

Security Intelligence.  
**Think Integrated.**

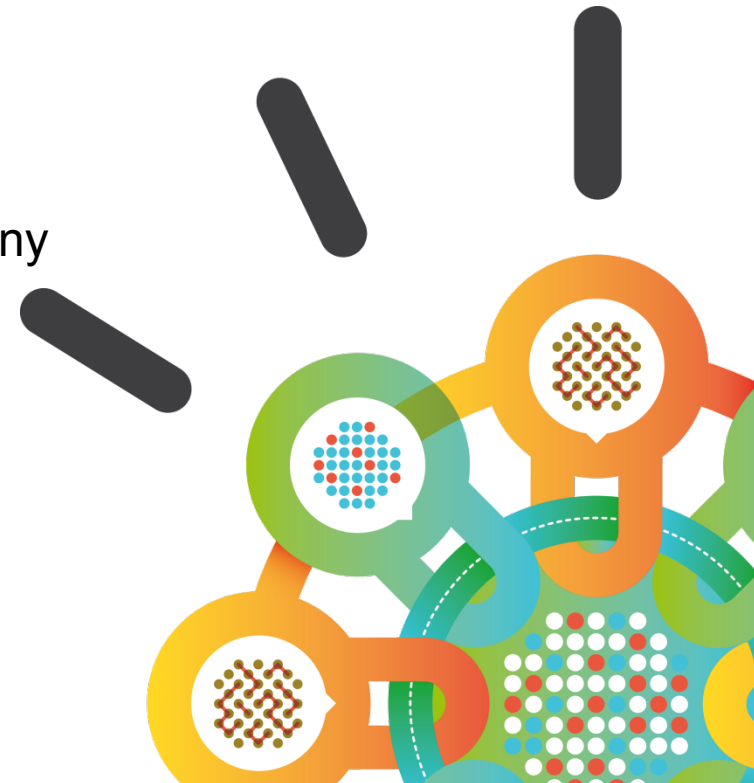
## Security Intelligence:

How to protect against targeted attacks,  
insider fraud & unauthorized configuration  
changes

Steve Durkin,

Europe Channel Director, Q1 Labs, an IBM Company

[steve.durkin@uk.ibm.com](mailto:steve.durkin@uk.ibm.com)





**“Given the dynamic nature of the challenge, measuring the state of security within an organization is increasingly important. Since threats are always moving and solutions are more complex, dynamic and often partial, knowing where you are is essential.”**

