21st August 2012 | Thailand

Security Intelligence - How to protect against targeted attacks, insider fraud, and unauthorized configuration changes?

Tan Ching Song,IBM Q1labs,
APAC Technical Sales

Pulse Comes to You 2012

Business without **LIMITS**

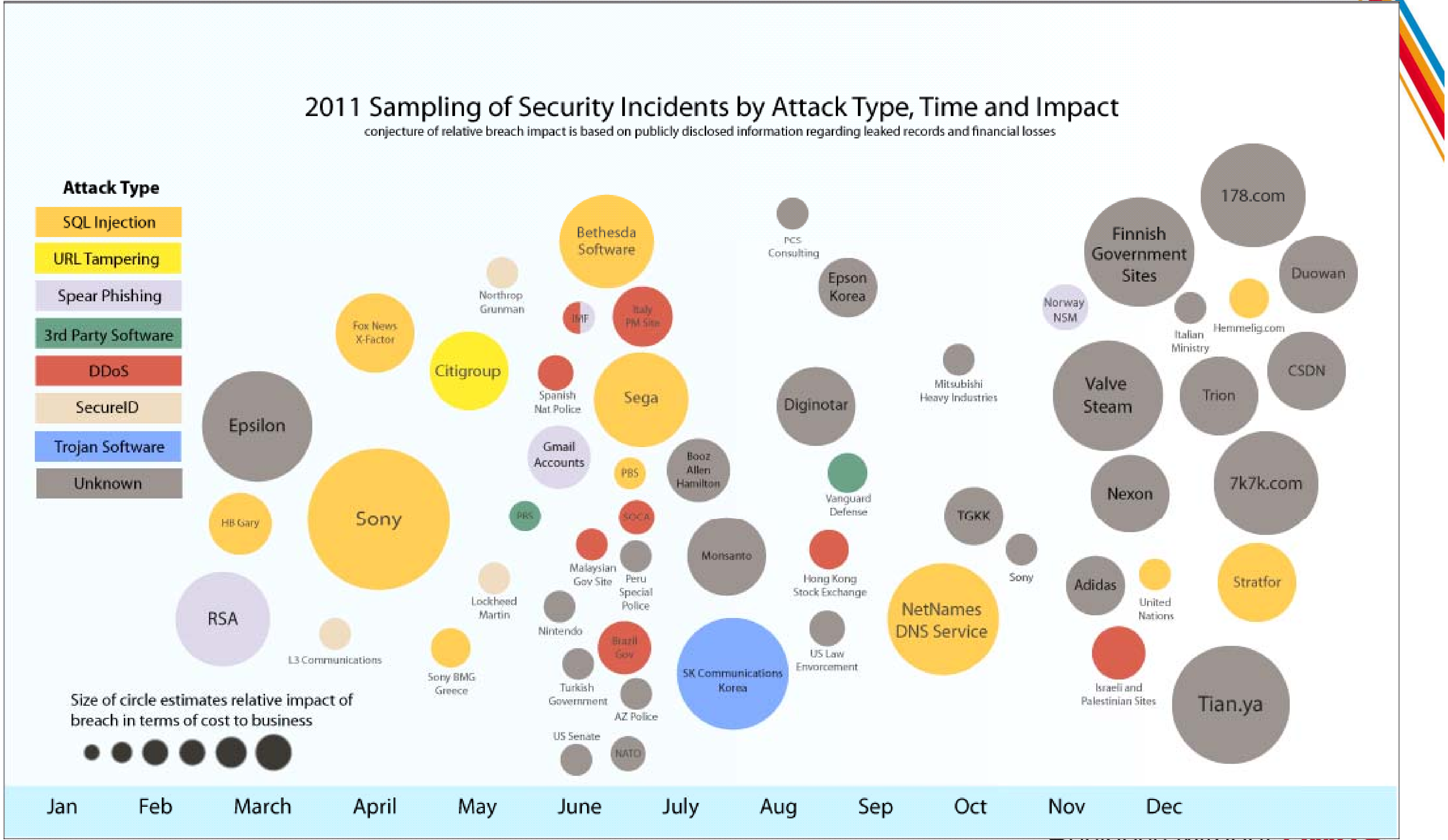
Date | Venue

"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

Targeted Attacks Shake Businesses and Governments in 2011



2011 Sampling of Security Incidents by Attack Type, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

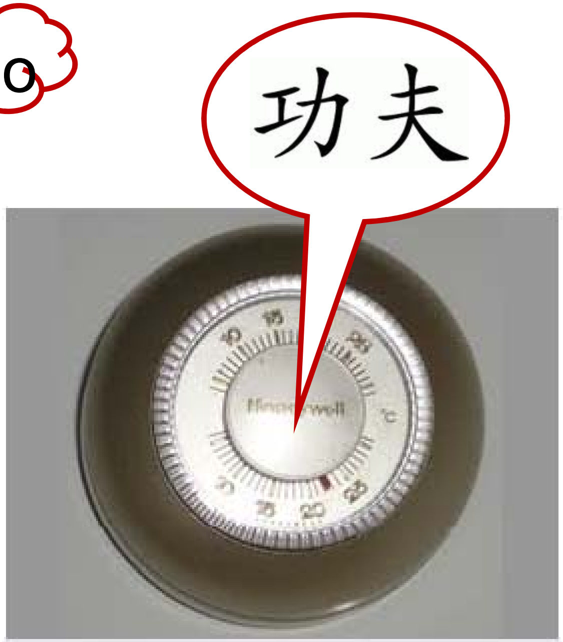
Source: IBM X-Force® 2011 Trend and Risk Report – March 2012

Have We Learned Anything?

SUBWAY (2011)
Theft of credit card data from 80,000 customers

Romanians accessed POS systems in NH, NY, OH & CA then exfiltrated data to compromised server in PA

CYBER-CRIME



US CHAMBER OF COMMERCE (2010)
Theft of intellectual property

Chinese hackers used spearphishing to steal employee credentials & install malware

CYBER-ESPIONAGE

SONY (2011)
Brand impact, remedies & lost business = $1B loss est.

Hackers exploited Web application vulnerability to access back-end customer databases

