IBM SolutionsConnect 2013
Turning Opportunity into Outcomes.

Defend your organization and keep attackers at bay with Security Intelligence

Nico de Smidt, IBM Security

Peter Mesker, SecureLink

IBM Security Framework (ISF)

ISF recognises 6 security domains.

Software and appliances for each of these doamins 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

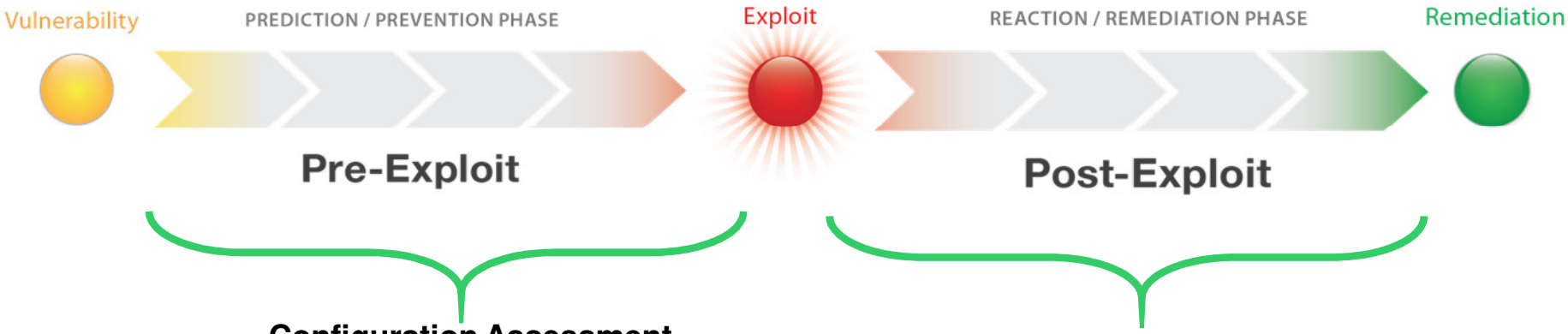
Better predicting risks to your business

- 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



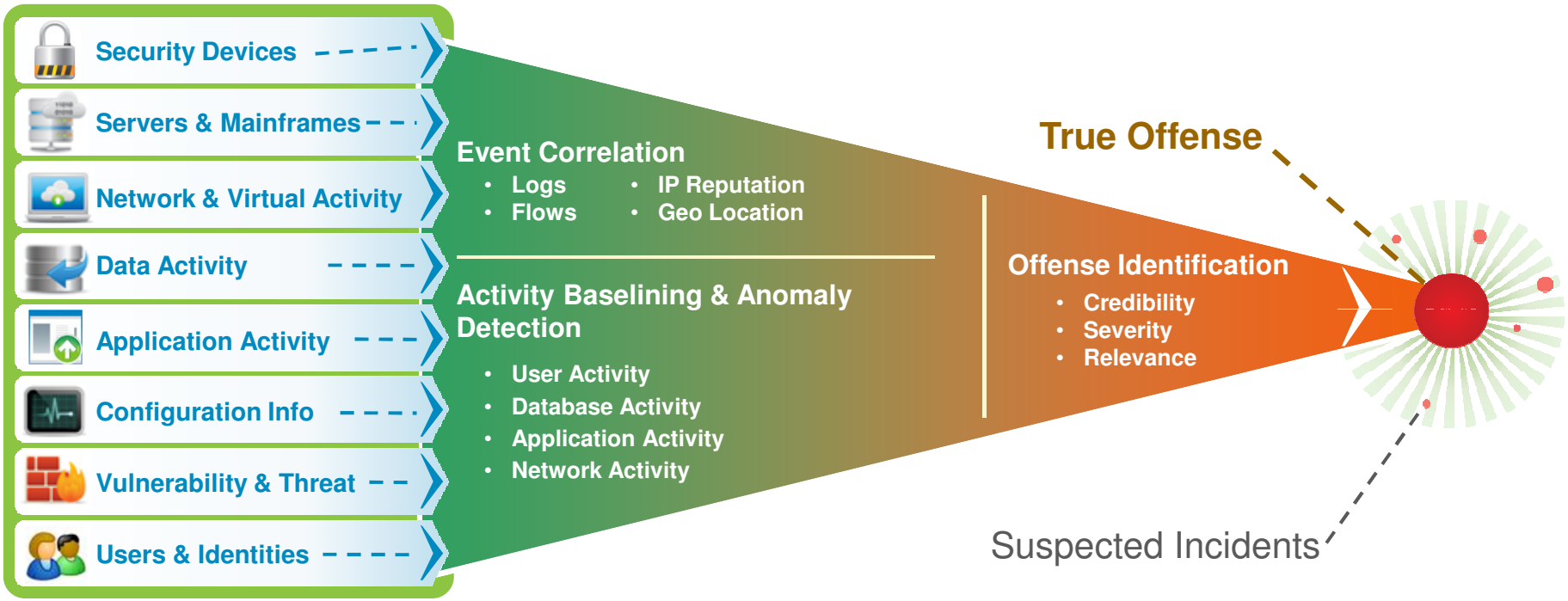
Configuration Assessment
Compliance Assessment
Vulnerability Assessment
Risk Assessment