**Deutsche Bank**



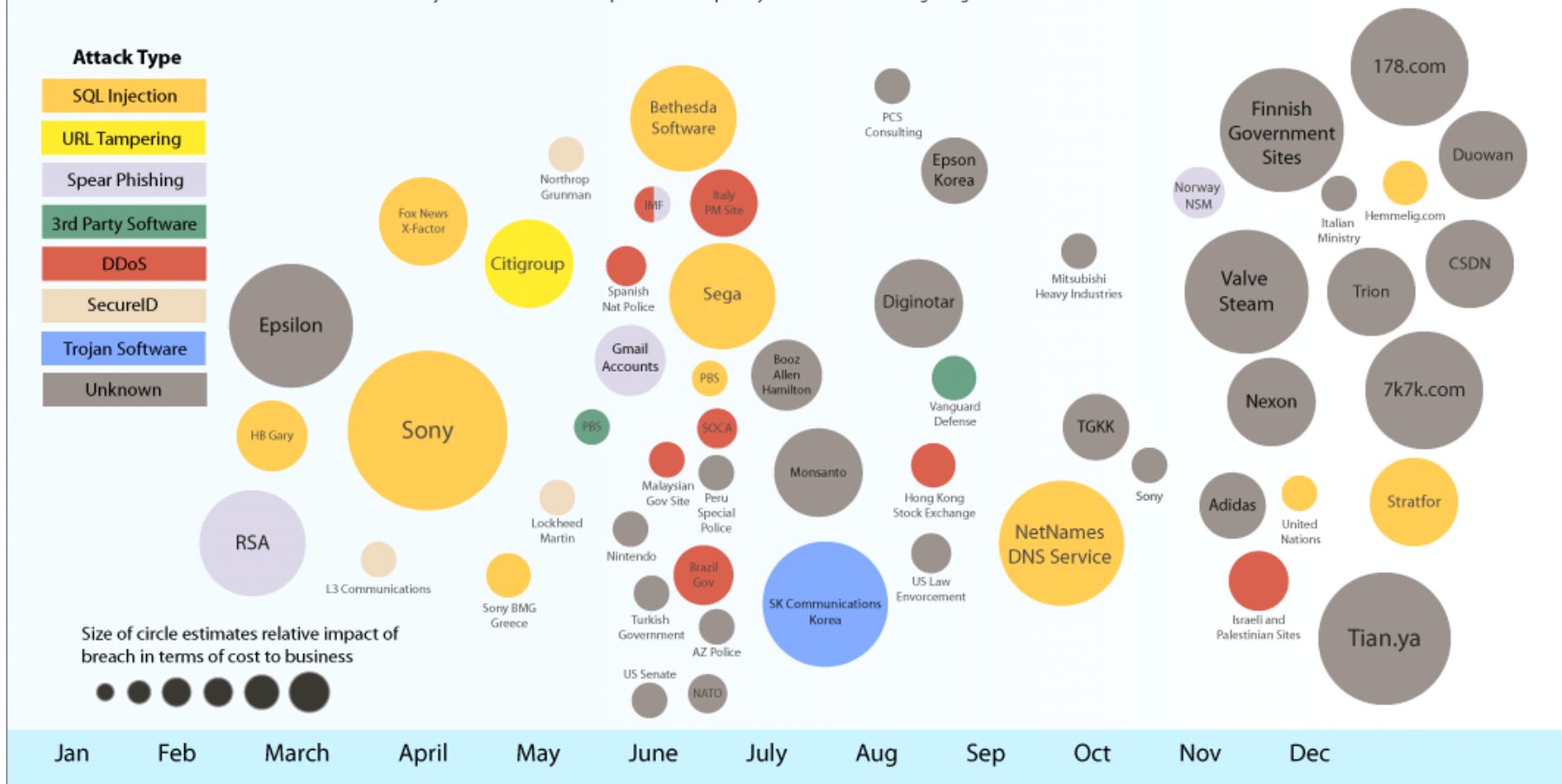
*John Meakin*

Global Head of Security Solutions & Architecture,  
Deutsche Bank

# Targeted Attacks Shake Businesses and Governments


## 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

# IT Security is a board room discussion



Business results	Brand image	Supply chain	Legal exposure	Impact of hacktivism	Audit risk
Sony estimates potential \$1B long term impact – \$171M / 100 customers*	HSBC data breach discloses 24K private banking customers	Epsilon breach impacts 100 national brands	TJX estimates \$150M class action settlement in release of credit / debit card info	Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony ...	Zurich Insurance PLC fined £2.275M (\$3.8M) for the loss and exposure of 46K customer records

# Have we learned anything?



самбо

功夫

\*!!@&#



## 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**



## EU Directive- Privacy is essential

- EU Justice Commissioner, Viviane Reding, at the Digital Life Design (DLD) conference in Munich Jan 2012
- All 27 European member states will be governed by the new rules
- Companies with > 250 employees will have to appoint a privacy officer
- If customers' privacy is breached, companies:
  - May be fined up to €1M or 2% of co's global annual turnover
  - Will have to inform the Information Commissioner within 24 hours of discovery





## UK Government target UK Business Leaders on Cyber Threats

- Government & intelligence agencies are directly targeting the most senior levels in the UK's largest companies
- Providing advice on how to safeguard their most valuable assets, such as personal data, online services and intellectual property
- The new guidance, produced by parties including CESG (the Information Security arm of GCHQ), will help the private sector minimise the risks to company assets.
- Key objective, within the Government's Cyber Security Strategy, is to work hand in hand with industry and make the UK one of the most secure places in the world to do online business



## Attacks from all sides

Cyber vandals

Cyber warfare

Targets of opportunity

Nation states

Cyber crime

Hacktivists

Targets of choice

Cyber terrorism

Corporate espionage

Cyber espionage

Client-side vulnerabilities

Insiders

APTs

Data exfiltration



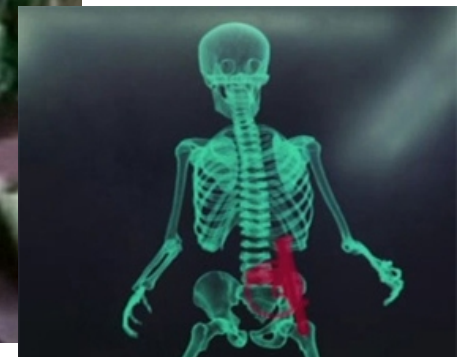
...but all is not lost...