CYBER-ACTIVISM

Attacks from All Sides

Cyber vandals

Cyber warfare

Targets of opportunity

Nation states

Cyber crime

Hacktivists

Targets of choice

Cyber terrorism

Corporate espionage

Client-side vulnerabilities

Cyber espionage

Insiders

Data exfiltration

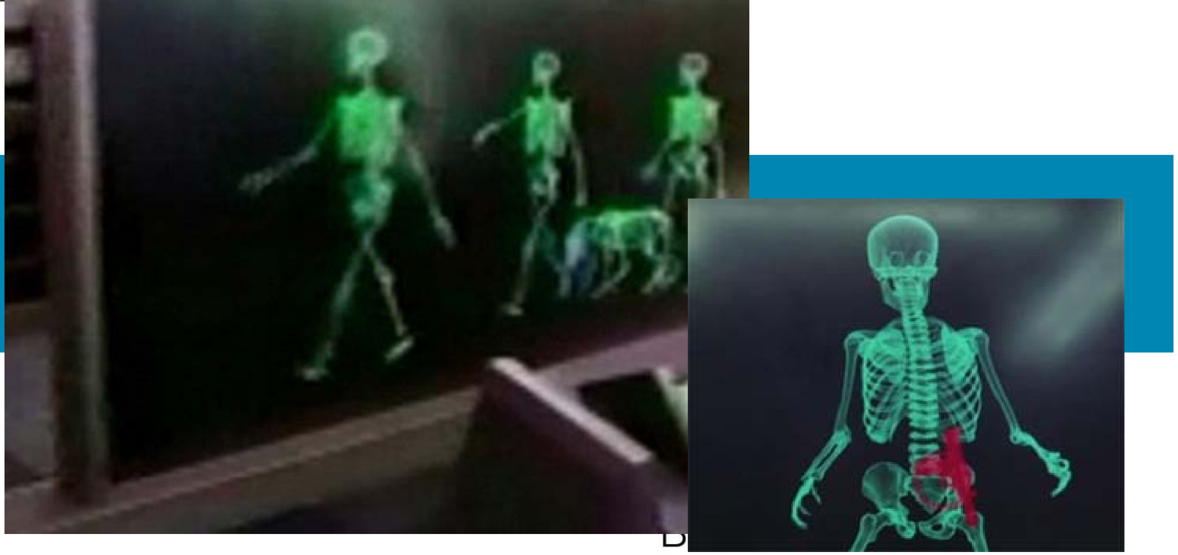
APTs

…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

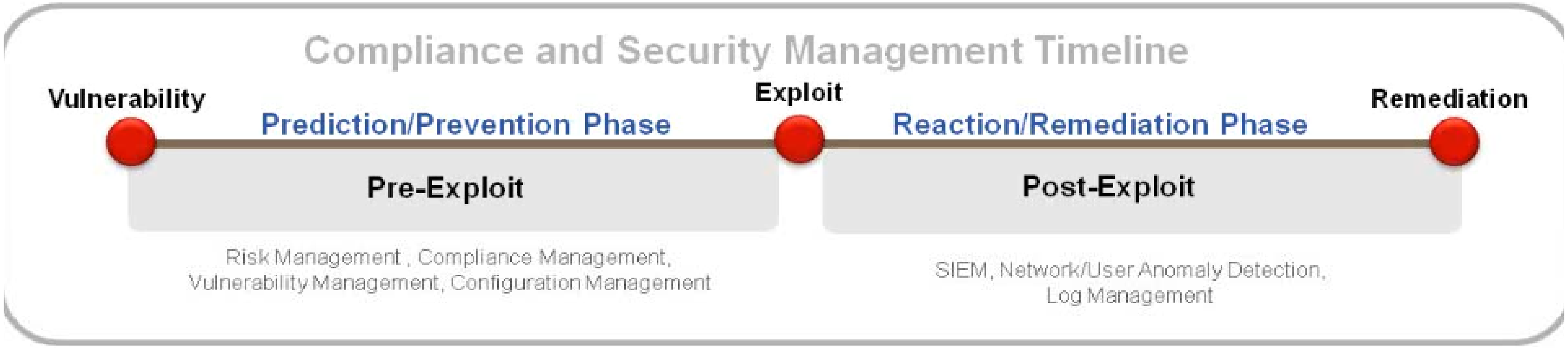
- No plane departing Ben Gurion Airport has ever been hijacked
- Use human intelligence
- “Questioning” looks for suspicious behavior
- Simple metal detectors

Scotland Yard

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

Security Intelligence

Solutions for the Full Compliance and Security Intelligence Timeline

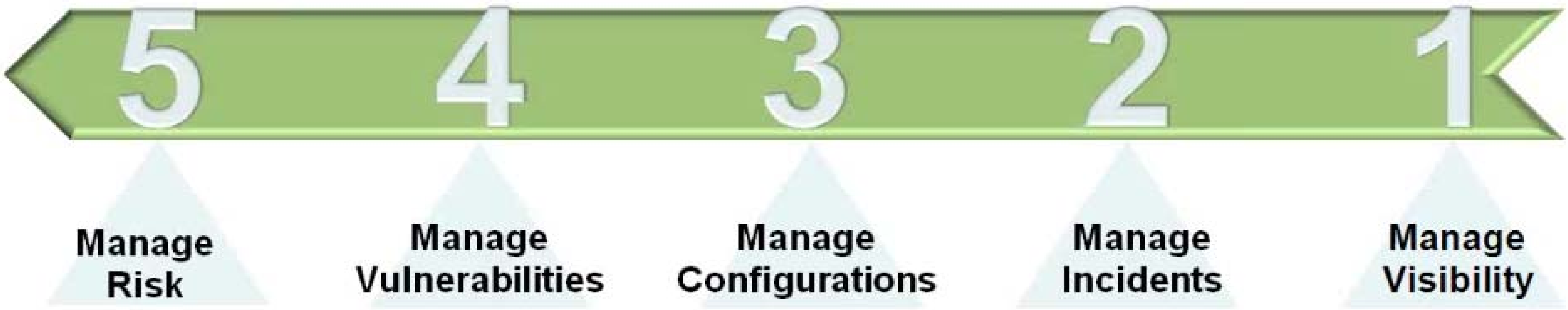


Compliance and Security Management Timeline

Risk Management , Compliance Management, Vulnerability Management, Configuration Management

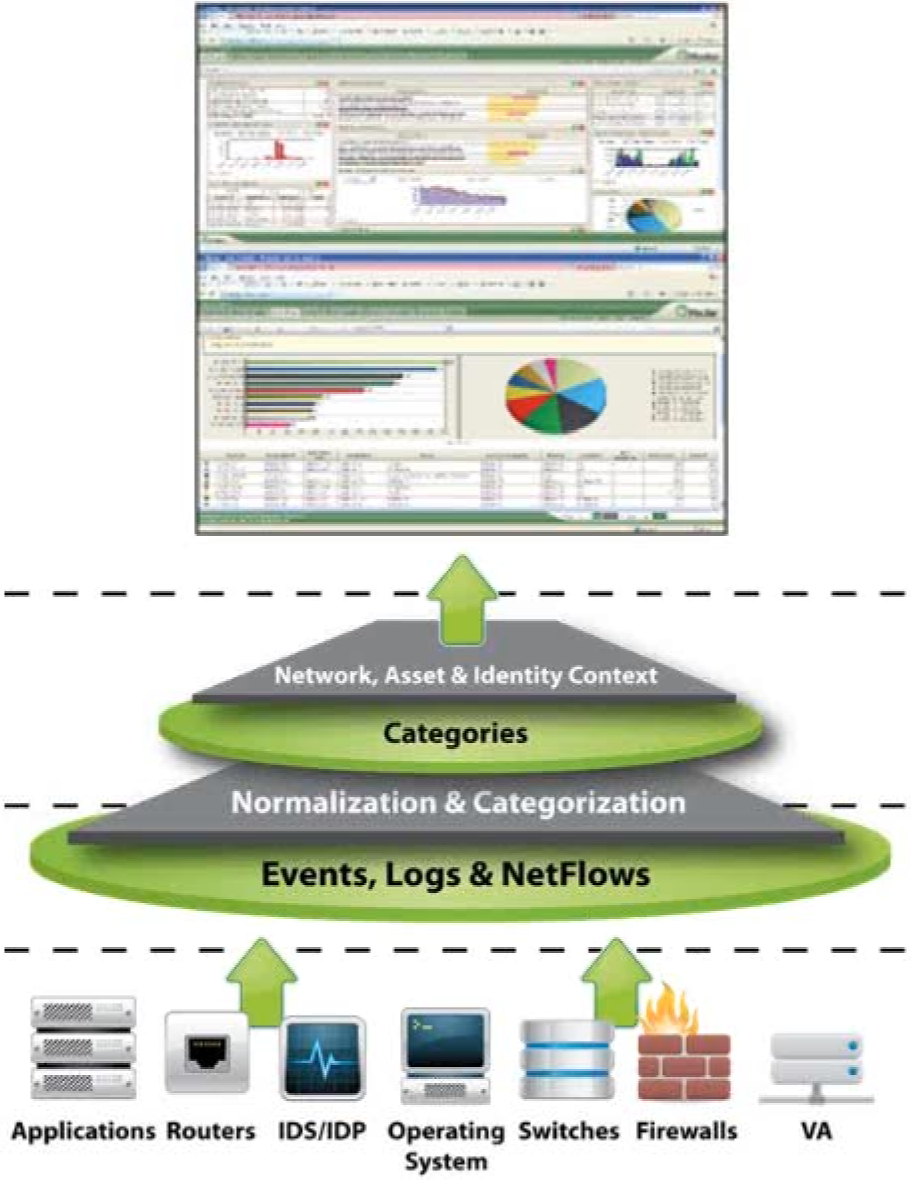
SIEM, Network/User Anomaly Detection, Log Management

