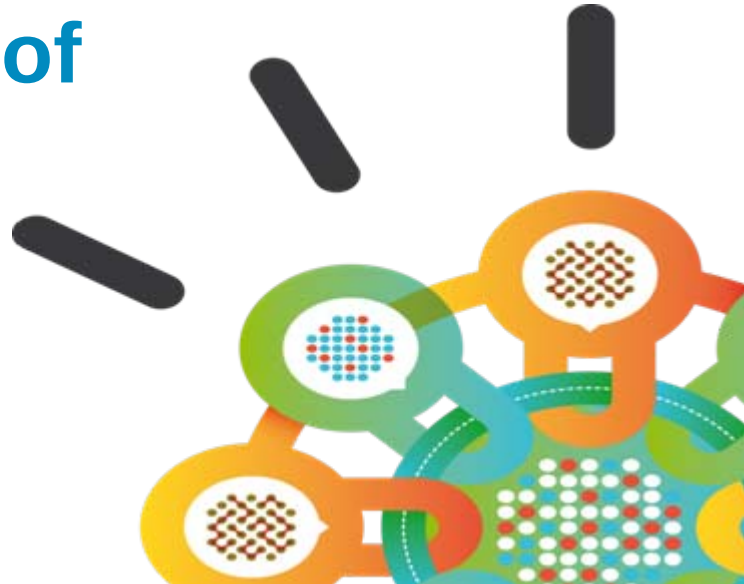
Security Intelligence.
Think Integrated.

No One is Immune to Being Hacked:

Strategies for Staying Out of the Headlines

QRadar Security Intelligence Platform



"Our most formidable challenge is getting companies to detect they have been compromised …"

Kim Peretti, senior counsel,
US Department of Justice (DoJ)

Source: http://www.scmagazine.com/rsa-conference-gonzalez-may-receive-largest-ever-us-hacking-sentence/article/165215/ – March 2010

Attacks from All Sides

‘Flame’ cyber espionage worm

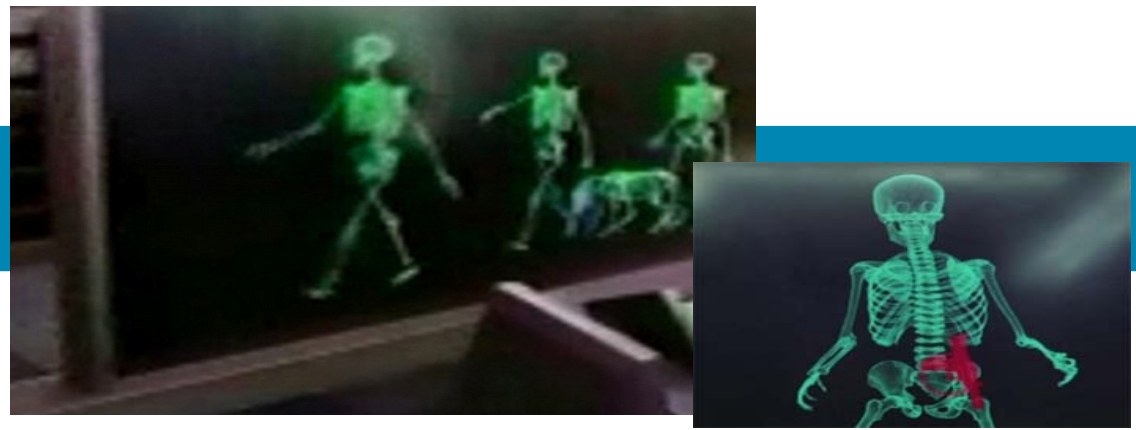
- Successor to Duqu and Stuxnet
- Targeted Attack!
- What is it?
  - Sophisticated Attack Toolkit
  - Backdoor, Trojan, Worm-Like
- Exploits Current Vulnerabilities

…but all is not lost…

Choose the Right Technology

Protection technology is critical, but choose wisely

There is no magic security technology



People and Processes First

A lesson from airport security:

Instead of expensive equipment, use what works

In Israel

- No plane departing Ben Gurion Airport has ever been hijacked
- Use human intelligence
- “Questioning” looks for suspicious behavior
- Simple metal detectors

Scotland Yard

- 24+ men planned to smuggle explosive liquids
- Foiled beforehand because of intelligence
- Before they even got to the airport

What Can Help You Defend Against an APT?