## Choose the Right Solution



Protection technology is critical,  
but choose wisely

There is no magic  
security technology





# Security Intelligence = Context + Situational Awareness

## Massive Data Collection

- Logs / Events
- Network Activity

## Context—Risk Assessment & Prioritization

- Asset classification
- Accounts: roles & users
- Configuration data
- Vulnerability data

## Situational Awareness

- Advanced threat detection
- Malicious insider detection
- Data leak prevention
- Anomaly detection and forensic investigation

# Solutions for the Full Compliance and Security Intelligence Timeline



## Pre-Exploit

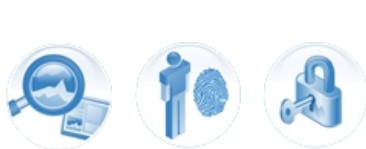
## Post-Exploit

### Prediction & Prevention

### Reaction & Remediation

Risk Management. Vulnerability Management.  
Configuration Monitoring. Compliance Management.  
Reporting and Scorecards.

SIEM. Log Management.  
Network Anomaly Detection. Packet Forensics.  
Incident Response and Workflow.



# Security Intelligence Use Cases

## How Next-Generation SIEM Can Help

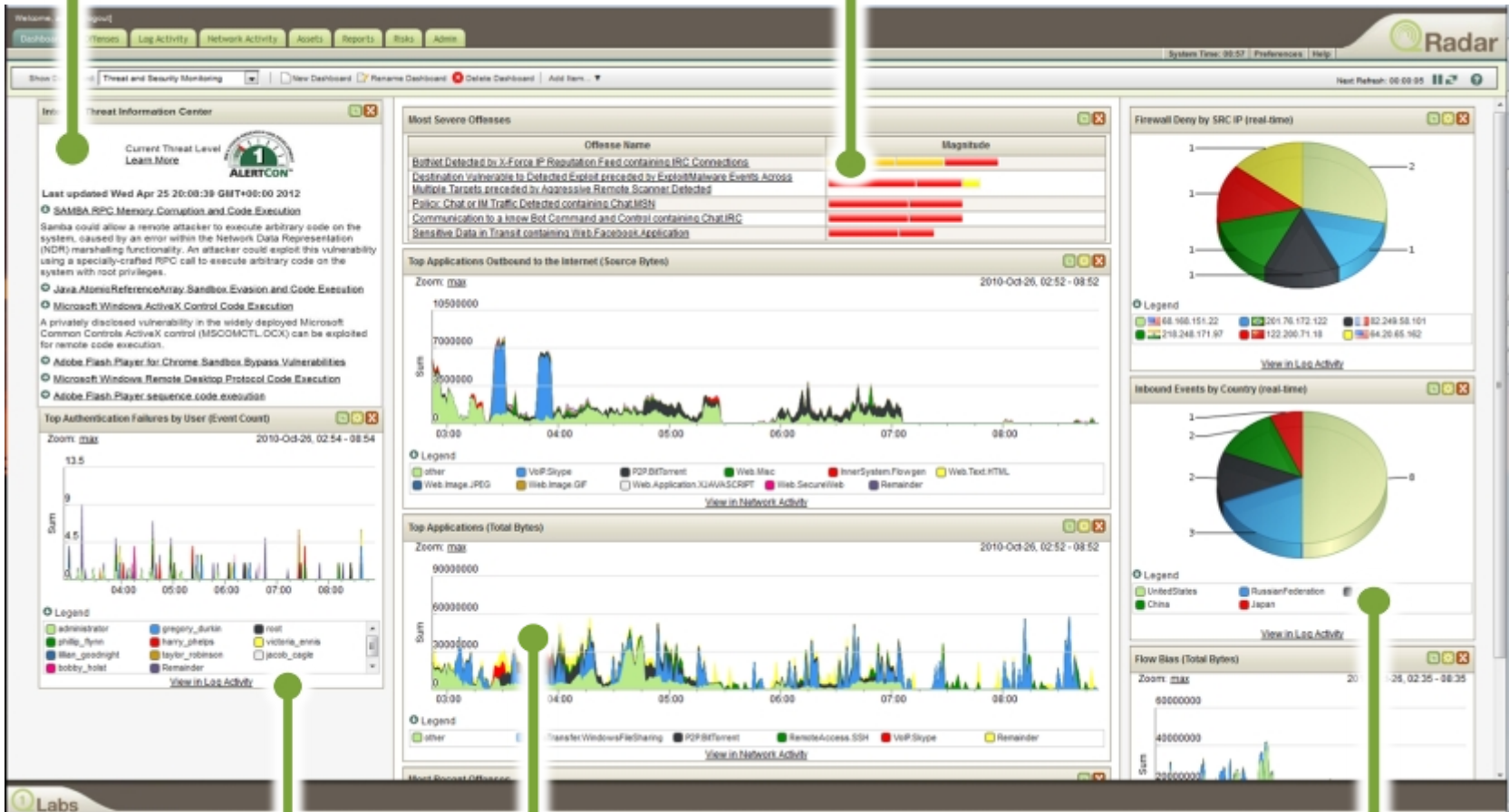
- Continuously monitor all activity and correlate in real-time
- Gain visibility into *unauthorized or anomalous* activities
  - Server communicating with IP address in unusual country – foreign intrusion?
  - Unusual Windows service – backdoor or spyware program?
  - Spike in download volume from SharePoint server – suspicious access?
  - High number of failed logins to critical servers – brute-force password attack?
  - Inappropriate use of protocols – sensitive data being exfiltrated via P2P?
  - New service initiated on a known host – potentially signaling a breach?
- Automation => reduced cost & complexity, simplified compliance, lower Total Cost of Ownership (TCO)



