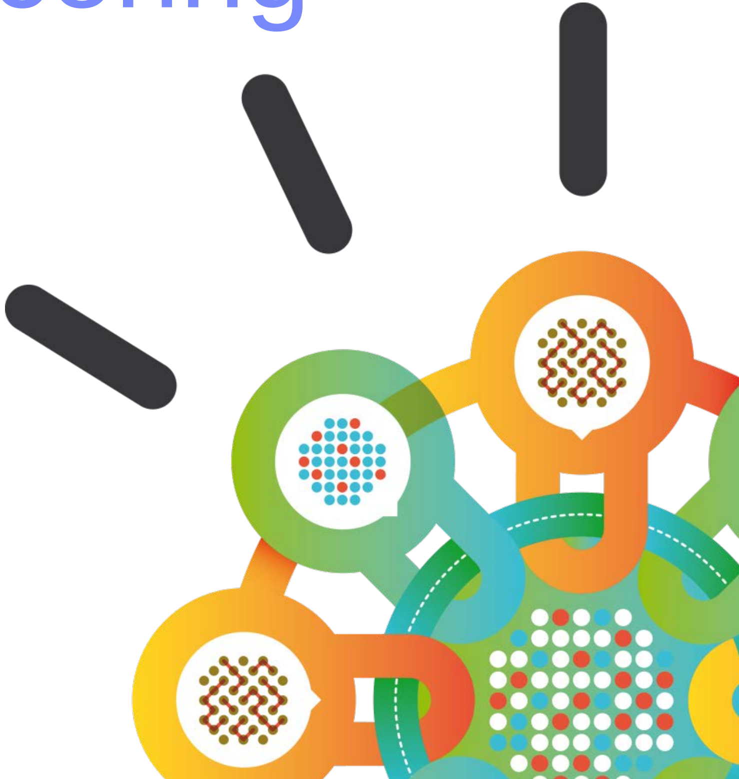
Security Intelligence.
Think Integrated.