❖ Focus on both prevention and detection

- A truly advanced and persistent adversary will breach your defenses
- How quickly you detect the breach will determine its impact

❖ Smart *preventive* measures reduce weaknesses…

- Control your endpoints – Make sure patches are up to date
- Audit Web applications
- Find and remediate bad passwords
- Monitor device configurations for errors and vulnerabilities

❖ And advanced *detection* finds intrusions faster & assesses impact

- Flow analytics and network anomaly detection
- User anomaly detection
- Reconnaissance detection
- Stealthy malware detection
- Database monitoring

Q1 Labs®
Total Security Intelligence | An IBM Company

Security Intelligence Use Cases

How Security Intelligence Can Help

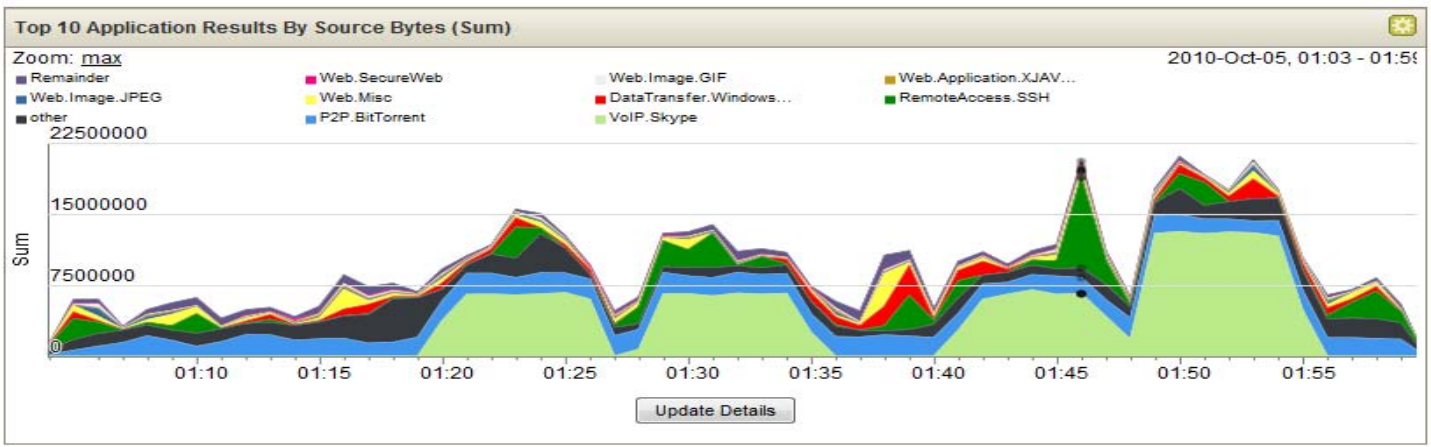
- **Continuously monitor** all activity and correlate in real-time
- Gain visibility into *unauthorized or anomalous* activities
  - Server (or thermostat) communicating with IP address in China
  - Unusual Windows service -- backdoor or spyware program
  - Query by DBA to credit card tables during off-hours – possible SQL injection attack
  - Spike in network activity -- high download volume from SharePoint server
  - High number of failed logins to critical servers -- brute-force password attack
  - Configuration change -- unauthorized port being enabled for exfiltration
  - Inappropriate use of protocols -- sensitive data being exfiltrated via P2P

Why Should You Care?