5 Steps to Proactive Risk Management

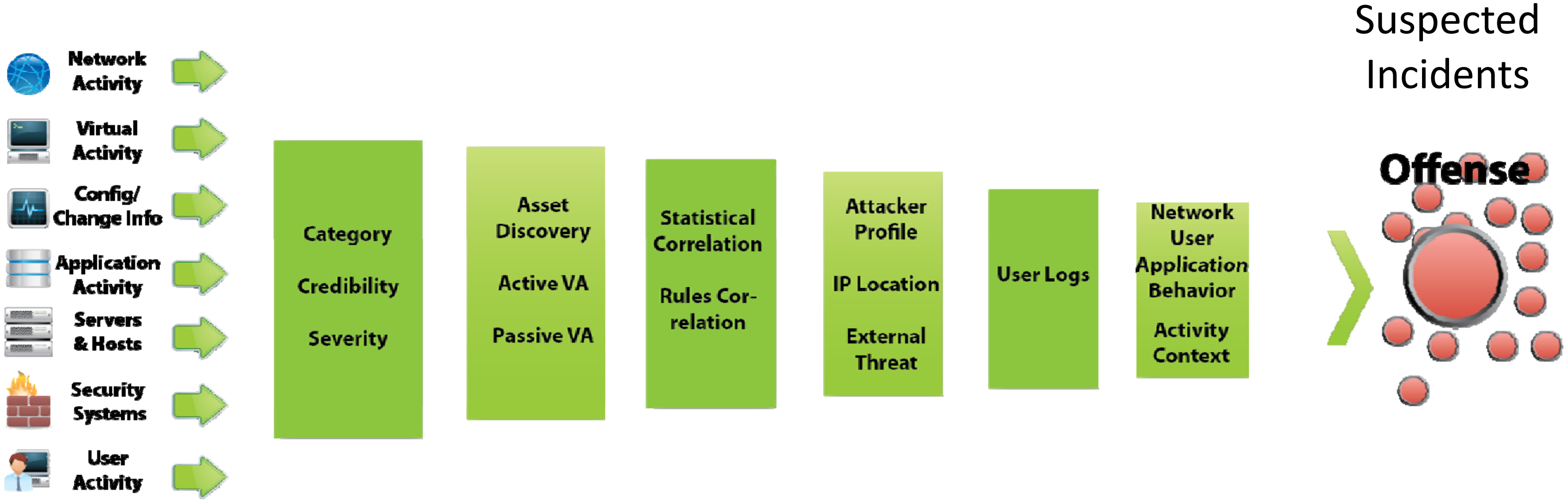


Manage Visibility

- Introduce Log Management /SIEM to gain visibility into:
  - Network infrastructure
  - Security infrastructure
  - Server infrastructure
  - Application infrastructure
  - Deliver consistent analysis
- Gain “consistency” across analysis through effective normalization and categorization
- Meet required compliance and information security driven analysis and reporting



Manage Incident



Network Activity

Virtual Activity

Config/ Change Info

Application Activity

Servers & Hosts

Security Systems

User Activity

Category

Credibility

Severity

Asset Discovery

Active VA

Passive VA

Statistical Correlation

Rules Correlation

Attacker Profile

IP Location

External Threat

User Logs

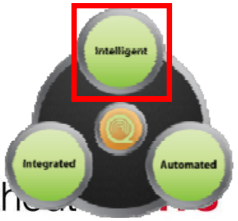
Network User Application Behavior

Activity Context

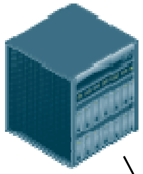
Suspected Incidents

Offense

Most Sources + Most Intelligence ⇨ *Most Accurate & Actionable Insight*



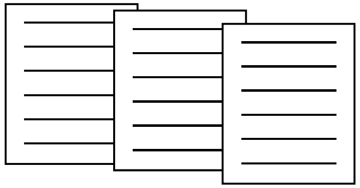
Manage Configurations



Switches
Routers
Firewalls
IDP/IDS

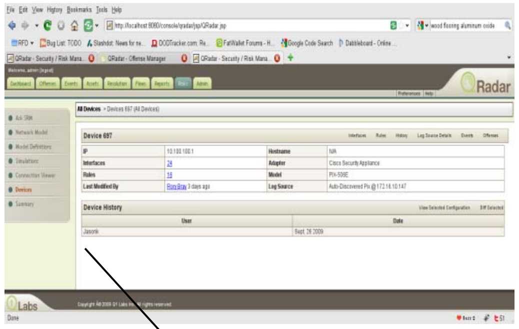
Scheduled Configuration Collection

Dynamic/ad-hoc Configuration Collection



Device Configuration History

Device Configuration Details



All Devices > Devices 697 (All Devices)

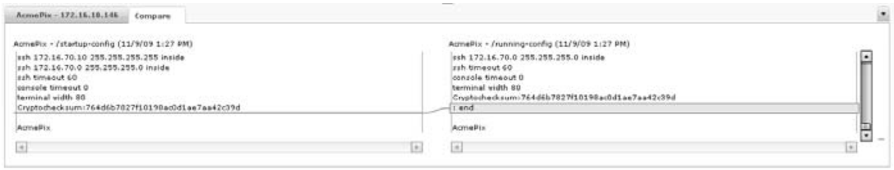
Device 697

IP	10.100.100.1	Hostname	N/A
Interfaces	24	Adapter	Cisco Security Appliance
Rules	16	Model	PIX-506E
Last Modified By	Rory Bray 3 days ago	Log Source	Auto-Discovered Pix @ 172.16.10.147