Continuous Monitoring & Real-Time Risk Scoring

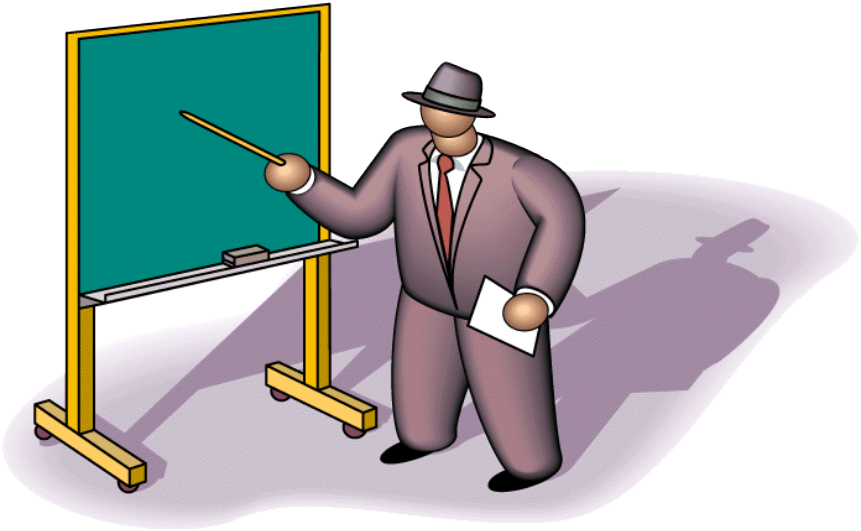


Chris Poulin

Security Strategist, IBM

Agenda

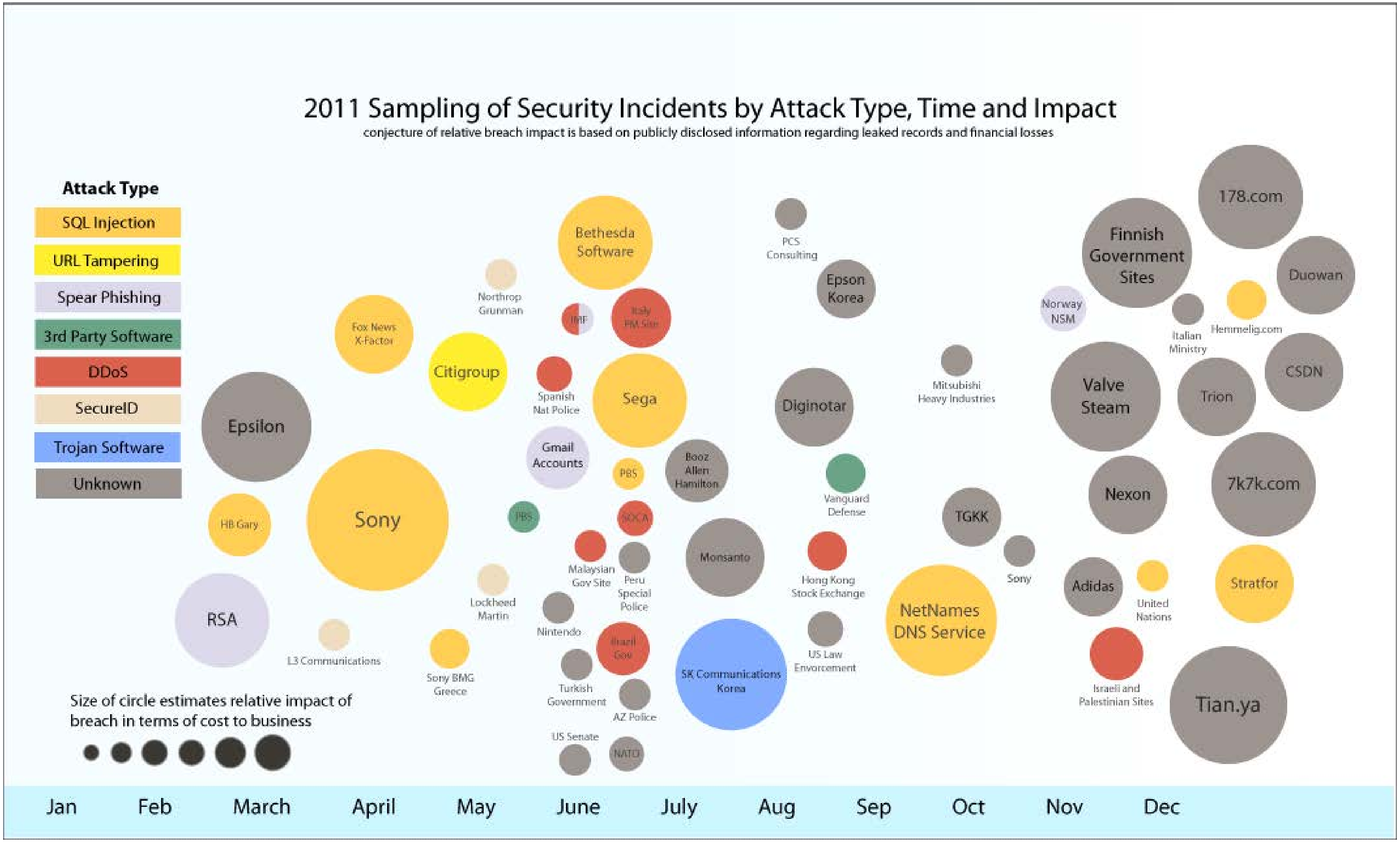
- Why Continuous Monitoring is critical
- Level set on Continuous Monitoring
  - Goals
  - CAESARS
  - A roadmap
  - (This is not a tutorial)
- Security Intelligence
- Practical implementation
  - Asset discovery & profiling
  - Protecting against threats
  - Detection & forensics
- Not undertaking ISCM process:
  - Strategy
  - Tools