- Detect suspicious behavior
  - Privileged actions being conducted from a contractor's workstation
  - DNS communications with external system flagged as malicious
- Detect policy violations
  - Baseline against reality (CMDB)
  - Social media, P2P, External File Sharing, etc.
- Detect APTs
  - File accesses out of the norm—behavior anomaly detection
  - Least used applications or external systems; occasional traffic
- Detect fraud
  - Determine baselines on credit pulls or trading volumes, and detect anomalies
  - Correlate eBanking PIN change with large money transfers
- Forensic evidence for prosecution
- Impact analysis
- Compliance
  - Change & configuration management
- Metrics

Network Activity Monitoring (Network Flows)

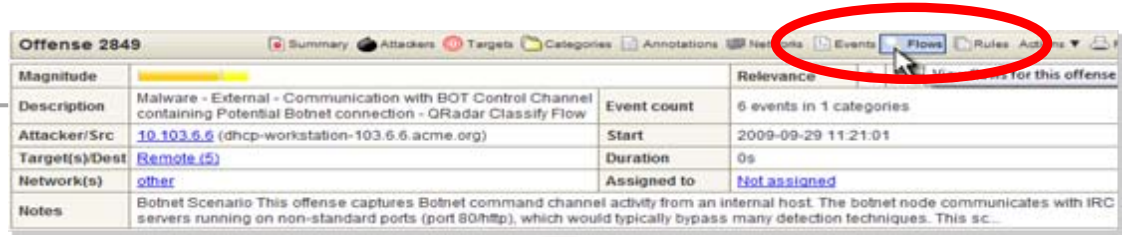
- Attackers can stop logging and erase their tracks, but can't cut off the network
- Helps detect day-zero attacks with no signature; provides visibility into attacker communications
- Network activity can build up an asset database and profile assets
- Useful for non-security related issues as well



Application and Threat Detection with Forensic Evidence

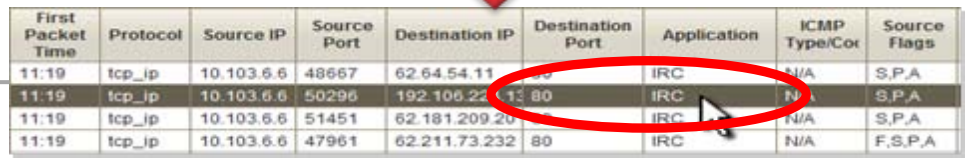
Potential Botnet Detected?

This is as far as traditional SIEM can go



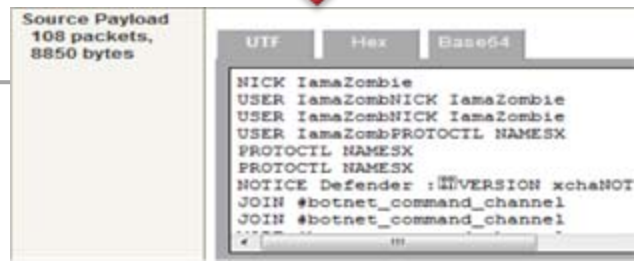
IRC on port 80?

IBM Security QRadar QFlow detects a covert channel



Irrefutable Botnet Communication

Layer 7 flow data contains botnet command control instructions



Application layer flow analysis can detect threats others miss

Detecting Insider Fraud and Data Loss

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)
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-vm	N/A	Suspicious Pattern Detected
	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vm	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