Device History

User	Date
Jasonk	Sept. 26 2009

Assess/Report Configuration Change: Rules, Interfaces

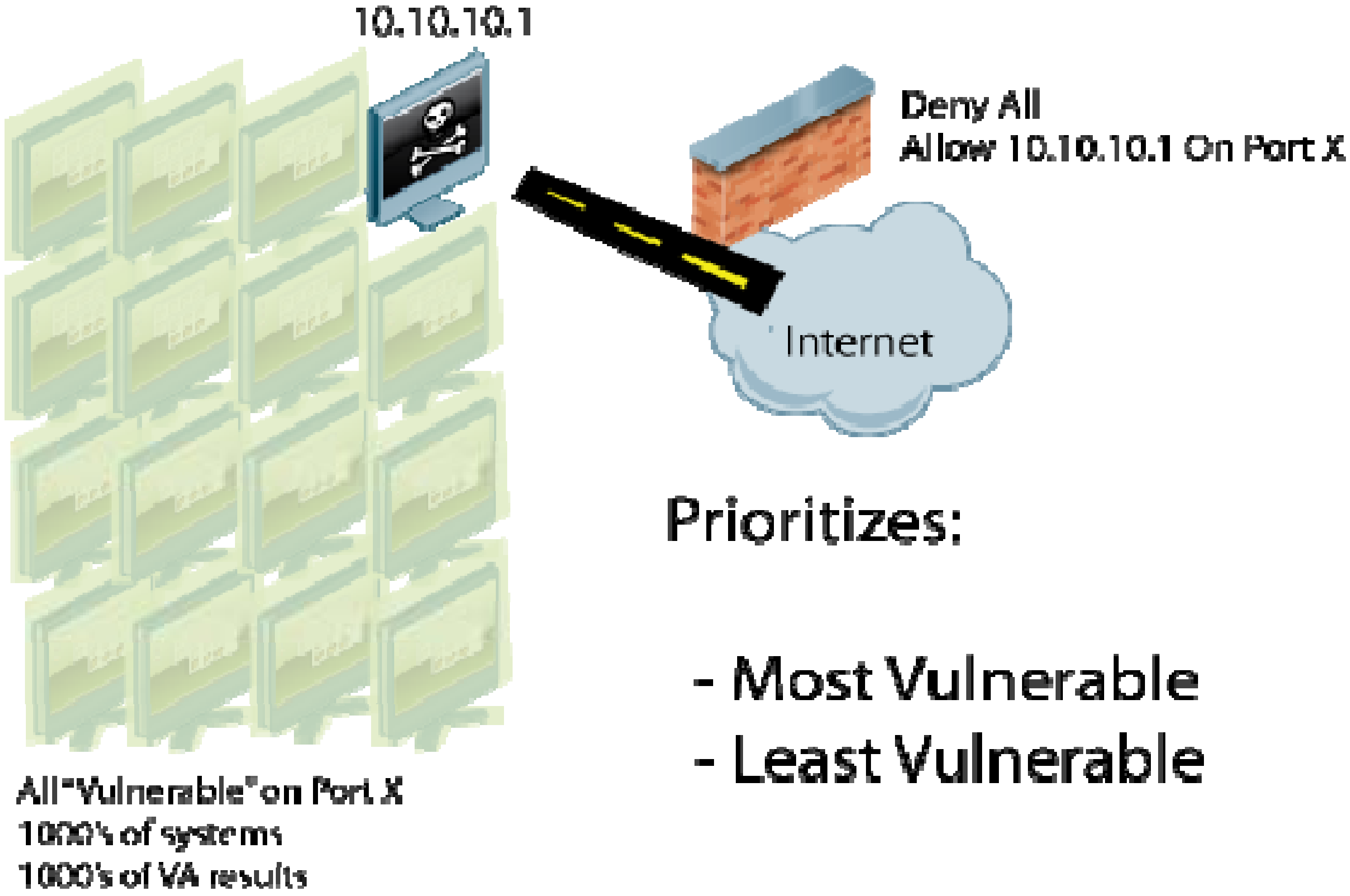


```
AcmePix - /startup-config (11/9/09 1:27 PM)
ssh 172.16.70.10 255.255.255.255 inside
ssh 172.16.70.0 255.255.255.0 inside
ssh timeout 60
console timeout 0
terminal width 80
Cryptochecksum:764d6b7827f10198ac0d1ae7aa42c39d

AcmePix
```

```
AcmePix - /running-config (11/9/09 1:27 PM)
ssh 172.16.70.0 255.255.255.0 inside
ssh timeout 60
console timeout 0
terminal width 80
Cryptochecksum:764d6b7827f10198ac0d1ae7aa42c39d
: end

AcmePix
```

Feature	Benefit
Automates the collection and analysis of network configuration and vulnerability data	Reduces expensive manual processes
Verifies network configuration against out-of-the-box compliance baselines or corporate standards (e.g. for PCI, NERC, and SOX)	Improves the ability to meet specific compliance-driven audit requirements
Delivers compliance and policy driven configuration reports, spanning a broad spectrum of technical controls	Helps assess operational priorities

Manage Vulnerabilities



Prioritizes:

- Most Vulnerable
- Least Vulnerable

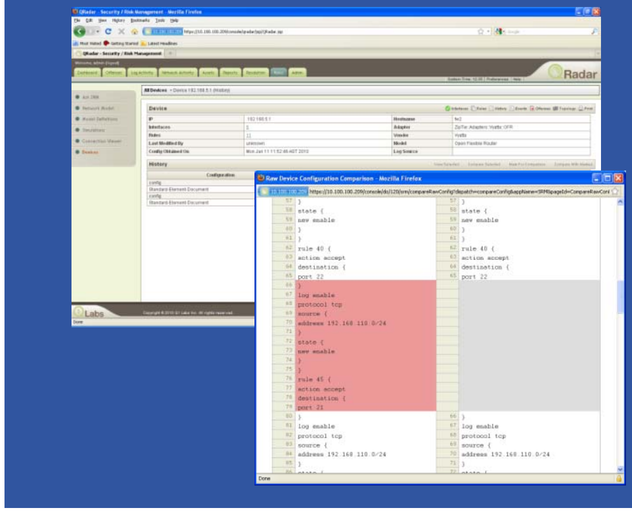
Manage Risk

Moving beyond reactive risk management….

Multi-vendor network configuration monitoring & audit

Automated compliance and risk assessment

Predictive threat modeling & simulation


QRadar - Security / Risk Management - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Radar
Labs
Done

All Devices > Device 192.168.5.1 (History)

Device

IP	192.168.5.1	Hostname	fw2
Interfaces	5	Adapter	ZipTie Adapters Vyatta OFR
Rules	11	Vendor	Vyatta
Last Modified By	unknown	Model	Open Flexible Router
Config Obtained On	Mon Jan 11 11:52:46 AST 2010	Log Source	

History

Configuration
config
Standard Element Document
config
Standard Element Document

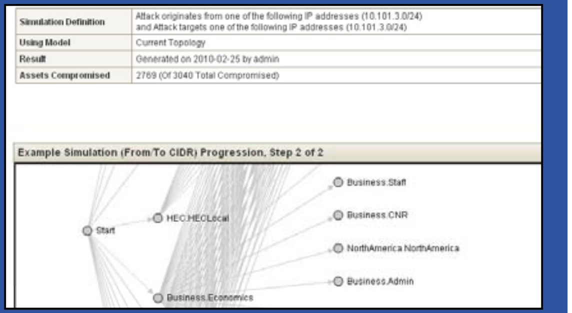
Raw Device Configuration Comparison - Mozilla Firefox

https://10.100.100.209/console/do/120/srm/compareRawConfig?dispatch=compareConfig&appName=SRM&pageId=CompareRawConf

```
}                              }
state {                        state {
new enable                     new enable
}                              }
}                              }
rule 40 {                      rule 40 {
action accept                  action accept
destination {                  destination {
port 22                        port 22
}
log enable
protocol tcp
source {
address 192.168.110.0/24
}
state {
new enable
}
}
rule 45 {
action accept
destination {
port 21
}                              }
log enable                     log enable
protocol tcp                   protocol tcp
source {                       source {
address 192.168.110.0/24       address 192.168.110.0/24
}                              }
```

Manage Vulnerabilities

Risk Indicators	
Configuration/ Topology	✓
Network Activity	✓
Vulnerability Management	✓
Network & vulnerability context	✓



Simulation Definition	Attack originates from one of the following IP addresses (10.101.3.0/24) and Attack targets one of the following IP addresses (10.101.3.0/24)
Using Model	Current Topology
Result	Generated on 2010-02-25 by admin
Assets Compromised	2769 (Of 3040 Total Compromised)