Radar RISK MANAGER

Log Management
SIEM
Behavior Analysis

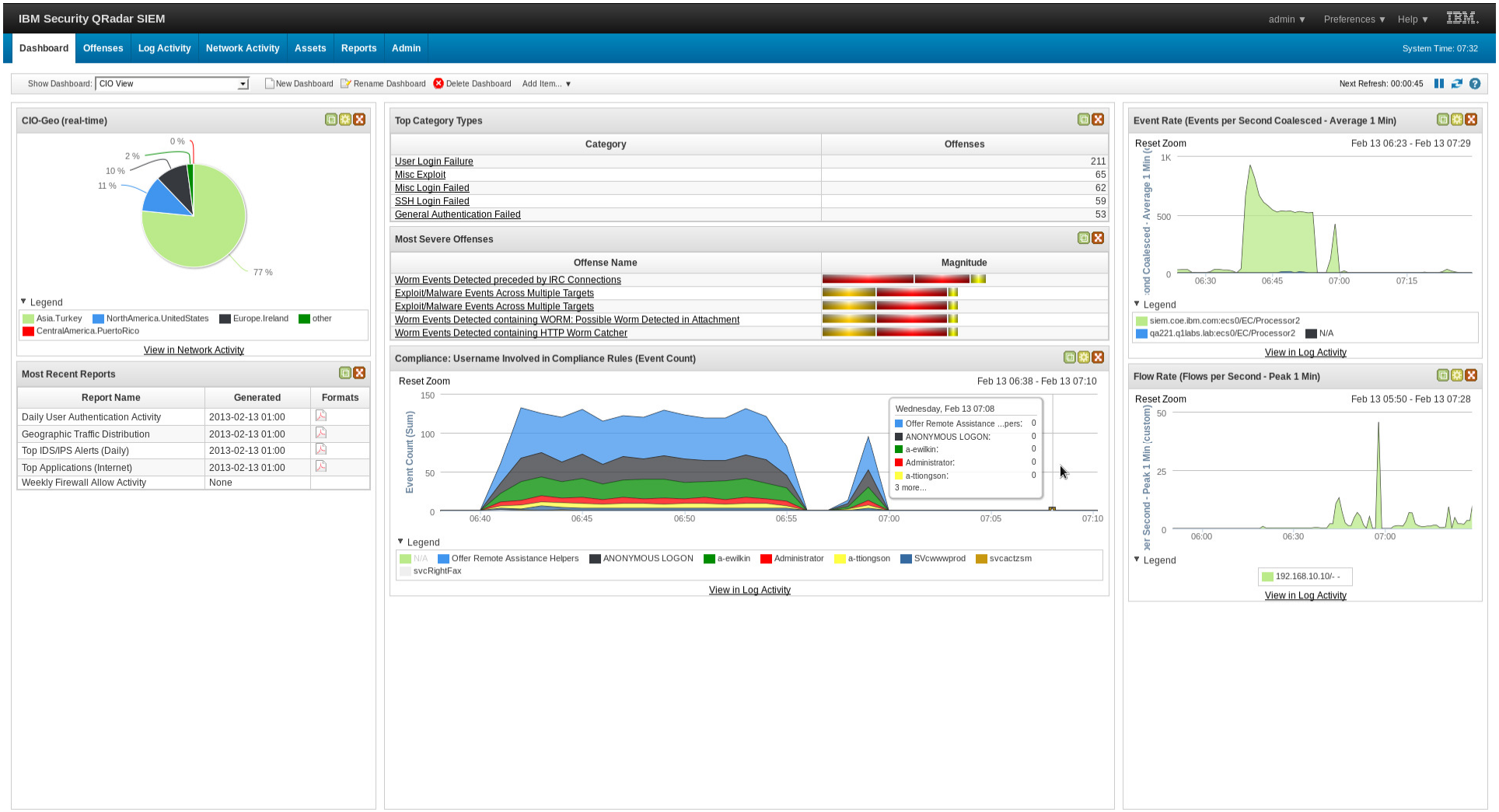
Radar SIEM

Context and Correlation Drive Security Intelligence



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

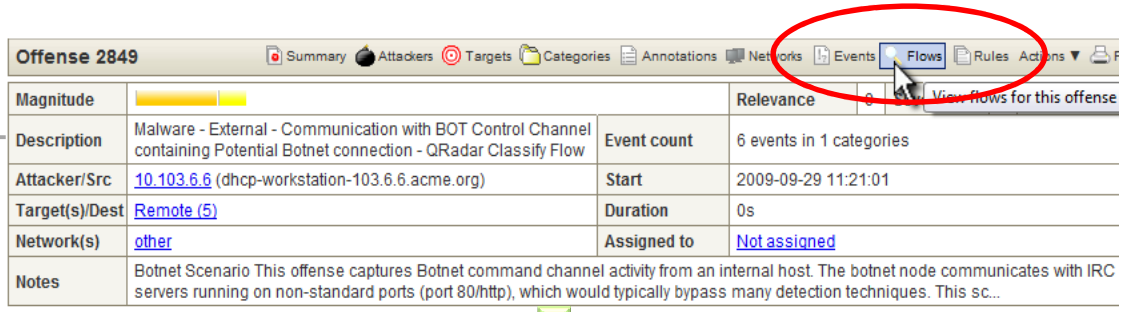
Fully Integrated Security Intelligence in One Console



Challenge 1: Detecting Threats Others Miss

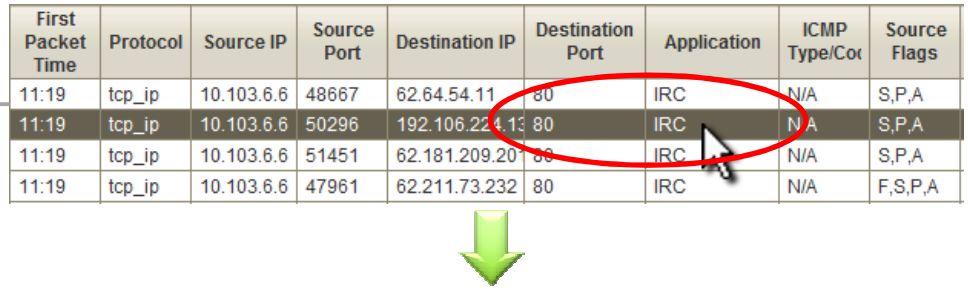
Potential Botnet Detected?

This is as far as traditional SIEM can go



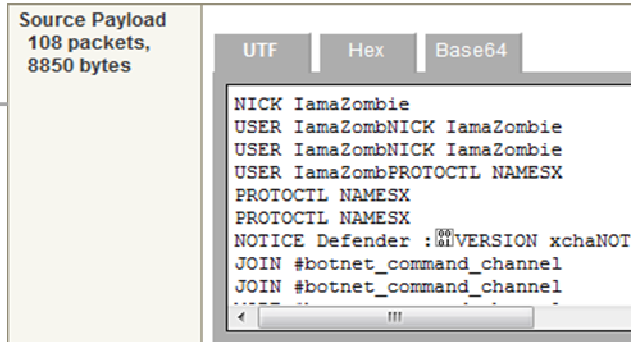
IRC on port 80?

IBM Security QRadar QFlow detects a covert channel



Irrefutable Botnet Communication

Layer 7 flow data contains botnet command control instructions



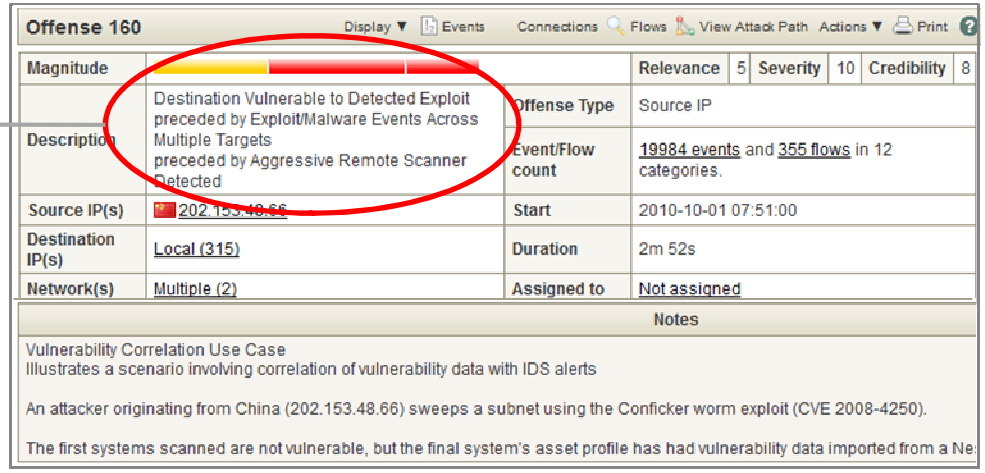
Challenge 2: Consolidating Data Silos

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



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 ...

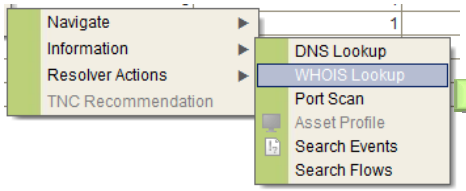
	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
	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



QRadar Has Completed Your Request

Go to APNIC results

[Querying whois.arin.net]
[whois.arin.net]

OrgName: Google Inc.
OrgID: GOGL

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 0

Risk Score for the selected question is 3

Asset Results

IP	Name	Weight	Destination Port(s)	Protocol(s)	Flow App(s)	Vuln(s)	Flow Count	Source(s)	Destinat
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?