Background

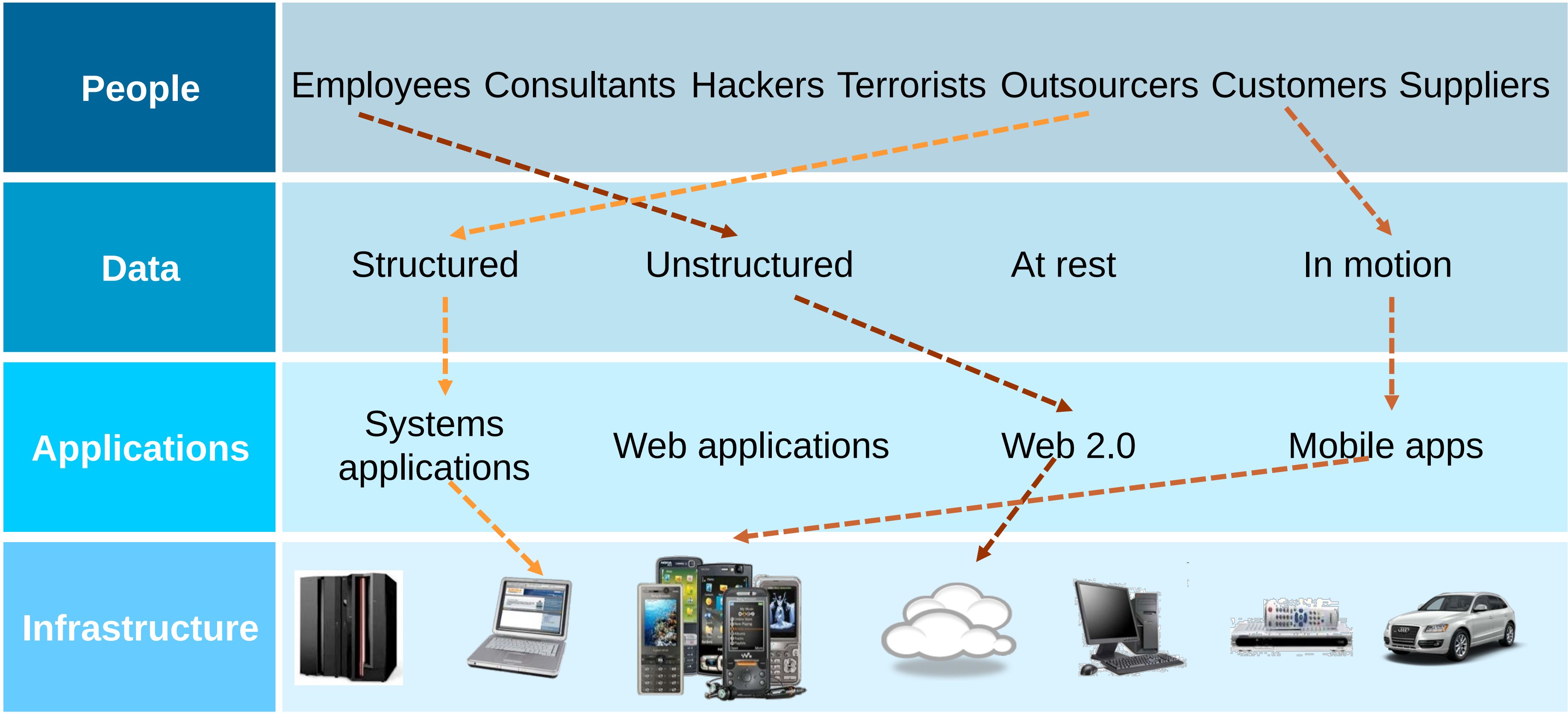
- USAF / DoD (1984 – 1991)
  - Programmer
  - Intelligence
  - Tiger/red team leader
  - DC area: Pentagon, various bases, 3-letter orgs
- FireTower (1994 – 2004)
  - Founder, president
  - Information security consulting
  - Nationwide clients: US HoR, FHLBs, Cisco, Time-Warner, NatGeo
- Private Consulting (2004 – 2009)
- Q1 Labs, Chief Security Officer (2009 – 2011)
  - Outward facing: pre- and post-sales, evangelist, customer council blogger
  - Product: compliance, Security Council, product management
- IBM, Security Strategist (2011 – present)

Set & Forget Isn't Working



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

Security is a Complex, Four-Dimensional Puzzle



People

Employees Consultants Hackers Terrorists Outsourcers Customers Suppliers

Data

Structured Unstructured At rest In motion

Applications

Systems applications Web applications Web 2.0 Mobile apps

Infrastructure

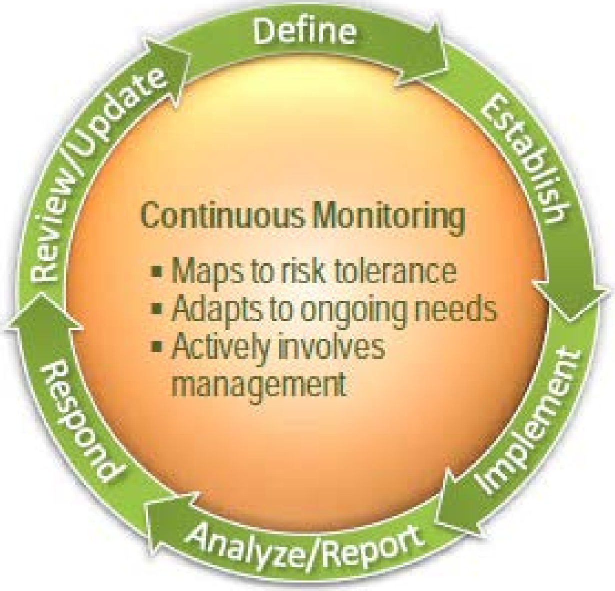
It is no longer enough to protect the perimeter – siloed point products will not secure the enterprise