Example Simulation (From/To CIDR) Progression, Step 2 of 2

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

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

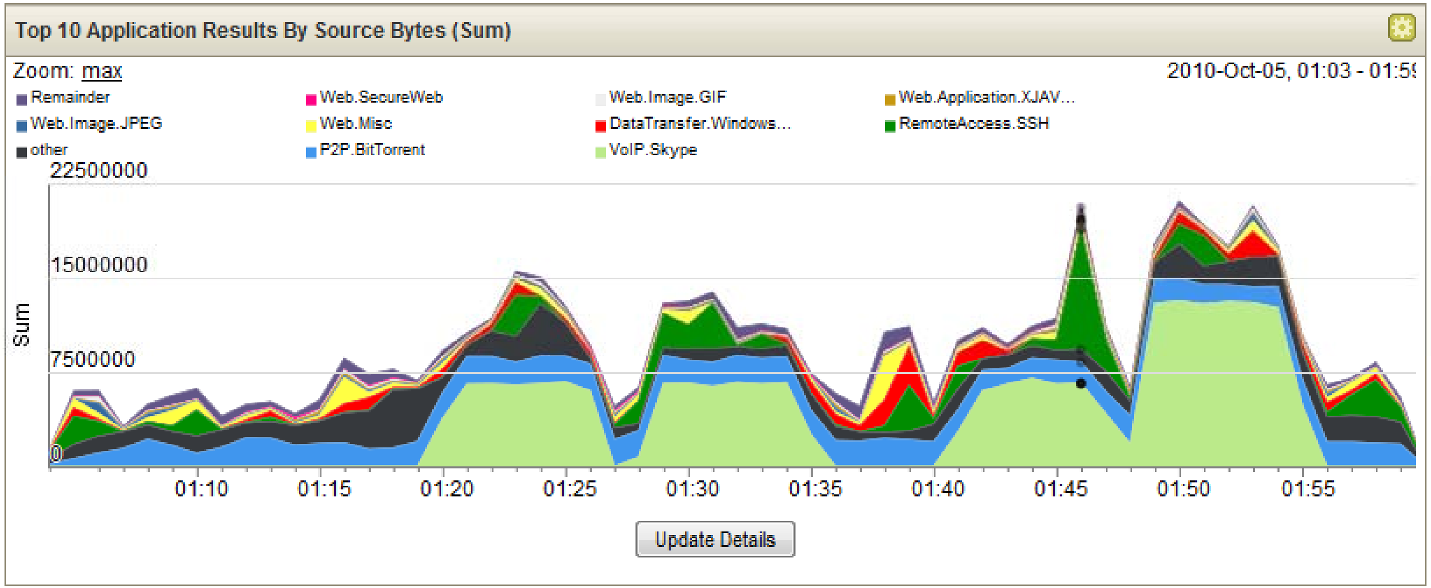
❖ And advanced *detection* finds intrusions faster & assesses impact

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

Q1 Labs®
Total Security Intelligence | An IBM Company

Network Activity Monitoring (Network Flows)

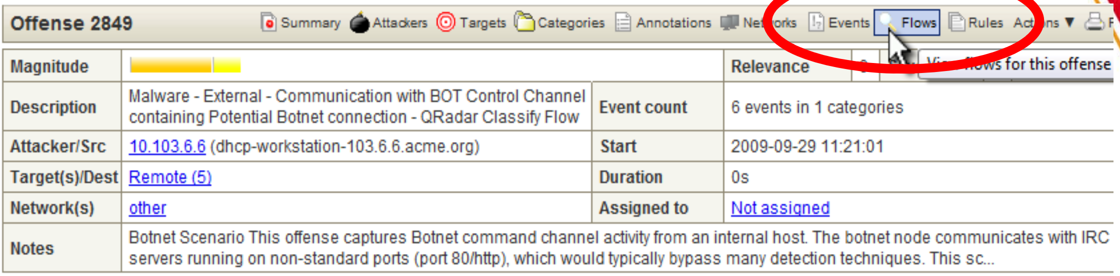
- Attackers can stop logging and erase their tracks, but can't cut off the network
- Helps detect day-zero attacks with no signature; provides visibility into attacker communications
- Network activity can build up an asset database and profile assets
- Useful for non-security related issues as well



Application and Threat Detection with Forensic Evidence

Potential Botnet Detected?

This is as far as traditional SIEM can go

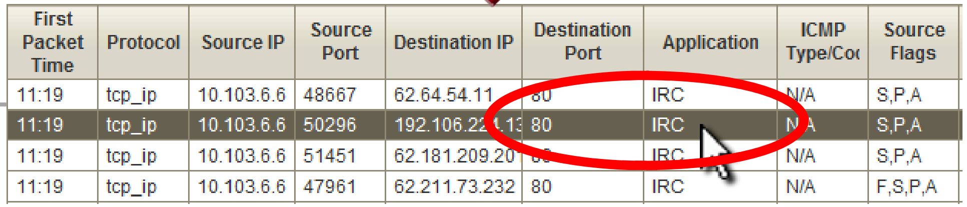


Offense 2849

Magnitude		Relevance	
Description	Malware - External - Communication with BOT Control Channel containing Potential Botnet connection - QRadar Classify Flow	Event count	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?

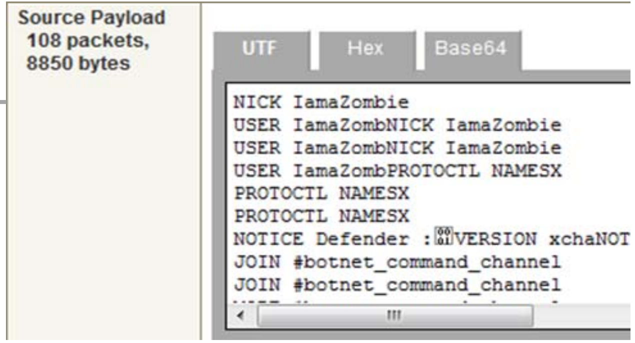
IBM Security QRadar QFlow detects a covert channel



First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Coc	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	192.106.22[illegible].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



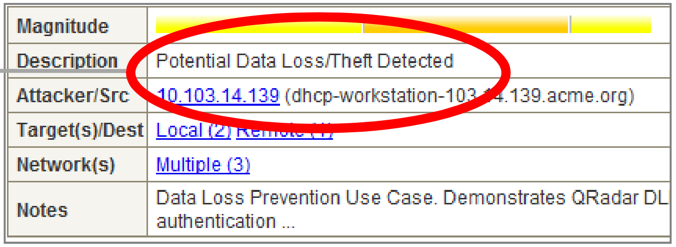
Source Payload
108 packets,
8850 bytes

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

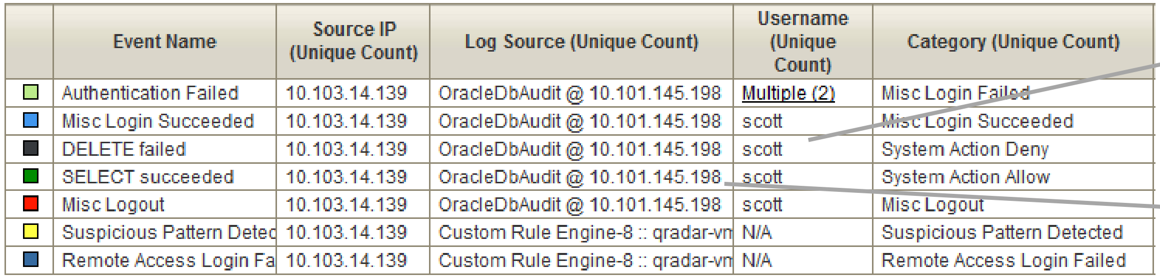
Application layer flow analysis can detect threats others miss

Detecting Insider Fraud

Potential Data Loss
Who? What? Where?



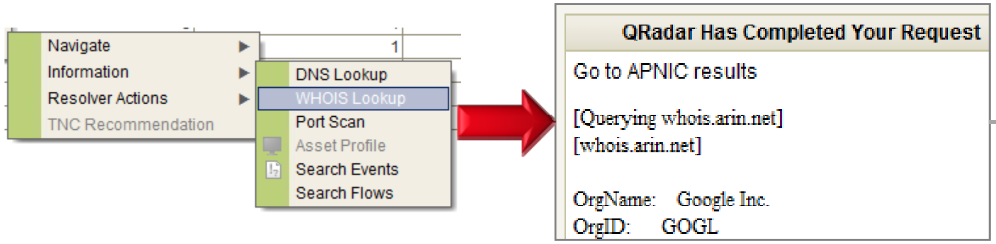
Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.14.139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...