# Security Intelligence: QRadar provides security visibility

## IBM X-Force® Threat Information Center

## Real-time Security Overview w/ IP Reputation Correlation



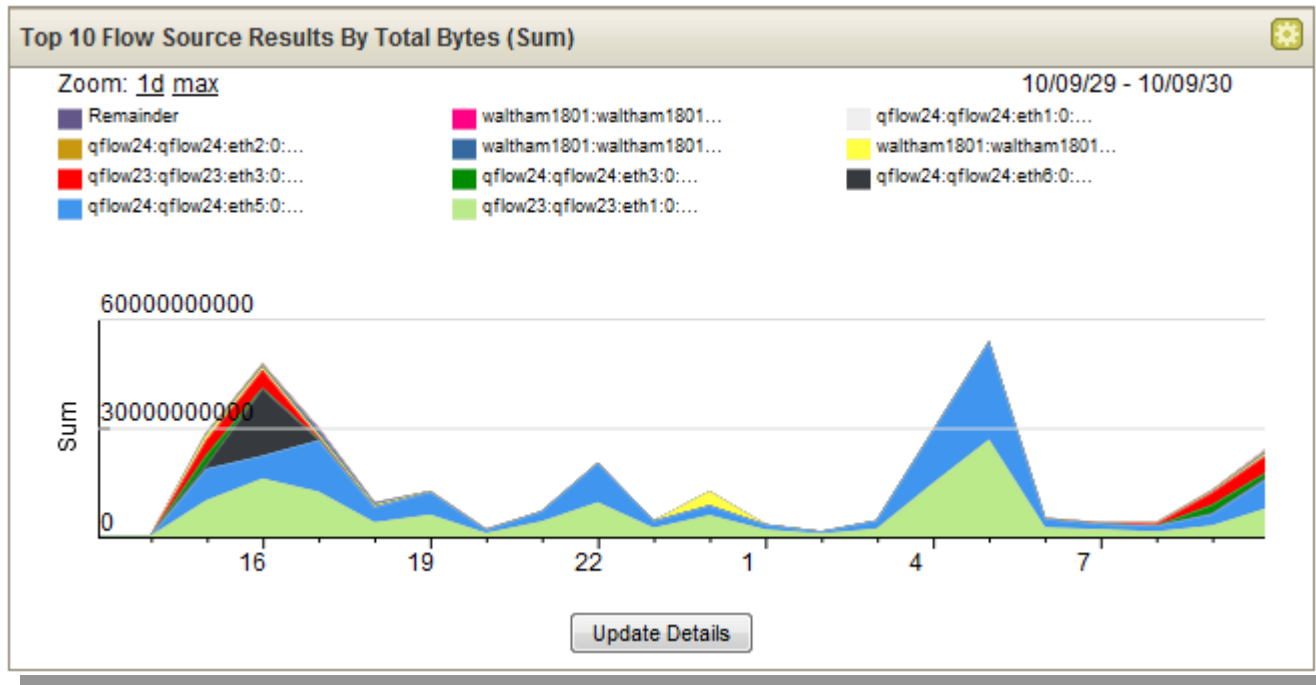
**Identity and User Context**

**Real-time Network Visualization and Application Statistics**

**Inbound Security Events**

## Network Activity Monitoring (Network Flows)

- Attackers can stop logging and erase their tracks, but can't cut off the network.
- Network activity can build up an asset database and profile assets
- Application detection can look at application level data
- 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