Impetus for Continuous Monitoring

- Security incidents between 2006 – 2012 increased 650%
- Move away from ad-hoc, occasional, irregular VA scans
  - Does not reflect real state of security between scans
- Get away from “roomful of paper”
  - Strive for near real time situational awareness

Goals of Continuous Monitoring

- Maintain situational awareness of all systems across the organization;
- Provide actionable communication of security status across all tiers of the organization;
- Maintain an understanding of threats and threat activities;
- Assess all security controls;
- Collect, correlate, and analyze security-related information;
- Actively manage risk.
- (Maintain ATO)



Continuous Monitoring

- Maps to risk tolerance
- Adapts to ongoing needs
- Actively involves management

The ultimate goal of Continuous Monitoring is to evaluate individual organizations, both in relation to each other and in compliance to an established higher-level standard.

Key References / Guidelines—Strategic

- NIST SP 800-137:

  Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

- NIST IR7756, DRAFT:

  CAESARS Framework Extension: an Enterprise Continuous Monitoring Technical Reference Architecture

- NIST SP 800-55, rev 1:

  Performance Measurement Guide for Information Security

- NIST SP 800-37, rev 1:

  Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

- NIST SP 800-39:

  Managing Information Security Risk: Organization, Mission, and Information System View

Key References / Guidelines—Operational

- NIST SP 800-53, rev 3:

  Recommended Security Controls for Federal Information Systems and Organizations

- NIST SP 800-128:

  Guide for Security-Focused Configuration Management of Information Systems

- NIST SP 800-40, ver 2:

  Creating a Patch and Vulnerability Management Program

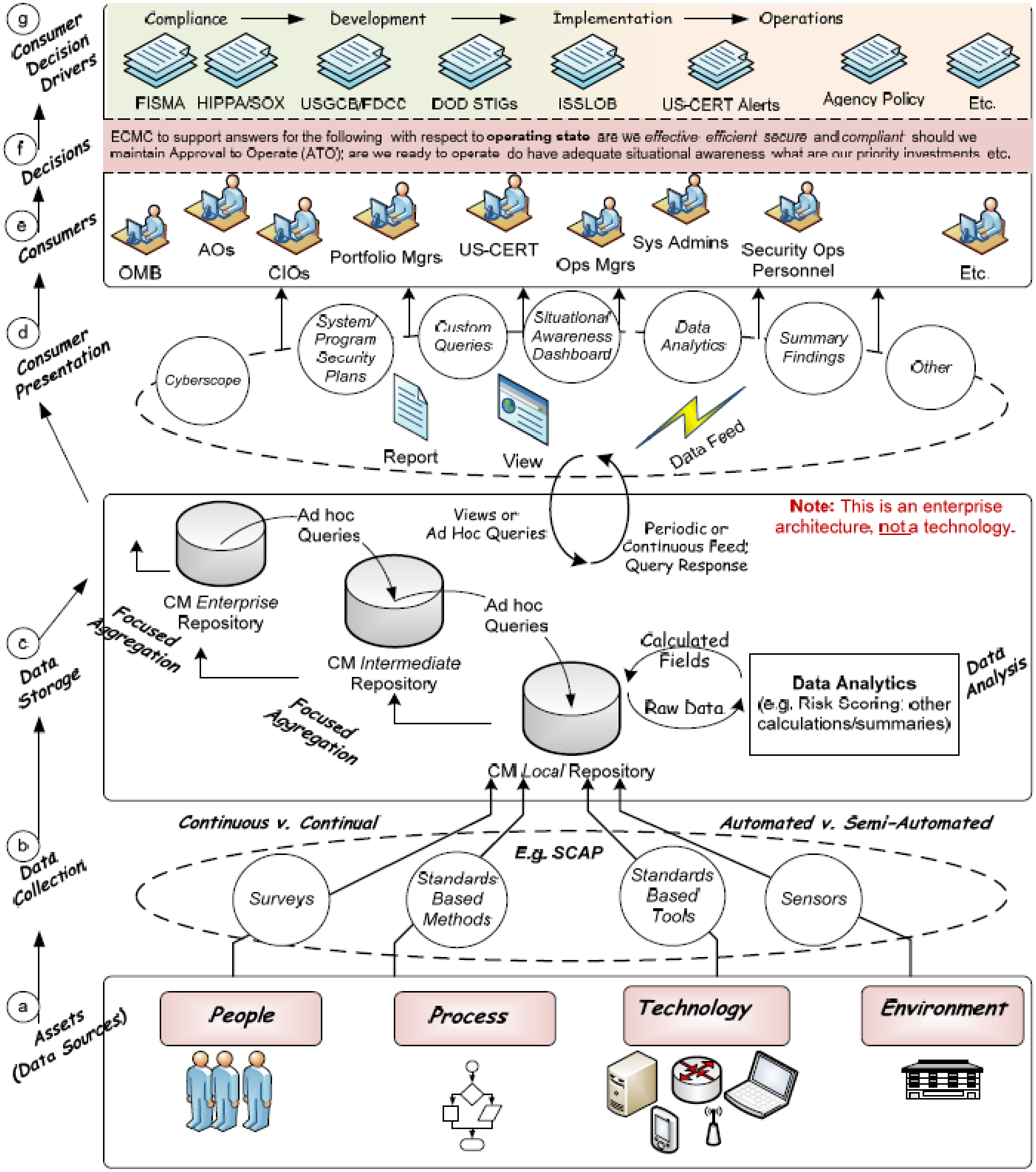
- NIST SP 800-92:

  Guide to Computer Log Management

CAESARS

- Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture
  - Sensor subsystem
  - Database/repository
  - Analysis/Risk Scoring
  - Presentation & Reporting
- Focused on organization’s assets
- Gap between actual & desired states of security protection
- Relative scoring value
  - Prioritize remedial actions
- Does not take into account criticality of assets;
  does consider severity of threat

Enterprise Architecture View of Continuous Monitoring

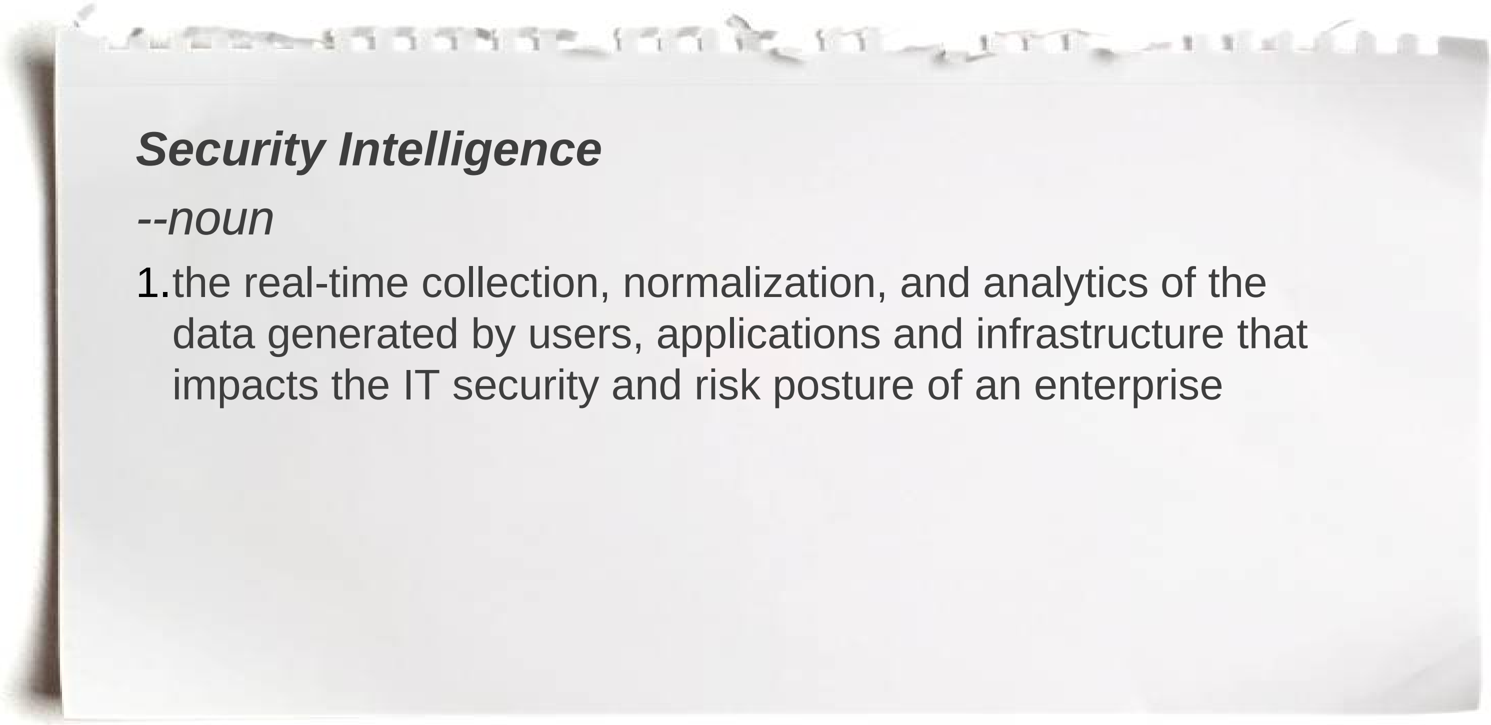


Source:
NIST IR 7756
Public Draft Rev 2

Roadmap for Continuous Monitoring

- Assets:
  - Enumerate with associated properties
  - Assess current state
  - Assess deviation from accepted baselines (“vulnerabilities”):
    - Security controls
    - Configurations
  - Quantify relative severity of gaps