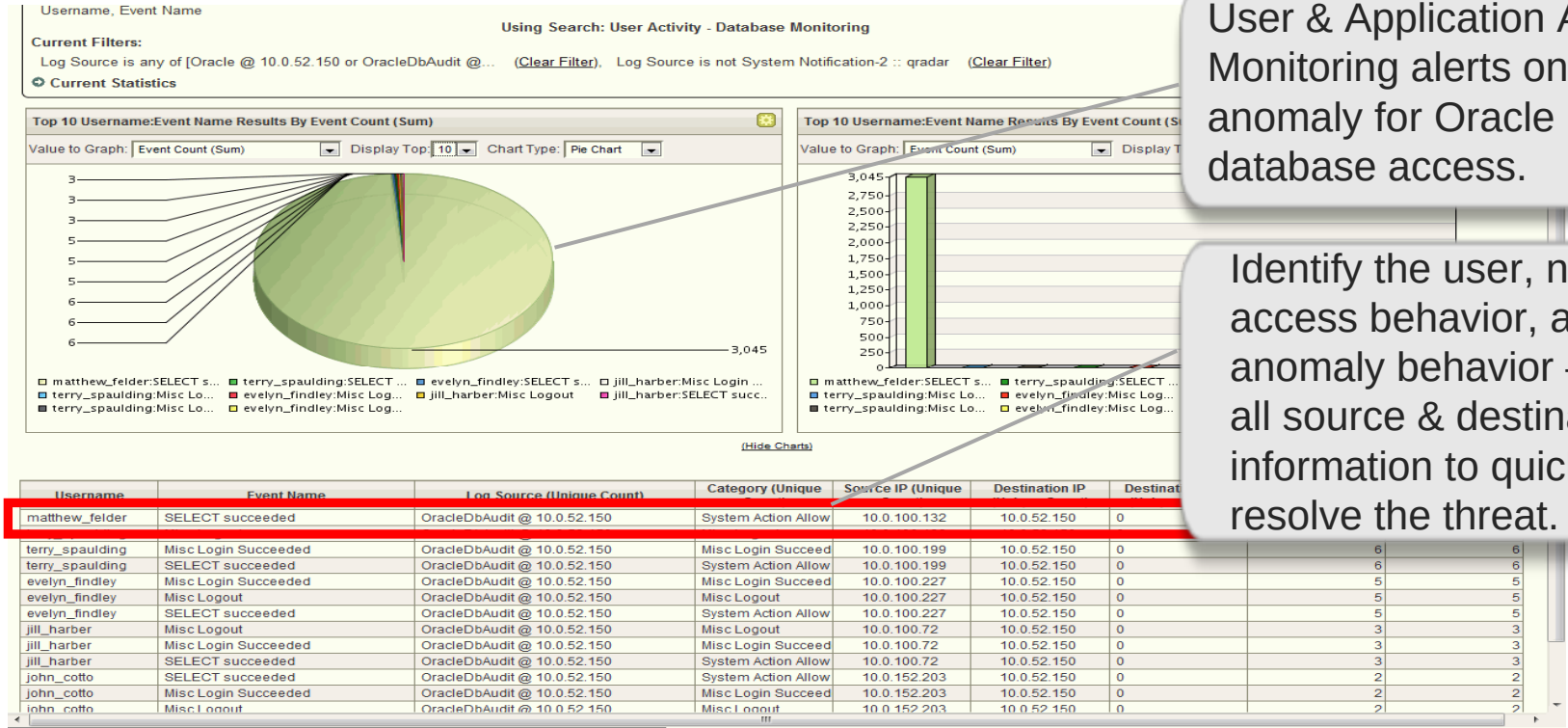
Where?

Gmail

Threat detection in the post-perimeter world

User anomaly detection and application level visibility are critical to identify inside threats

User Activity Monitoring to Combat Advanced Persistent Threats

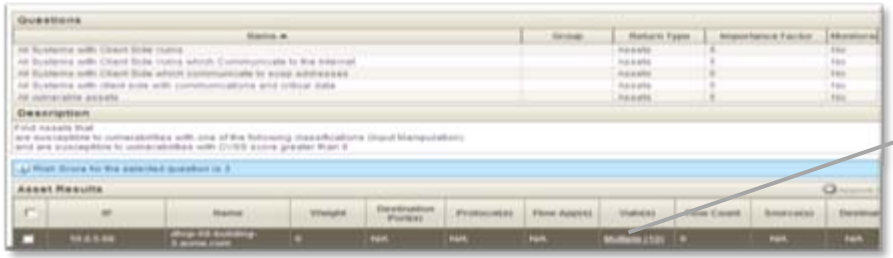


User & Application Activity Monitoring alerts on a user anomaly for Oracle database access.

Identify the user, normal access behavior, and the anomaly behavior – with all source & destination information to quickly resolve the threat.