	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

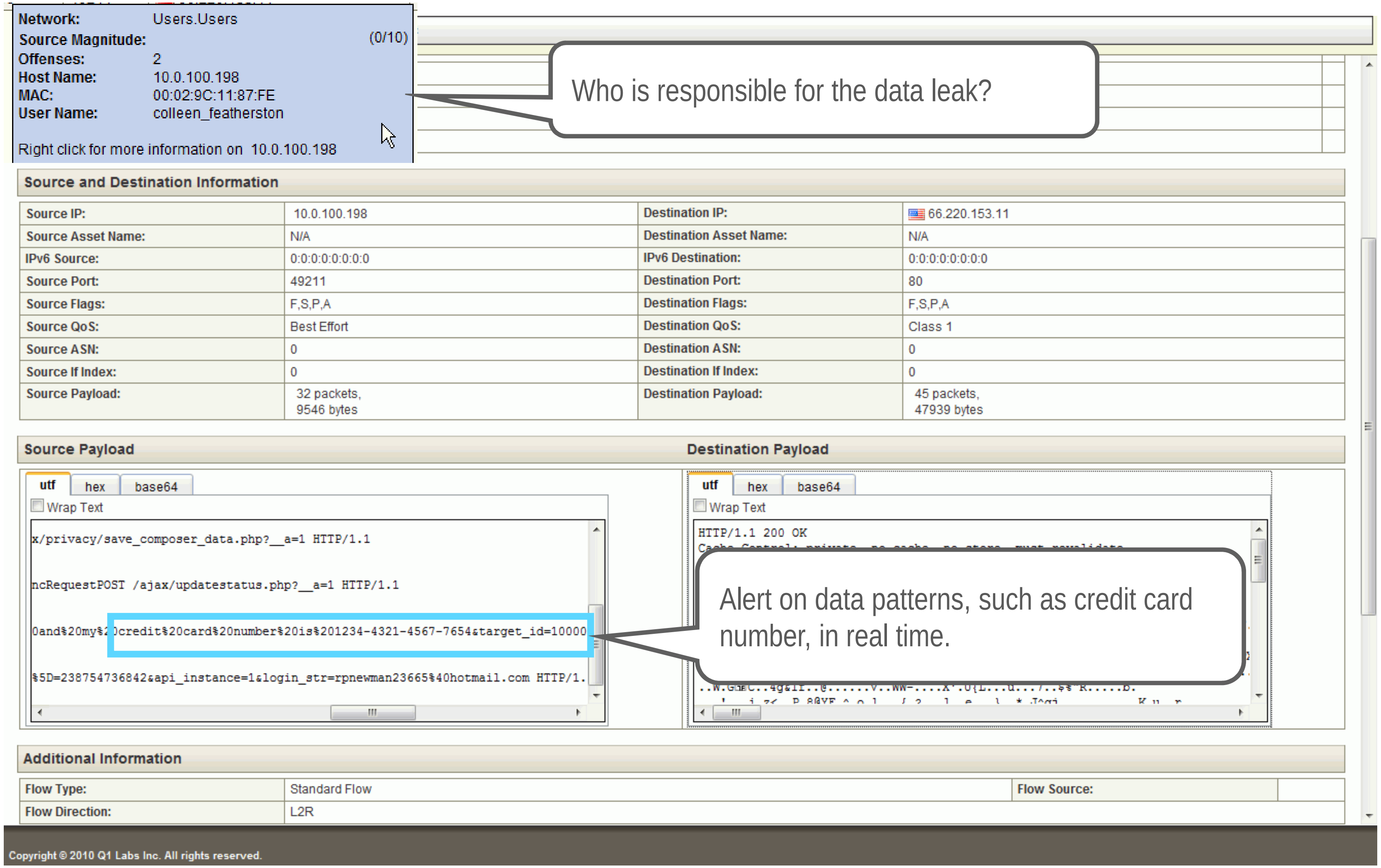
```
[Querying whois.arin.net]
[whois.arin.net]

OrgName:    Google Inc.
OrgID:      GOGL
```

Where?
Gmail

Threat detection in the post-perimeter world

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

Data Leakage



Network:	Users.Users
Source Magnitude:	(0/10)
Offenses:	2
Host Name:	10.0.100.198
MAC:	00:02:9C:11:87:FE
User Name:	colleen_featherston

Right click for more information on 10.0.100.198

Who is responsible for the data leak?

Source and Destination Information

Source IP:	10.0.100.198	Destination IP:	66.220.153.11
Source Asset Name:	N/A	Destination Asset Name:	N/A
IPv6 Source:	0:0:0:0:0:0:0:0	IPv6 Destination:	0:0:0:0:0:0:0:0
Source Port:	49211	Destination Port:	80
Source Flags:	F,S,P,A	Destination Flags:	F,S,P,A
Source QoS:	Best Effort	Destination QoS:	Class 1
Source ASN:	0	Destination ASN:	0
Source If Index:	0	Destination If Index:	0
Source Payload:	32 packets, 9546 bytes	Destination Payload:	45 packets, 47939 bytes

Source Payload

```
x/privacy/save_composer_data.php?__a=1 HTTP/1.1

ncRequestPOST /ajax/updatestatus.php?__a=1 HTTP/1.1

0and%20my%20credit%20card%20number%20is%201234-4321-4567-7654&target_id=10000

%5D=238754736842&api_instance=1&login_str=rpnewman23665%40hotmail.com HTTP/1.
```