First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Cod	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	192.106.22.113	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 :00VERSION xchaNOT
JOIN #botnet_command_channel
JOIN #botnet_command_channel
    
```

**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) 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 Detect	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

- Navigate
- Information
- Resolver Actions
- TNC Recommendation

- DNS Lookup
- WHOIS Lookup
- Port Scan
- Asset Profile
- Search Events
- Search Flows

**QRadar Has Completed Your Request**

Go to APNIC results

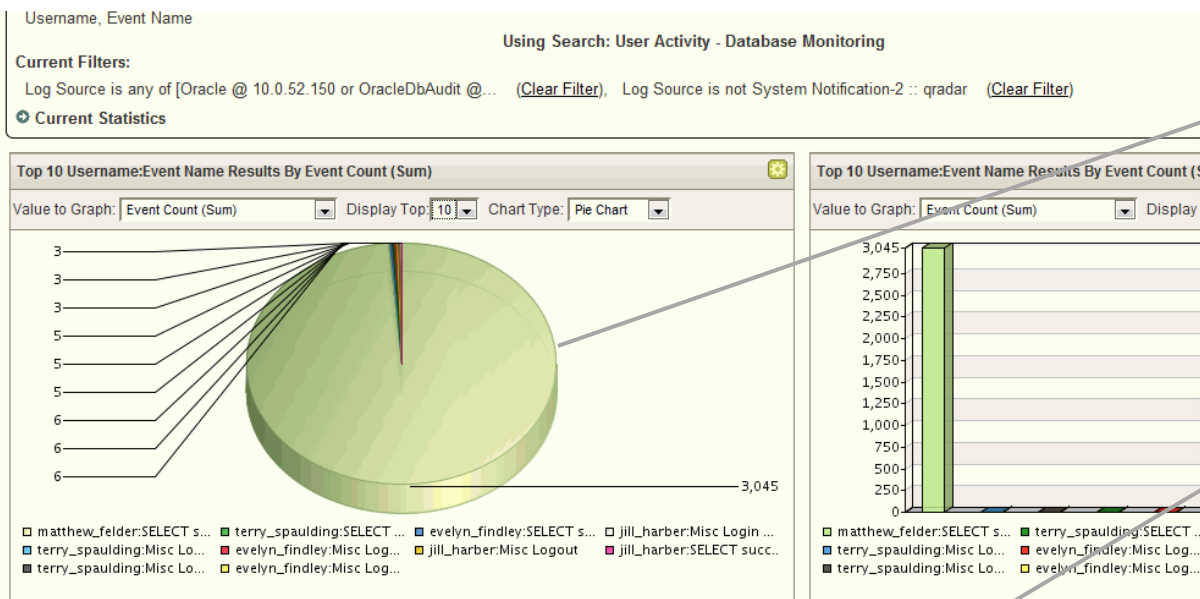
[Querying whois.arin.net]  
[whois.arin.net]

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

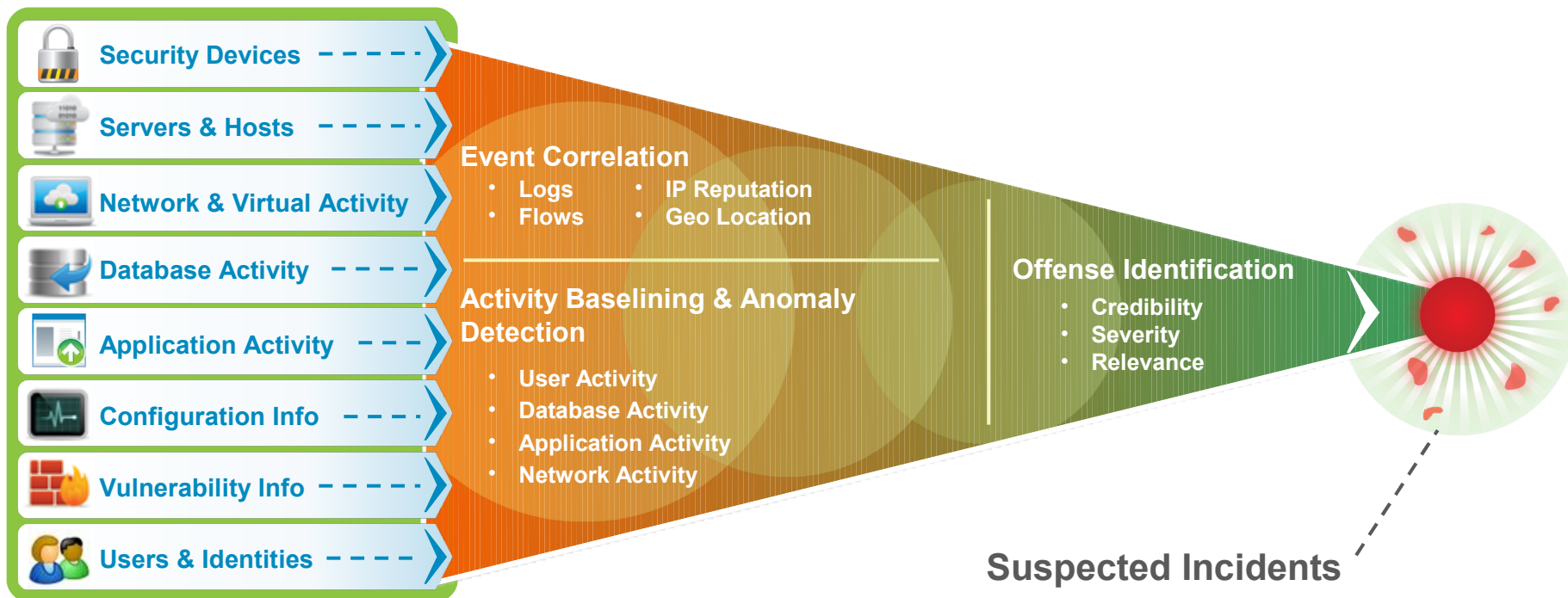


User & Application Activity Monitoring alerts on a user anomaly for Oracle database access.

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

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

# Context and Correlation Drive Deep Insight



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

## Solving Complex Problems for Clients

<b>Major Electric Utility</b>	Detecting threats	<ul style="list-style-type: none"><li>• Discovered 500 hosts with “Here You Have” virus, which other solutions missed</li></ul>
<b>Fortune 5 Energy Company</b>	Consolidating data silos	<ul style="list-style-type: none"><li>• 2 Billion logs and events per day reduced to 25 high priority offenses</li></ul>