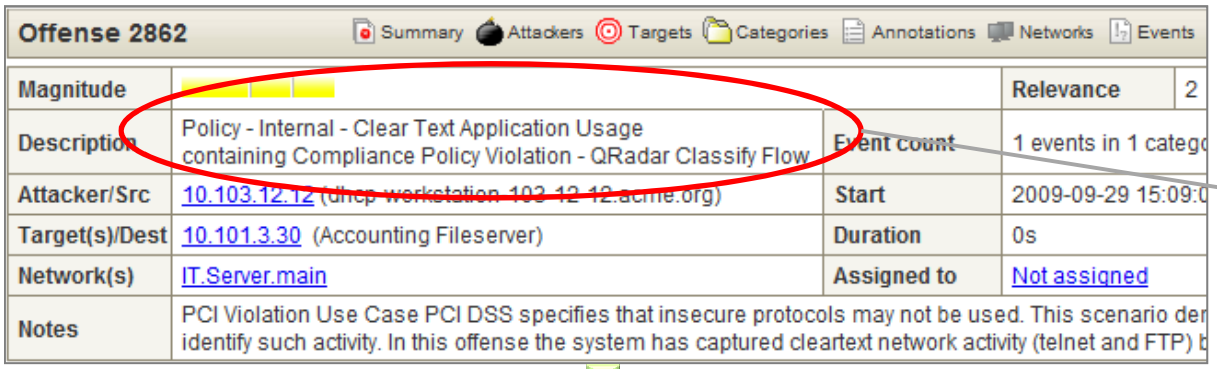
What are the details?
Vulnerability details, ranked by risk score

9723	Multiple Vendor LDAP Server NULL Bind Connection Information Disclosure	Multiple LDAP Server contains a flaw that may lead to an unauthorized information disclosure. Â The 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 SMBv2 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 SMBv2 packet with an & (ampersand) character in a Process ID High header field, causing an attempted dereference of an out-of-bour arbitrary code execution 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 t

How do I remediate the vulnerability?

Challenge 5: Addressing Regulatory Mandates



Offense 2862	Summary	Attackers	Targets	Categories	Annotations	Networks	Events
Magnitude					Relevance	2	
Description	Policy - Internal - Clear Text Application Usage containing Compliance Policy Violation - QRadar Classify Flow			Event count	1 events in 1 categ		
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

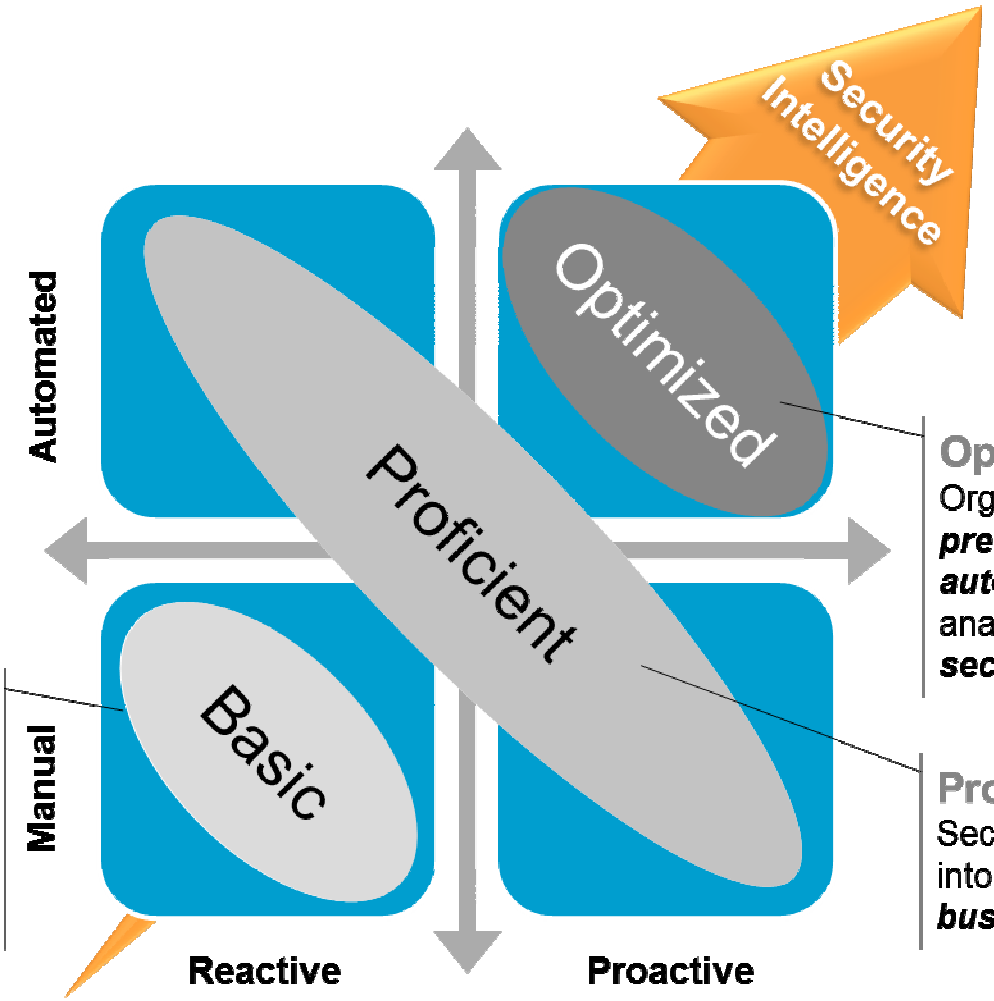
Event Name	Log Source	Source IP	Source Port	Destination IP	Destination Port
Compliance Policy Violation - C	Flow Classification Engine-5 :	10.103.12.12	1482	10.101.3.30	23