    - Expressed in simple terms
    - Letter grades reflecting aggregate risk
    - Scores for hosts, sites, enterprises
  - Assign responsibility for remediation
- Processes & People: GRC
- Report to CyberScope
- Have plan to improve grade

Continuous Monitoring Is Closely Related to Security Intelligence



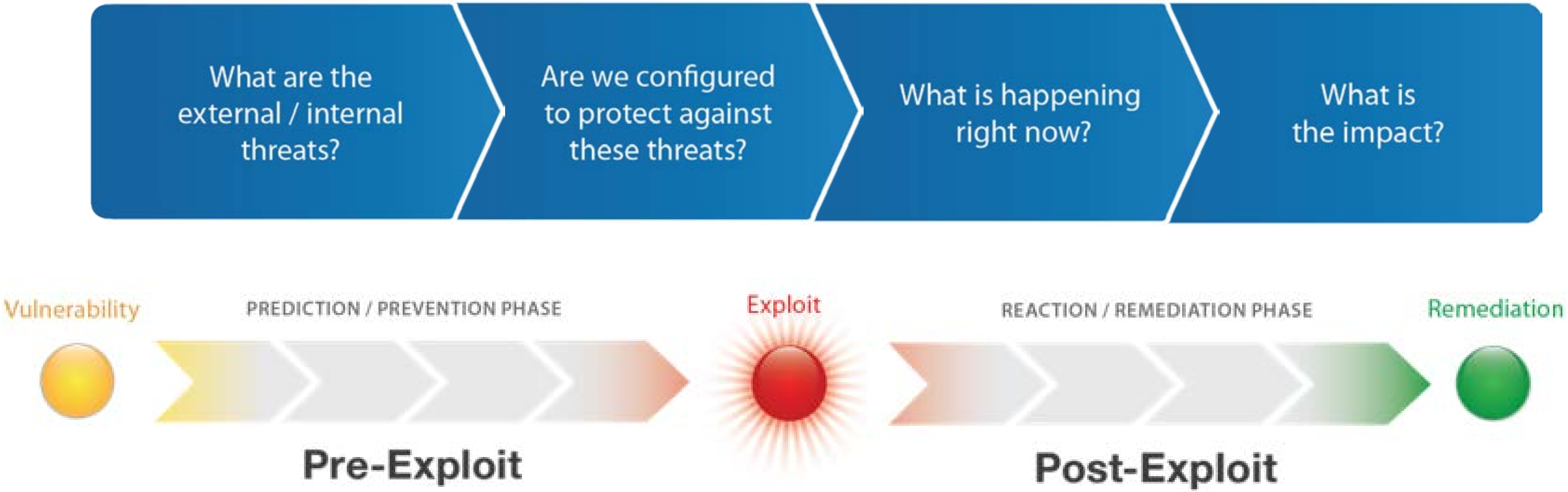
Security Intelligence

--noun

1. the real-time collection, normalization, and analytics of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise

Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

Security Intelligence Timeline


What are the external / internal threats?
Are we configured to protect against these threats?
What is happening right now?
What is the impact?
Vulnerability
PREDICTION / PREVENTION PHASE
Exploit
REACTION / REMEDIATION PHASE
Remediation
Pre-Exploit
Post-Exploit

