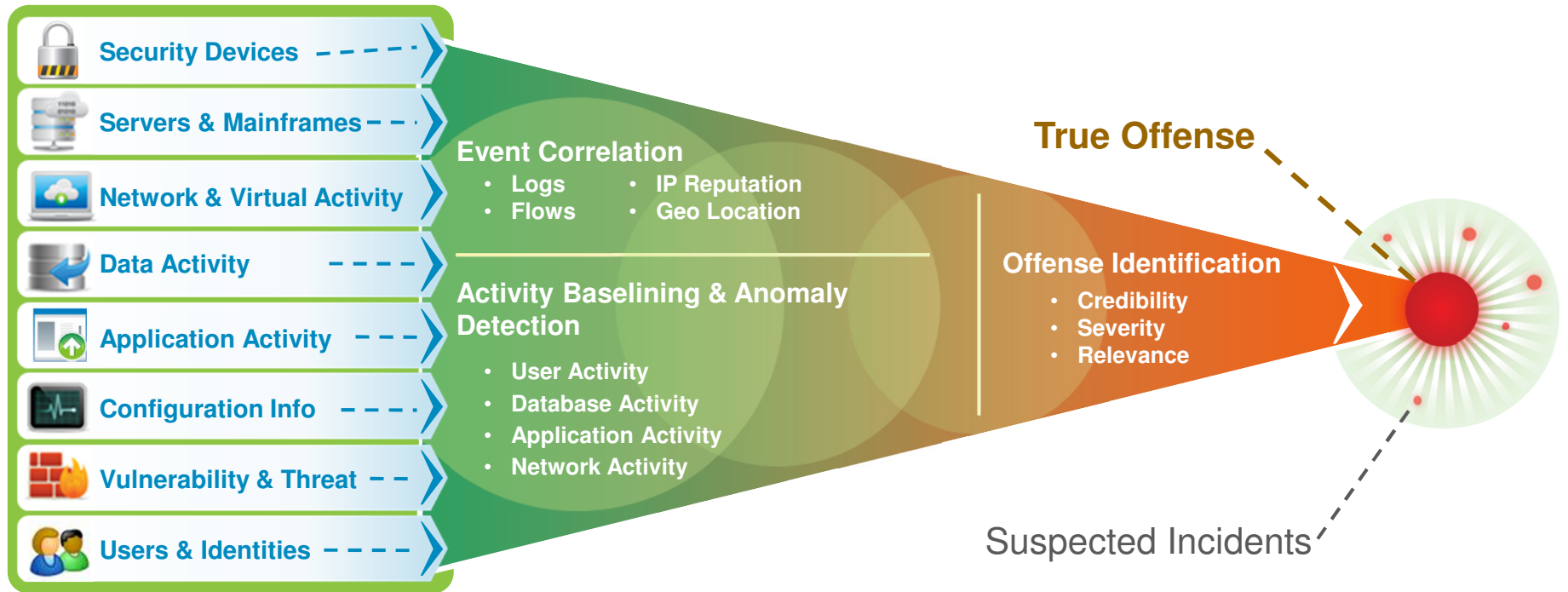
- Automated data collection and configuration audits



Full Compliance and Security Intelligence Time line



Context and Correlation Drive Security Intelligence



Infra, People, Application, Data + Deep Intelligence = Exceptionally Accurate and Actionable Insight

Fully Integrated Security Intelligence in One Console



IBM Security QRadar SIEM

admin | Preferences | Help | IBM

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin

System Time: 07:32

Show Dashboard: CIO View | New Dashboard | Rename Dashboard | Delete Dashboard | Add Item...

Next Refresh: 00:00:45

CIO-Geo (real-time)

Legend

- Asia.Turkey
- NorthAmerica.UnitedStates
- Europe.Ireland
- CentralAmerica.PuertoRico
- other

[View in Network Activity](#)

Most Recent Reports

Report Name	Generated	Formats
Daily User Authentication Activity	2013-02-13 01:00	
Geographic Traffic Distribution	2013-02-13 01:00	
Top IDS/IPS Alerts (Daily)	2013-02-13 01:00	
Top Applications (Internet)	2013-02-13 01:00	
Weekly Firewall Allow Activity	None	

Top Category Types

Category	Offenses
User Login Failure	211
Misc Exploit	65
Misc Login Failed	62
SSH Login Failed	59
General Authentication Failed	53

Most Severe Offenses

Offense Name	Magnitude
Worm Events Detected preceded by IRC Connections	
Exploit/Malware Events Across Multiple Targets	
Exploit/Malware Events Across Multiple Targets	
Worm Events Detected containing WORM: Possible Worm Detected in Attachment	
Worm Events Detected containing HTTP Worm Catcher	

Compliance: Username Involved in Compliance Rules (Event Count)

Reset Zoom | Feb 13 06:38 - Feb 13 07:10

Wednesday, Feb 13 07:08

- Offer Remote Assistance ...pers: 0
- ANONYMOUS LOGON: 0
- a-ewilkin: 0
- Administrator: 0
- a-ttongson: 0
- 3 more...