Unencrypted Traffic

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



Basic
Organizations employ ***perimeter protection***, which regulates access and feeds manual reporting

Optimized
Organizations use ***predictive and automated*** security analytics to drive toward ***security intelligence***

Proficient
Security is layered into the ***IT fabric*** and ***business operations***

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 SolutionsConnect 2013
Turning Opportunity into Outcomes.

Security Intelligence

Peter Mesker
SecureLink

Security & Networking Integrator

2003 opgericht

>100 SecureLinkers

30% is opgenomen in AEX

>2500 appliances in onderhoud

85 % van de support calls wordt zelf afgehandeld

>250 certificaten | **45** engineers

9 oplossingsgebieden binnen **5** thema's

End-to-end management

Security & network visibility, correlation
Security Information & Event Management,
Network Behavior & Anomaly Detection
Network Change & Configuration Management
Risk Analysis

- Toename aantal security devices, policies en logging
- Behoefte security event management en centralisatie en correlatie van log informatie
- Real-time rapportage
- Network automation
- Centraal management dashboard
- Compliancy

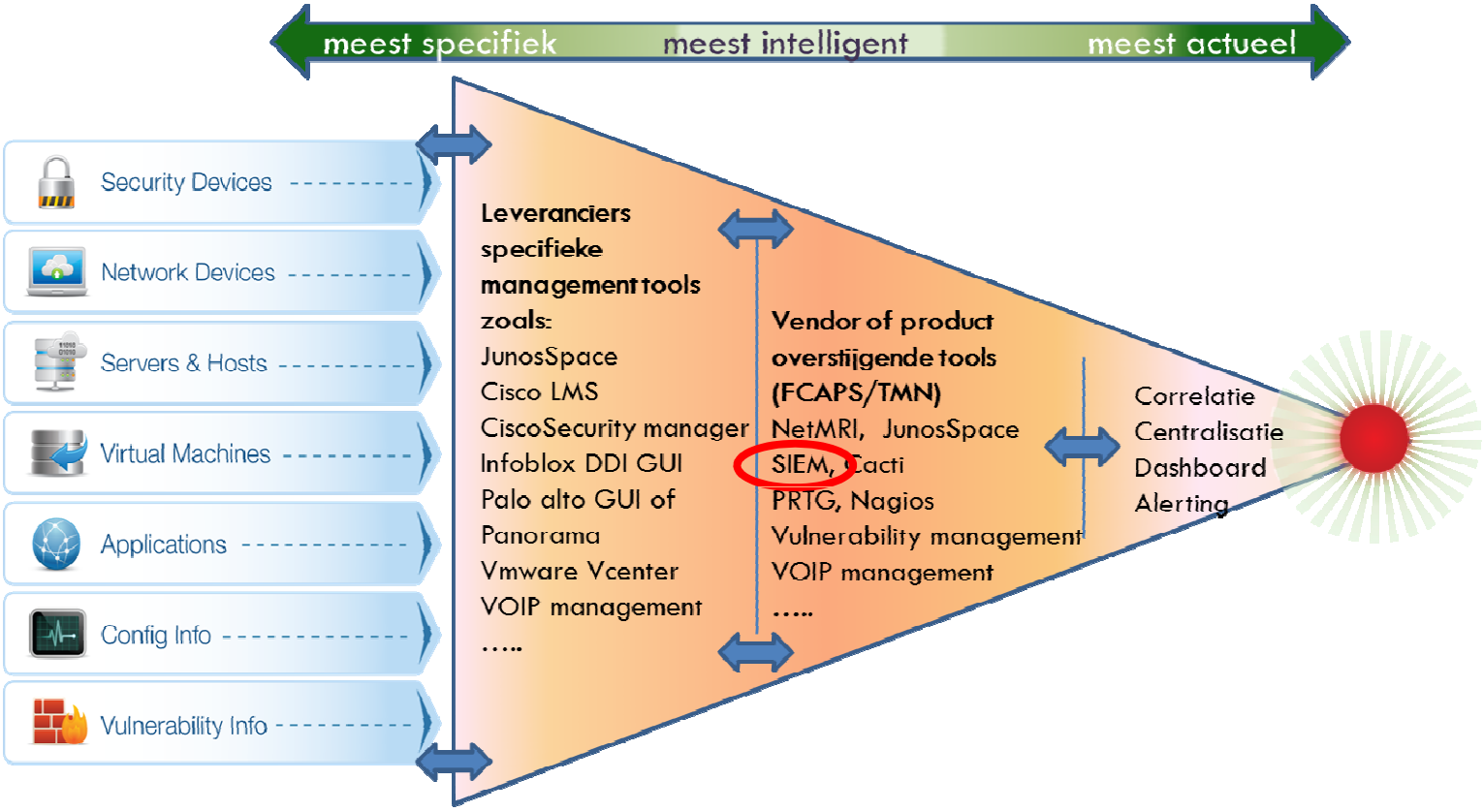
Uitdagingen voor grote gemeente in Nederland