Prediction & Prevention

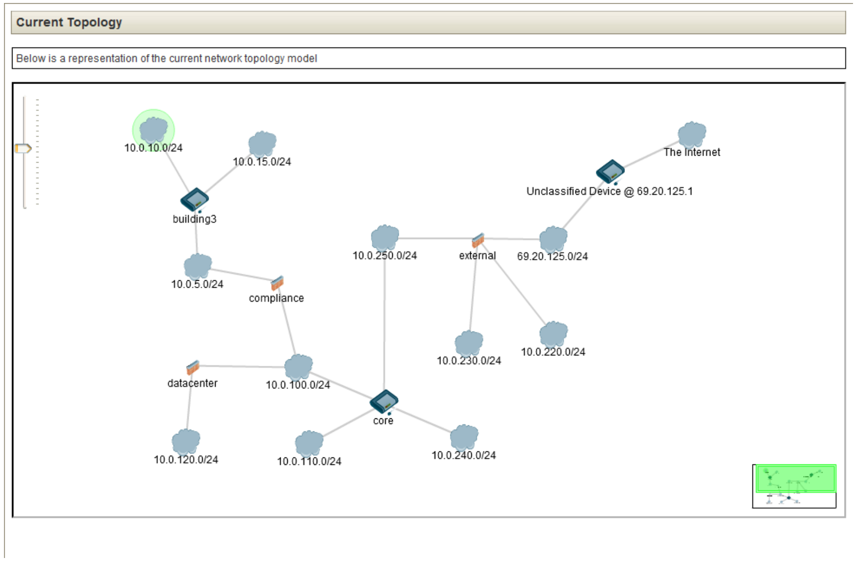
Risk Management. Vulnerability Management.
Configuration Monitoring. Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

Reaction & Remediation

SIEM. Log Management. Incident Response.
Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Loss Prevention.

Assess Internal & External Threats

- What are the Threats?
  - Internal: Risk Assessment
  - External: Threat Intelligence
- What are the Targets
  - Enumerate & Classify Assets
  - Determine interconnectivity
  - Systems, Applications, Data



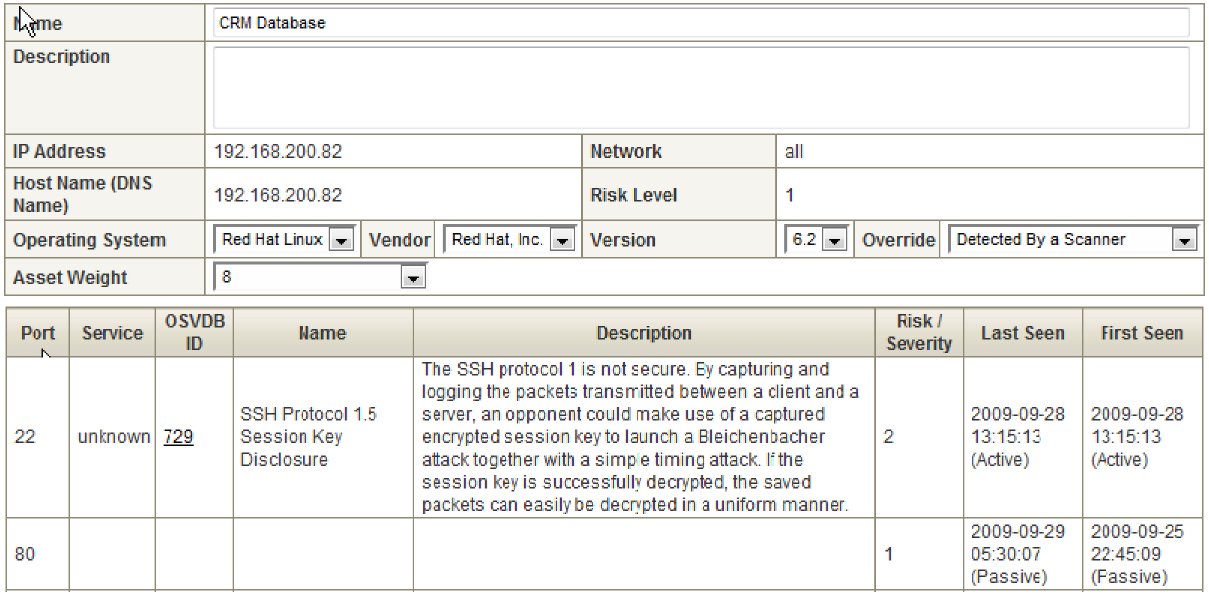
Current Topology

Below is a representation of the current network topology model

- Determine Local Baselines & Policies:
  - Endpoints (Servers, Workstations, VMs, & Mobile Devices)
  - Applications (A/V, Web, Database, Email, Finance, CRM, etc)
  - Security & Infrastructure Devices (Firewalls, IPSes, Switches/Routers)
  - Identity (Roles & Access Control)
- Define Policy
  - Access Control
  - Activities / Behavior