Predicting Risks to Your Business

Assess assets with high-risk input manipulation vulnerabilities



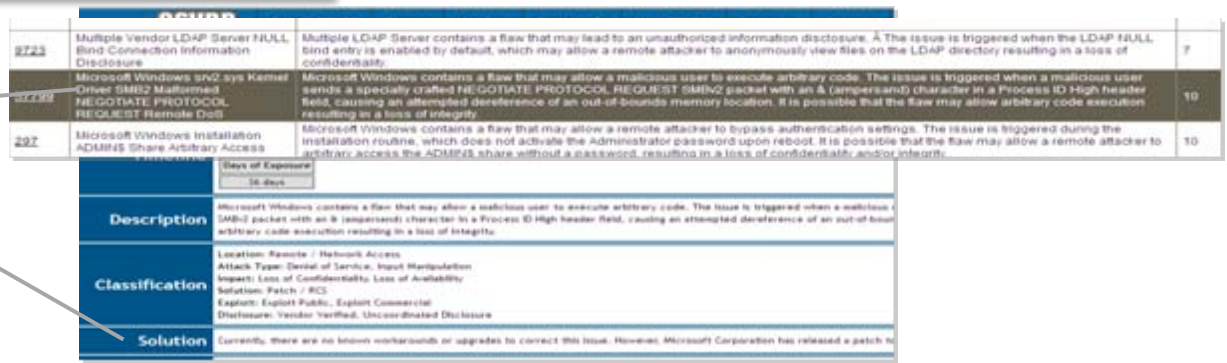
Which assets are affected?

How should I prioritize them?

What are the details?

Vulnerability details, ranked by risk score

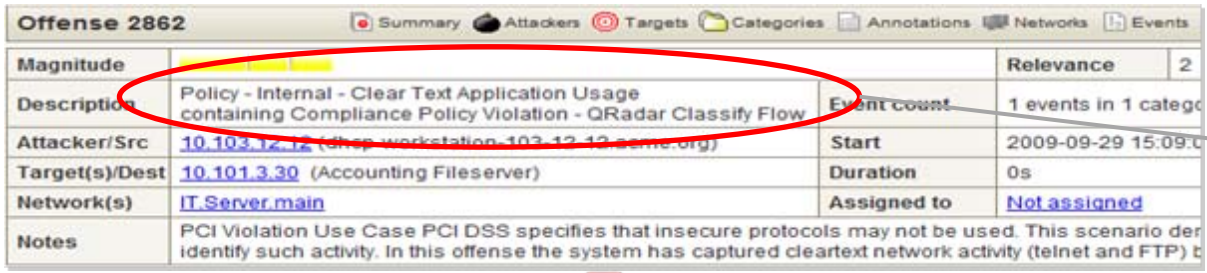
How do I remediate the vulnerability?



Pre-exploit Security Intelligence

Monitor the network for configuration and compliance risks, and prioritize them for mitigation

Exceeding Regulation 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.some.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) t		

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 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 all major compliance and regulatory standards