<b>Branded Apparel Maker</b>	Detecting insider fraud	<ul style="list-style-type: none"><li>• Trusted insider stealing and destroying key data</li></ul>
<b>\$100B Diversified Corporation</b>	Predicting risks against your business	<ul style="list-style-type: none"><li>• Automating the policy monitoring and evaluation process for configuration change in the infrastructure</li></ul>
<b>Industrial Distributor</b>	Addressing regulatory mandates	<ul style="list-style-type: none"><li>• Real-time extensive monitoring of network activity, in addition to PCI mandates</li></ul>



# SANS Poll Shows Q1 Labs as SIEM Leader in Installed Base

## ISC Poll

[Poll Results](#) | [Poll Archives](#)

### Poll Results

#### Are you currently using a Security Information and Event Management (SIEM) solution to collect security logs?

- 11.2 % => We use ArcSight
- 7.8 % => We use Splunk
- 1.5 % => We use NetForensics
- 7.1 % => We use RSA enVision
- 43.9 % => We use Q1 Labs
- 0.7 % => We use Trustwave
- 3.9 % => We use our home grown solution
- 11.1 % => Other
- 6 % => We are planning to acquire one in the next 12 months
- 6.8 % => We have no plan to use a SIEM

**Total Answers: 974**

# 43.9%



## What to do next?

- Download the QRadar platform datasheet:  
<http://q1labs.com/resource-center/brochures/details.aspx?id=21>
- Download the Gartner SIEM Critical Capabilities Report  
<http://q1labs.com/resource-center/analyst-reports/details.aspx?id=151>
- Read our blog <http://blog.q1labs.com/>
- Follow us on Twitter: [@q1labs](#) [@ibmsecurity](#)

[ibm.com/security](http://ibm.com/security)



© Copyright IBM Corporation 2012. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.