Destination Payload

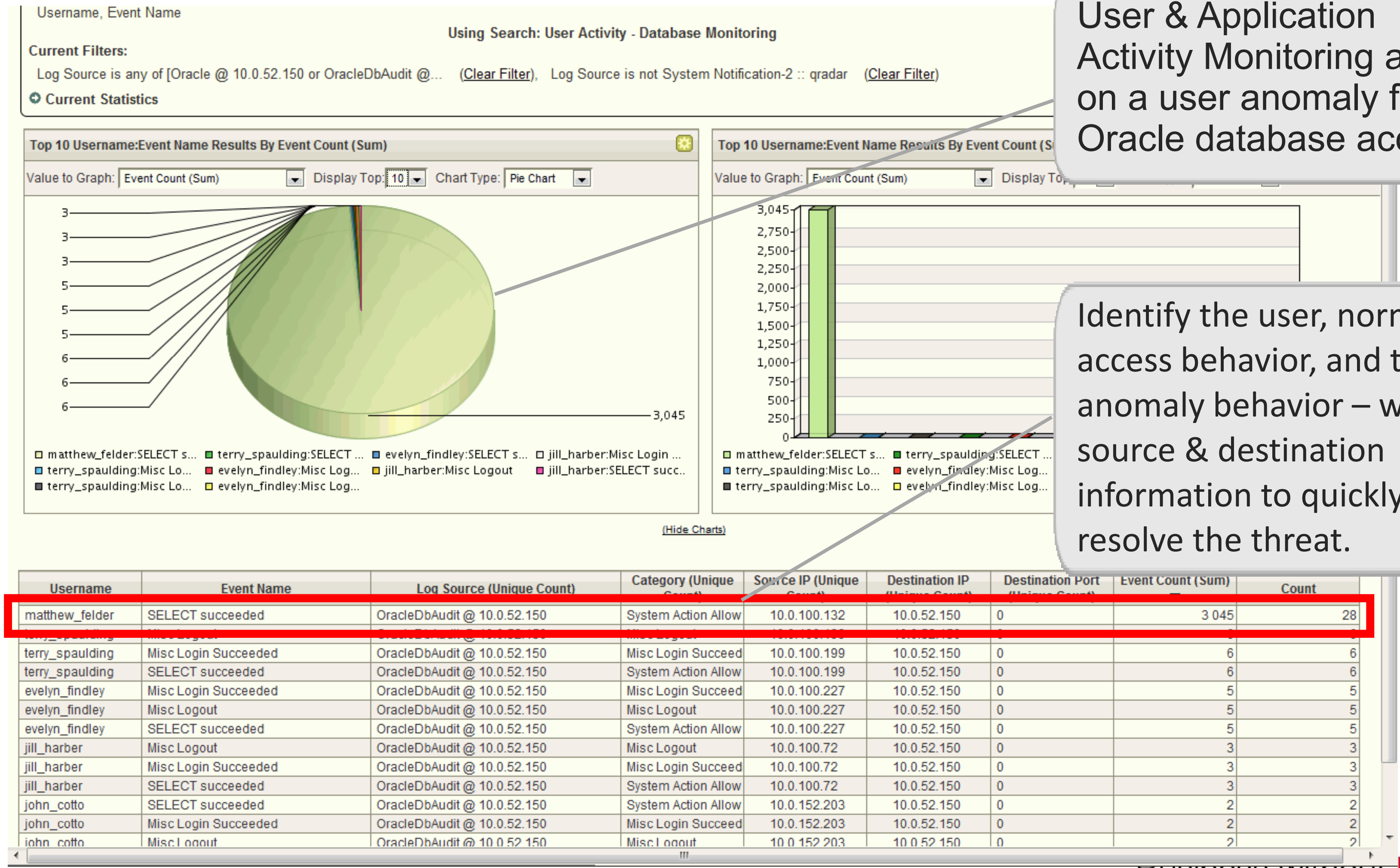
```
HTTP/1.1 200 OK
Cache-Control: private, no-cache, no-store, must-revalidate
```

Alert on data patterns, such as credit card number, in real time.

Additional Information

Flow Type:	Standard Flow	Flow Source:	
Flow Direction:	L2R		

User Activity Monitoring to Combat Advanced Persistent Threats



Username, Event Name

Using Search: User Activity - Database Monitoring

Current Filters:

Log Source is any of [Oracle @ 10.0.52.150 or OracleDbAudit @... (Clear Filter), Log Source is not System Notification-2 :: qradar (Clear Filter)

Current Statistics

Top 10 Username:Event Name Results By Event Count (Sum)

Value to Graph: Event Count (Sum) Display Top: 10 Chart Type: Pie Chart

3
3
3
5
5
5
6
6
6
3,045
□ matthew_felder:SELECT s...
🟩 terry_spaulding:SELECT ...
🟦 evelyn_findley:SELECT s...
□ jill_harber:Misc Login ...
🟦 terry_spaulding:Misc Lo...
🟥 evelyn_findley:Misc Log...
🟨 jill_harber:Misc Logout
🟪 jill_harber:SELECT succ..
■ terry_spaulding:Misc Lo...
🟨 evelyn_findley:Misc Log...

Top 10 Username:Event Name Results By Event Count (S

Value to Graph: Event Count (Sum) Display To

3,045
2,750
2,500
2,250
2,000
1,750
1,500
1,250
1,000
750
500
250
0
🟩 matthew_felder:SELECT s...
🟩 terry_spaulding:SELECT ...
🟦 terry_spaulding:Misc Lo...
🟥 evelyn_findley:Misc Log...
■ terry_spaulding:Misc Lo...
🟨 evelyn_findley:Misc Log...

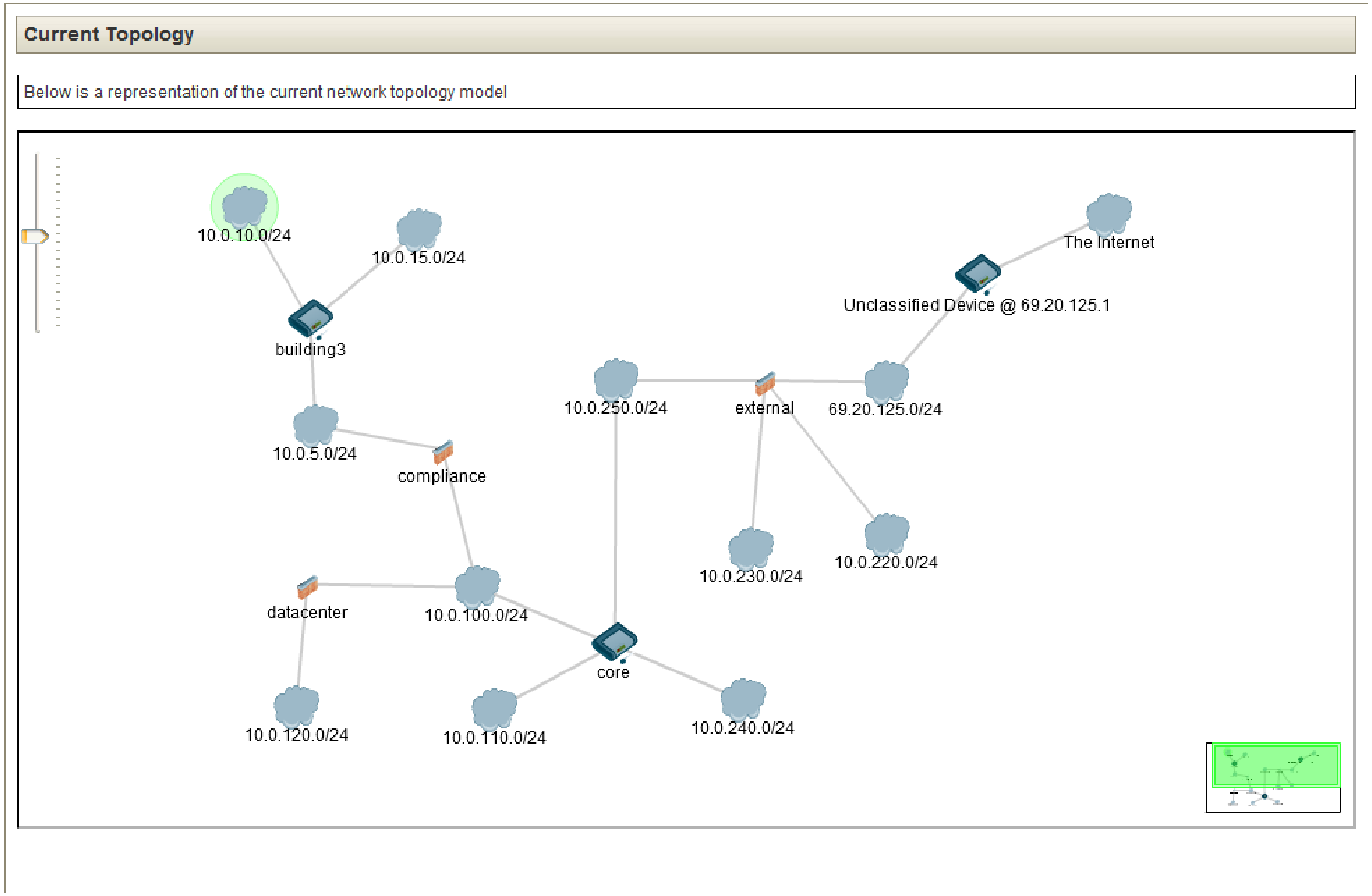
(Hide Charts)

Username	Event Name	Log Source (Unique Count)	Category (Unique Count)	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Count (Sum)	Count
matthew_felder	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.132	10.0.52.150	0	3 045	28
terry_spaulding	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.100.199	10.0.52.150	0	6	6
terry_spaulding	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.100.199	10.0.52.150	0	6	6
terry_spaulding	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.199	10.0.52.150	0	6	6
evelyn_findley	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.100.227	10.0.52.150	0	5	5
evelyn_findley	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.100.227	10.0.52.150	0	5	5
evelyn_findley	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.227	10.0.52.150	0	5	5
jill_harber	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.100.72	10.0.52.150	0	3	3
jill_harber	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.100.72	10.0.52.150	0	3	3
jill_harber	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.72	10.0.52.150	0	3	3
john_cotto	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.152.203	10.0.52.150	0	2	2
john_cotto	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.152.203	10.0.52.150	0	2	2
john_cotto	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.152.203	10.0.52.150	0	2	2

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.