Automated reports, pre-defined correlation rules and dashboards

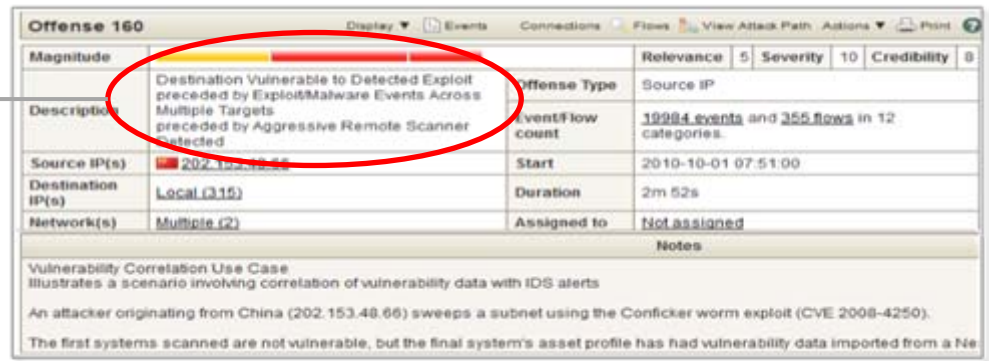
Consolidating Data Silos

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	1153571 : 1

Analyzing both flow and event data – only IBM QRadar can do this

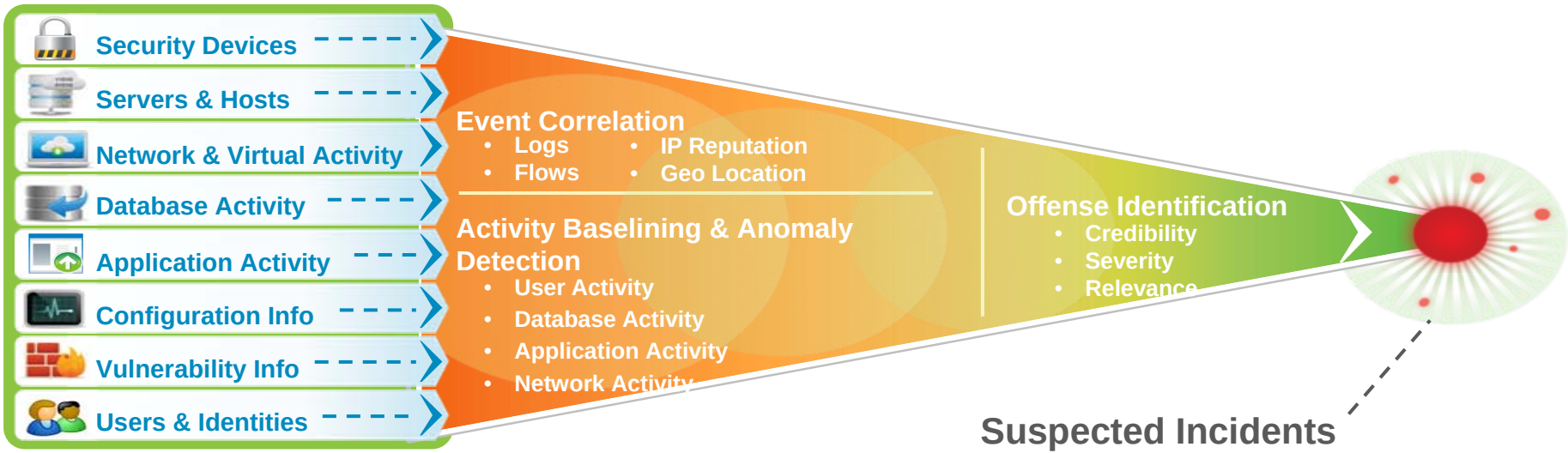
Reducing big data to manageable volumes

Advanced correlation for analytics across silos



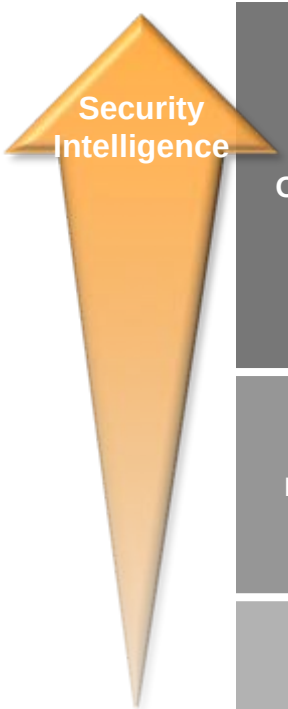
Most Data Sources + Intelligence = Most Accurate and Actionable Insight

Context and Correlation Drive Deep Insight



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

Security Intelligence is Enabling Progress to Optimized Security



	People	Data	Applications	Infrastructure
Optimized	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Secure systems
Proficient	User provisioning Access mgmt Strong authentication	Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset mgmt Endpoint / network security management
Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus

Security Intelligence:
Information and event management
Advanced correlation and deep analytics
External threat research

Solving Complex Problems for Clients

Major Electric Utility	Detecting threats	• Discovered 500 hosts with “Here You Have” virus, which other solutions missed
Fortune 5 Energy Company	Consolidating data silos	• 2 Billion logs and events per day reduced to 25 high priority offenses
Branded Apparel Maker	Detecting insider fraud	• Trusted insider stealing and destroying key data
$100B Diversified Corporation	Predicting risks against your business	• Automating the policy monitoring and evaluation process for configuration change in the infrastructure
Industrial Distributor	Addressing regulatory mandates	• Real-time extensive monitoring of network activity, in addition to PCI mandates

What to do next?

Download the Gartner SIEM Magic Quadrant Report: bit.ly/SIEM-MQ

Read the Q1 Labs Blog: blog.q1labs.com

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

Follow us on Twitter: @q1labs @ibmsecurity

ibm.com/security

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.