- ✓ Nieuwe private cloud gebaseerde infrastructuur
- ✓ Multi tenancy (gemeente is tevens service provider)
- ✓ Next generation security oplossingen
- ✓ Retentie, compliancy
- ✓ Security onderdeel van het IT proces

Hoe behoudt men zichtbaarheid en controle in deze complexe infrastructuur?

Mogelijke antwoorden:
Vendor specifieke tools, open source tools zoals (MRTG, CACTI), outsourcen, syslog server, flow collector, splunk, …

Beter antwoord | Creëer een integrated end-to-end management oplossing



Northbound verkeer
SNMP traps, syslog, netflow, backup, alert, ….

Southbound verkeer
SNMP set/get, ssh, XML, firmware upgrade, …

SIEM teleurstellingen

- ✓ 100k verder en nog niet compliant!
- ✓ Gehacked ondanks SIEM!
- ✓ Beleid schrijft SIEM voor, maar niemand wil het betalen…
- ✓ SIEM? Vertrouw je ons niet?

SIEM business succesfactoren

(deze vijf stappen heeft de gemeente doorlopen alvorens te gunnen)

Vaststellen businessdrivers

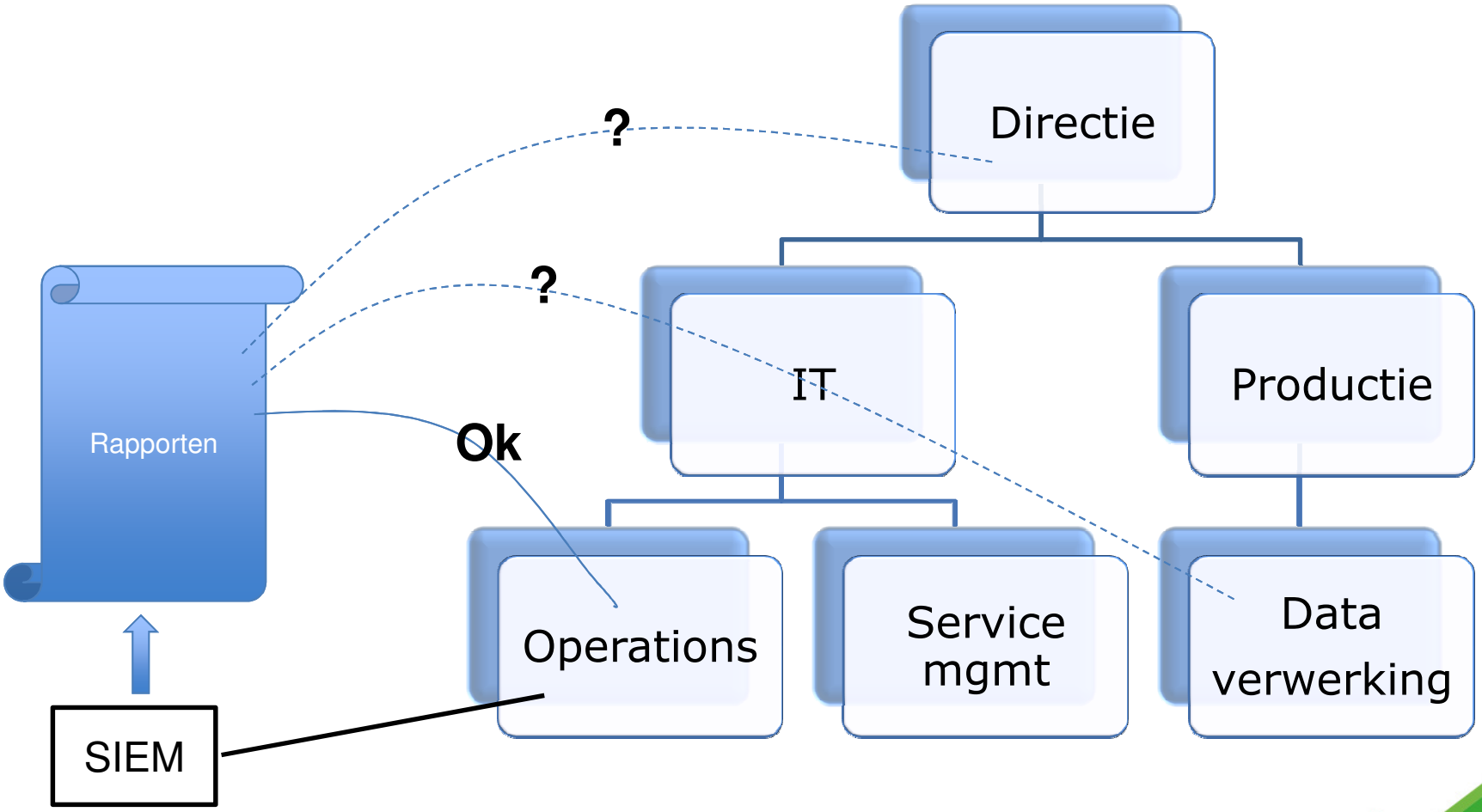
Vaststellen potentiele afnemers

Start architectuur bepalen

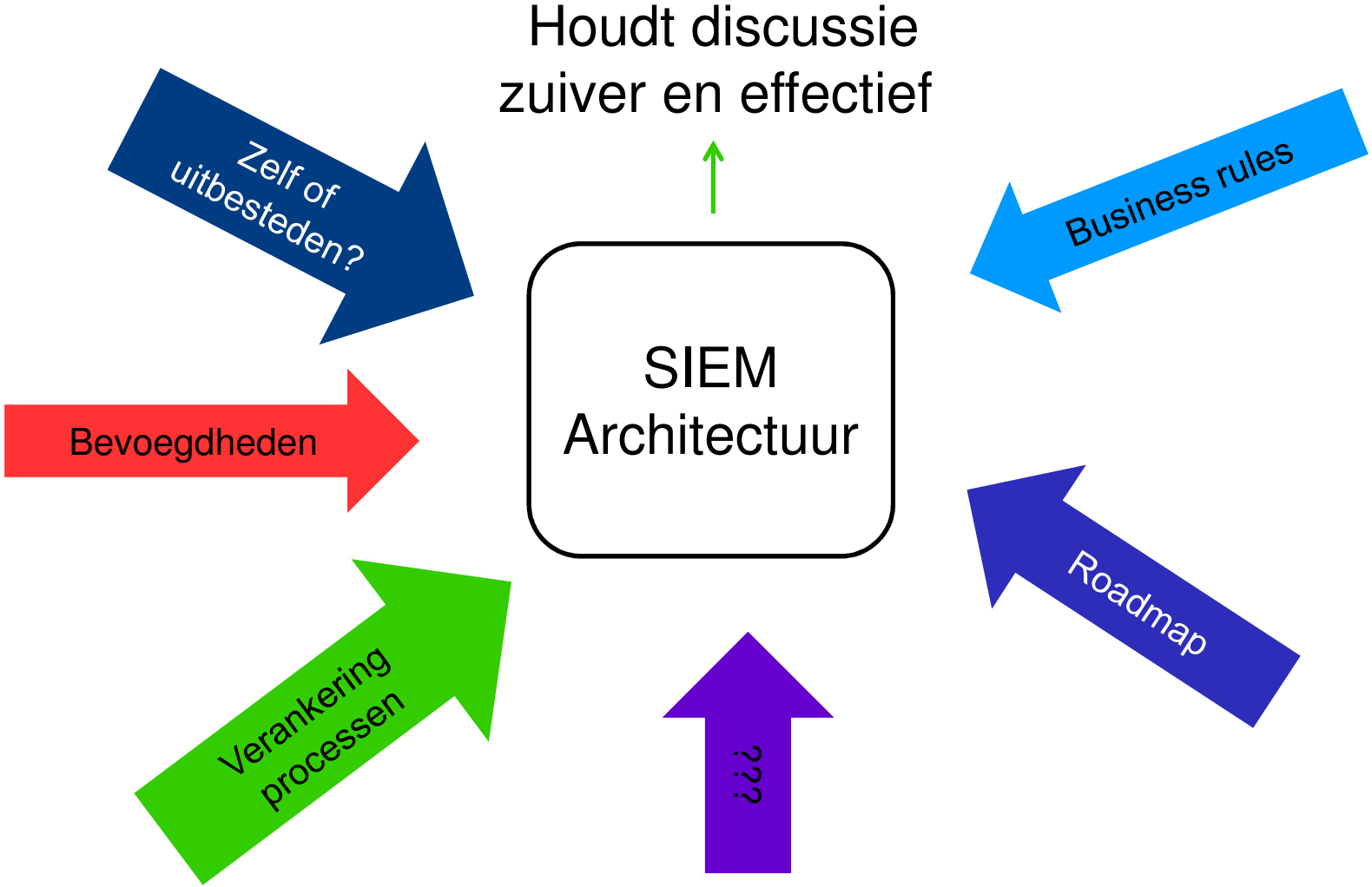
Financieringsmodel afstemmen

Product / dienst selectie

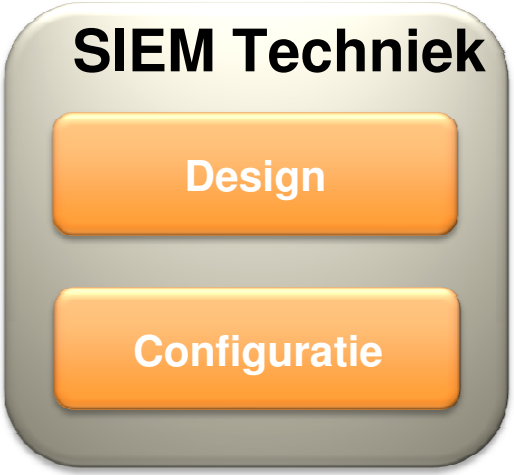
Wie zijn aan de klantkant de afnemers van SIEM



Architectuur SIEM



SIEM Techniek | Waarom QRadar



- ✓ Appliances en virtualisatie
- ✓ Rollen
- ✓ Opslag, retentie
- ✓ Compliancy

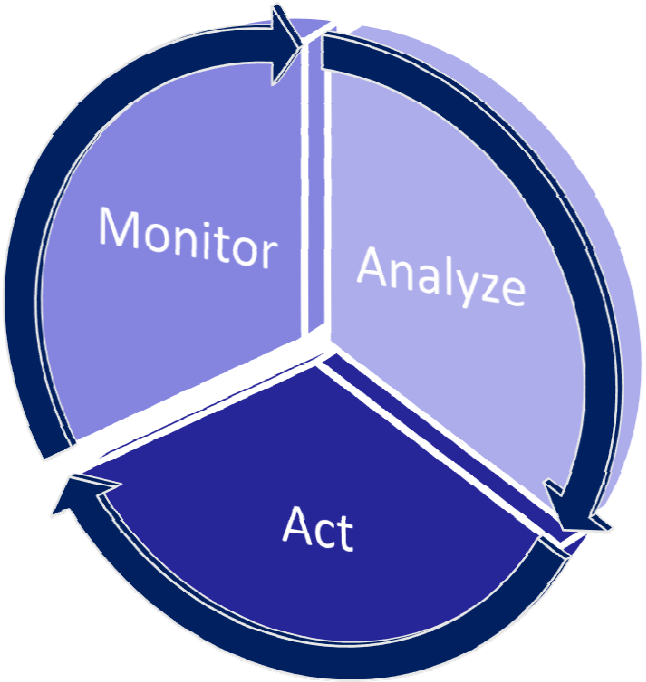
- ✓ Marktleider
- ✓ Referenties
- ✓ Roadmap
- ✓ Ease of deployment

Sizing en plaatsing