Configuration & Risk



Current Topology

Below is a representation of the current network topology model

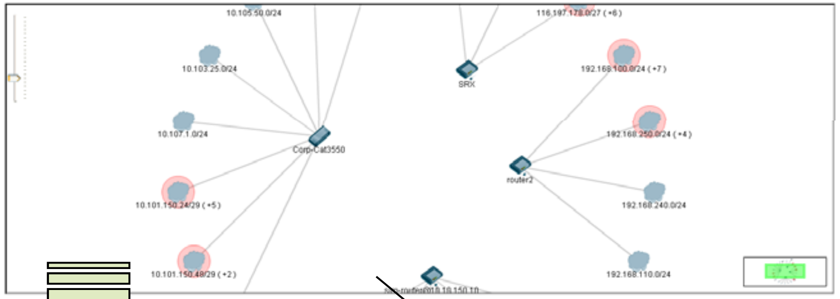
Network topology and open paths of attack add context

Rules can take exposure into account to:

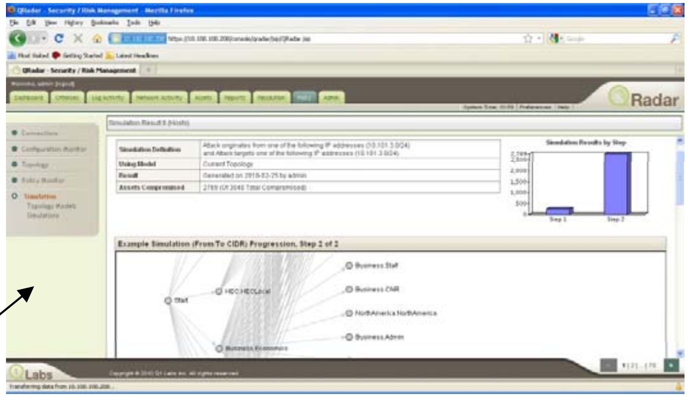
- Prioritize offenses and remediation
- Enforce policies

Predictive Threat Modeling and Simulation

- Play out what-if scenarios



Current Topology


QRadar - Security / Risk Management

Simulation Result 8 (Hosts)

Simulation Definition	Attack originates from one of the following IP addresses (10.101.3.0/24) and Attack targets one of the following IP addresses (10.101.3.0/24)
Using Model	Current Topology
Result	Generated on 2010-03-25 by admin
Assets Compromised	2769 (Of 3040 Total Compromised)

Topology Model

Simulation

When scheduled

Events or Offense

Modifies current topology:

±Firewall Rule

±IPS Signature

±Allowed Asset Communication

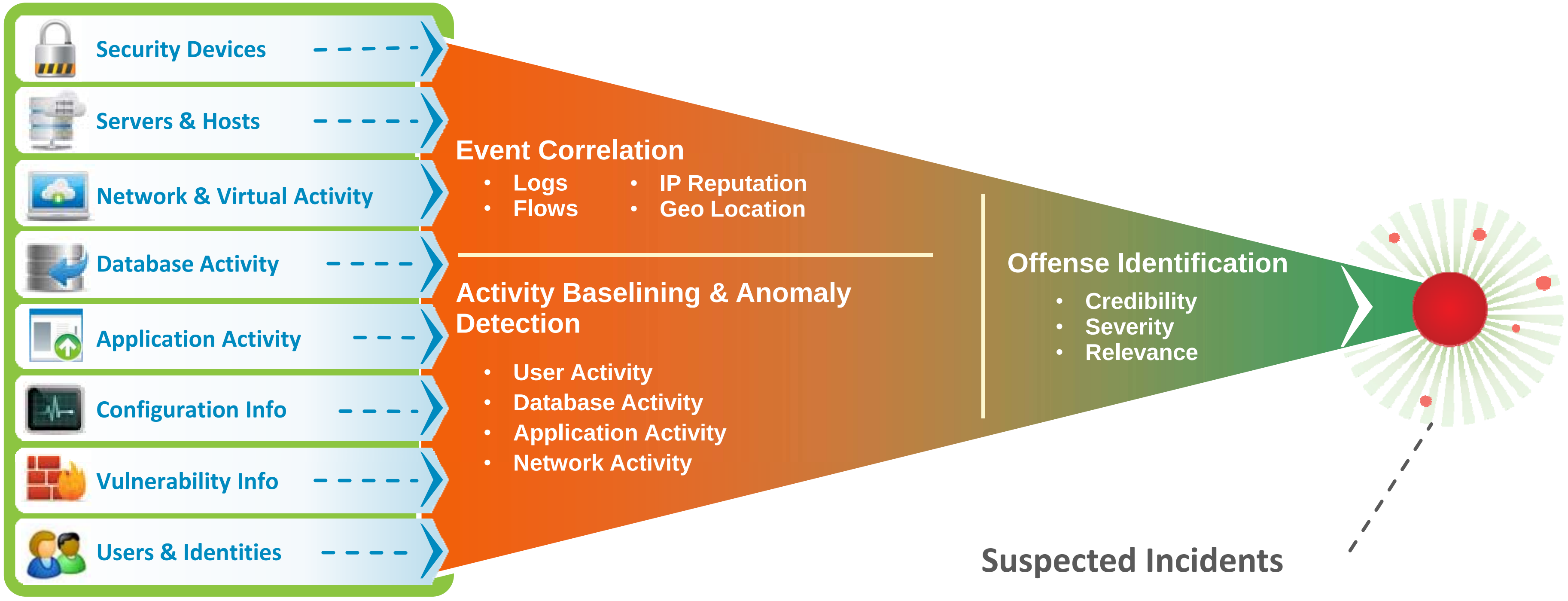
Simulates attack scenario using:

- Current Topology
- Or, Topology Model

Pulse Comes to You 2012

Business without LIMITS

Context and Correlation Drive Deep Insight

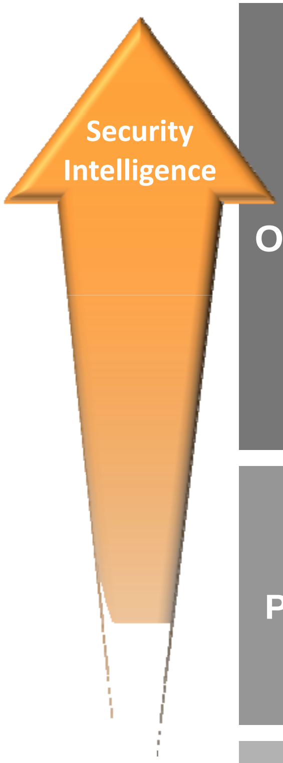


Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

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

Security Intelligence is Enabling Progress to Optimized Security



Optimized	**Security Intelligence:** Information and event management Advanced correlation and deep analytics External threat research			
	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
	People	**Data**	**Applications**	**Infrastructure**

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