Legend

- N/A
- Offer Remote Assistance Helpers
- ANONYMOUS LOGON
- a-ewilkin
- Administrator
- a-ttongson
- SVCwwwprod
- svccactsm
- svcRightFax

[View in Log Activity](#)

Event Rate (Events per Second Coalesced - Average 1 Min)

Reset Zoom | Feb 13 06:23 - Feb 13 07:29

Legend

- siem.coe.ibm.com:ecs0/EC/Processor2
- qaZ21.q1labs.lab:ecs0/EC/Processor2
- N/A

[View in Log Activity](#)

Flow Rate (Flows per Second - Peak 1 Min)

Reset Zoom | Feb 13 05:50 - Feb 13 07:28

Legend

- 192.168.10.10/-

[View in Log Activity](#)



Challenge 1: Detecting Threats Others Miss



Potential Botnet Detected?
This is as far as traditional SIEM can go

Magnitude	Relevance
Malware - External - Communication with BOT Control Channel containing Potential Botnet connection - QRadar Classify Flow	6 events in 1 categories
Attacker/Src: 10.103.6.6 (dhcp-workstation-103.6.6.acme.org)	Start: 2009-09-29 11:21:01
Target(s)/Dest: Remote (5)	Duration: 0s
Network(s): other	Assigned to: Not assigned

Notes: Botnet Scenario This offense captures Botnet command channel activity from an internal host. The botnet node communicates with IRC servers running on non-standard ports (port 80/http), which would typically bypass many detection techniques. This sc...

IRC on port 80?
IBM Security QRadar QFlow detects a covert channel

First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Cox	Source Flags
11:19	tcp_ip	10.103.6.6	48667	62.64.54.11	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	50296	192.106.224.13	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	51451	62.181.209.20	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	47961	62.211.73.232	80	IRC	N/A	F,S,P,A

Irrefutable Botnet Communication
Layer 7 flow data contains botnet command control instructions

Source Payload
108 packets,
8850 bytes

UTF Hex Base64

```
NICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombPROTOCTL NAMESX
PROTOCTL NAMESX
PROTOCTL NAMESX
NOTICE Defender :000VERSION xchaNOT
JOIN #botnet_command_channel
JOIN #botnet_command_channel
```

Challenge 2: Consolidating Data Silos



System Summary	
Current Flows Per Second	1.4M
Flows (Past 24 Hours)	1.3M
Current Events Per Second	17,384
New Events (Past 24 Hours)	677M
Updated Offenses (Past 24 Hours)	588
Data Reduction Ratio	310633 : 1

Analyzing both flow and event data. Only IBM Security QRadar fully utilizes Layer 7 flows.

Reducing big data to manageable volumes

Advanced correlation for analytics across silos

Offense 160			
Magnitude		Relevance	5
Description	Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Across Multiple Targets preceded by Aggressive Remote Scanner Detected	Severity	10
Source IP(s)	202.153.48.66	Credibility	8
Destination IP(s)	Local (315)	Offense Type	Source IP
Network(s)	Multiple (2)	Event/Flow count	19984 events and 355 flows in 12 categories.
		Start	2010-10-01 07:51:00
		Duration	2m 52s
		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 (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250).			
The first systems scanned are not vulnerable, but the final system's asset profile has had vulnerability data imported from a Ne			

Challenge 3: Detecting Insider Fraud



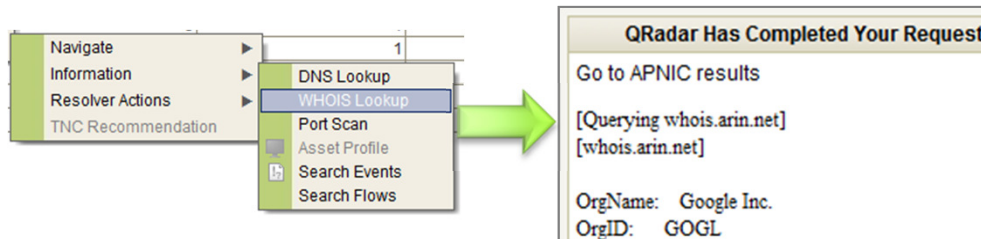
Potential Data Loss
Who? What? Where?

Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.14.139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
	DELETE failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Deny
	SELECT succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Allow
	Misc Logout	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Logout
	Suspicious Pattern Detec	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Suspicious Pattern Detected
	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Remote Access Login Failed

Who?
An internal user

What?
Oracle data



Where?
Gmail



Challenge 4: Better Predicting Risks Pre-exploit Security Intelligence

Assets with High-Risk Vulnerabilities

Questions					
Name	Group	Return Type	Importance Factor	Monitored	
All Systems with Client Side Vulns		Assets	5	No	
All Systems with Client Side Vulns which Communicate to the Internet		Assets	5	No	
All Systems with Client Side which communicate to susp addresses		Assets	5	No	
All Systems with client side with communications and critical data		Assets	5	No	
All vulnerable assets		Assets	5	No	

Description					
Find Assets that are susceptible to vulnerabilities with one of the following classifications (Input Manipulation) and are susceptible to vulnerabilities with CVSS score greater than 9					

Asset Results									
IP	Name	Weight	Destination Port(s)	Protocol(s)	Flow App(s)	Vuln(s)	Flow Count	Source(s)	Destination
10.0.5.68	dhcp-68-building-3.acme.com	0	N/A	N/A	N/A	Multiple (10)	0	N/A	N/A

Which assets are affected?
How should I prioritize them?

What are the details?
Vulnerability details,
ranked by risk score

How do I remediate the
vulnerability?

ID	Vulnerability Name	Description	Risk Score
9723	Multiple Vendor LDAP Server NULL Bind Connection Information Disclosure	Multiple LDAP Server contains a flaw that may lead to an unauthorized information disclosure. A issue is triggered when the LDAP NULL bind entry is enabled by default, which may allow a remote attacker to anonymously view files on the LDAP directory resulting in a loss of confidentiality.	7
57799	Microsoft Windows srv2.sys Kernel Driver SMB2 Malformed NEGOTIATE PROTOCOL REQUEST Remote DoS	Microsoft Windows contains a flaw that may allow a malicious user to execute arbitrary code. The issue is triggered when a malicious user sends a specially crafted NEGOTIATE PROTOCOL REQUEST SMB2 packet with an & (ampersand) character in a Process ID High header field, causing an attempted dereference of an out-of-bounds memory location. It is possible that the flaw may allow arbitrary code execution resulting in a loss of integrity.	10
297	Microsoft Windows Installation ADMIN\$ Share Arbitrary Access	Microsoft Windows contains a flaw that may allow a remote attacker to bypass authentication settings. The issue is triggered during the installation routine, which does not activate the Administrator password upon reboot. It is possible that the flaw may allow a remote attacker to arbitrary access the ADMIN\$ share without a password, resulting in a loss of confidentiality and/or integrity.	10

Days of Exposure	
36 days	

Description	
Microsoft Windows contains a flaw that may allow a malicious user to execute arbitrary code. The issue is triggered when a malicious user sends a specially crafted NEGOTIATE PROTOCOL REQUEST SMB2 packet with an & (ampersand) character in a Process ID High header field, causing an attempted dereference of an out-of-bounds memory location, resulting in a loss of integrity.	

Classification	
Location: Remote / Network Access	
Attack Type: Denial of Service, Input Manipulation	
Impact: Loss of Confidentiality, Loss of Availability	
Solution: Patch / RCS	
Exploit: Exploit Public, Exploit Commercial	
Disclosure: Vendor Verified, Uncoordinated Disclosure	

Solution	
Currently, there are no known workarounds or upgrades to correct this issue. However, Microsoft Corporation has released a patch to address this issue.	