- ✓ Wat is relevant?
- ✓ Schaalbaarheid
- ✓ Event informatie
- ✓ Flow informatie

Configuratie en integratie

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

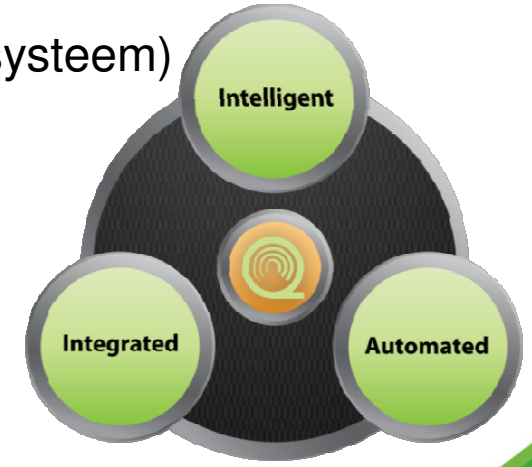


- ✓ Asset-based prioritization
- ✓ Auto-update of threats
- ✓ Auto-response
- ✓ Directed remediation

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

Benefits voor grote gemeente

- ✓ Real time dashboard voor threat detectie en detectie van security incidenten
- ✓ Goede analyse van impact en relevantie van een offense
- ✓ Verminderde manuele acties,
- ✓ Goede prijs/pret verhouding
- ✓ Maximale inzicht, grip op de business
- ✓ Goed integratie (bijv. Met Vulnerability Management systeem)
- ✓ Schaalbaar



ibm.com/security
smartersecurity.nl