Challenge 5: Addressing Regulatory Mandates



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 category
Attacker/Src	10.103.12.12 (dhep-workstation-103-12-12.acme.org)	Start	2009-09-29 15:09:00
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 identifies such activity. In this offense the system has captured cleartext network activity (telnet and FTP) to		

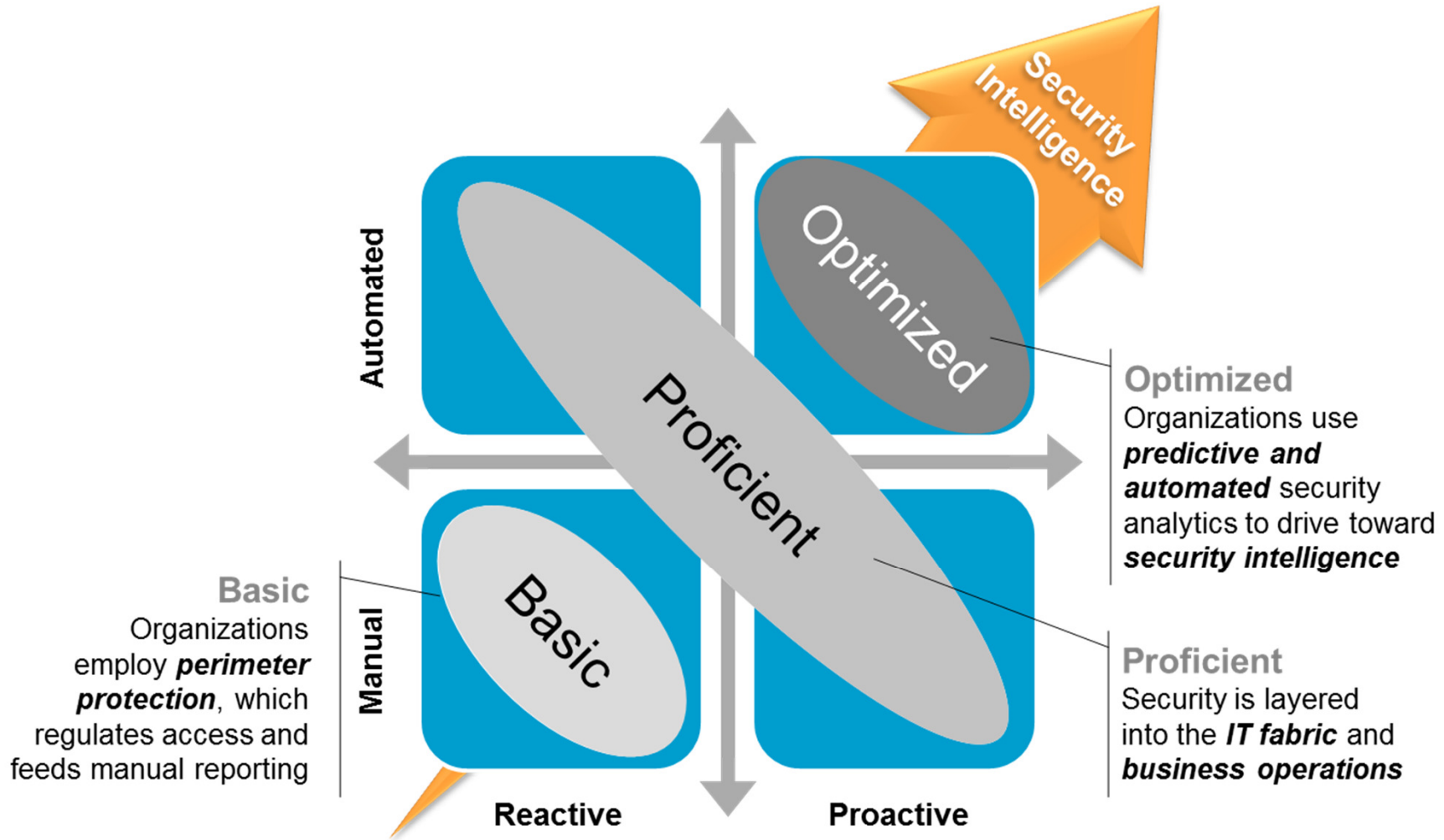
PCI compliance at risk?
Real-time detection of possible violation



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
IBM Security QRadar QFlow saw a cleartext service running on the Accounting server
PCI Requirement 4 states: Encrypt transmission of cardholder data across open, public networks

Get an Intelligent View into your Security Posture



QRadar's Unique Advantages



- Real-time context driven correlation and anomaly detection

➤ *Impact: More accurate threat detection, in real-time*



- Integrated flow analytics with Layer 7 application visibility

➤ *Impact: Superior situational awareness and threat identification*



- Automated data collection, asset discovery and asset profiling

➤ *Impact: Reduced manual effort, fast time to value, lower-cost operation*



- Easy to use and edit correlation rules, reports and dashboards

➤ *Impact: Maximum insight, business agility and lower cost of ownership*



- Scalability for largest deployments

➤ *Impact: QRadar supports your business needs at any scale*

ibm.com/security