Passive & Active Asset Discovery & Profiling

- Build up asset database:
  - Profile assets (OS, owner, applications, vulnerabilities)
  - Establish baseline and identify changes in near real time
- Identify:
  - New systems coming online
  - Existing systems accepting connections on new ports
  - Policy violations
- Compare against CMDB

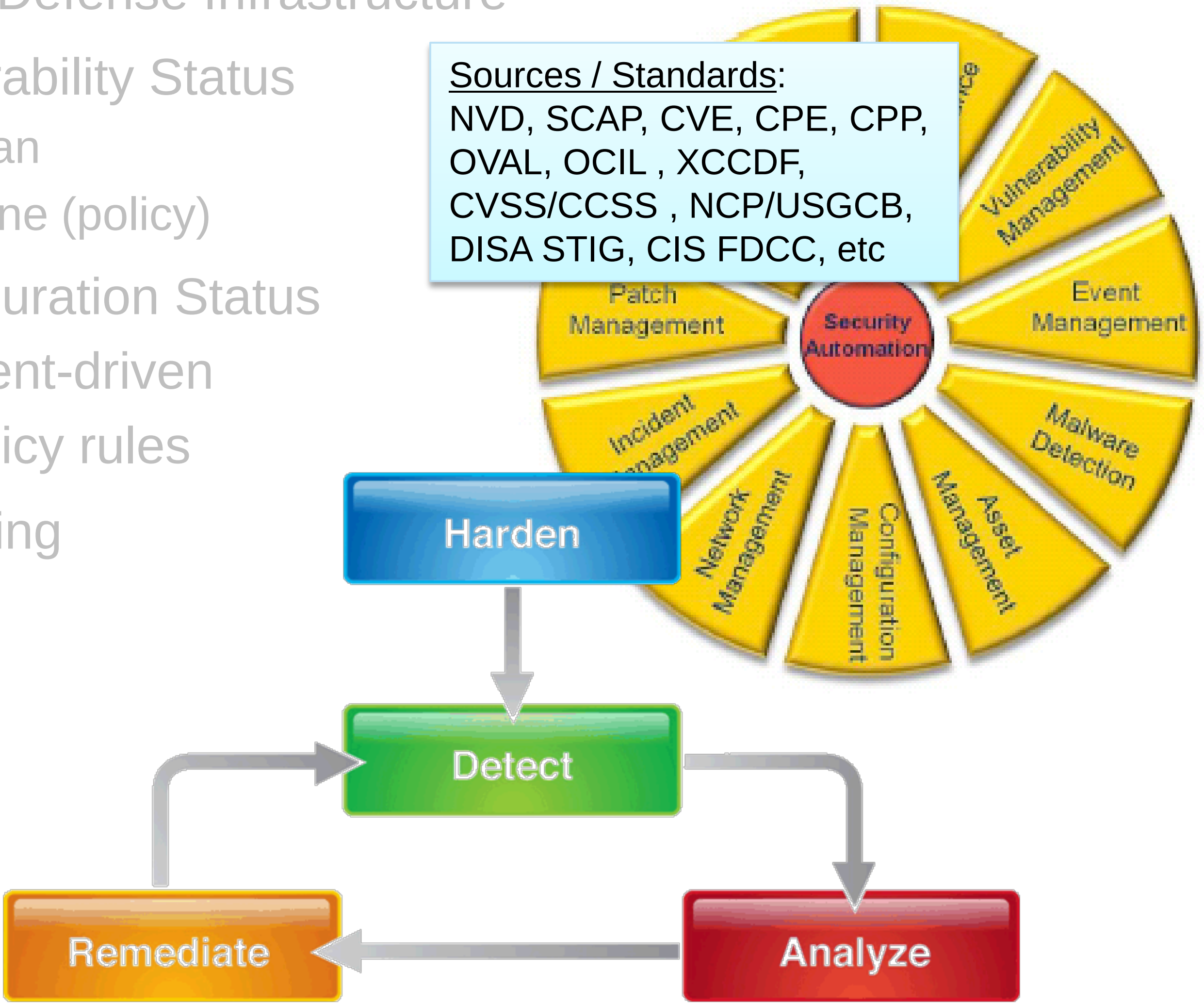


Name	CRM Database						
Description							
IP Address	192.168.200.82			Network	all		
Host Name (DNS Name)	192.168.200.82			Risk Level	1		
Operating System	Red Hat Linux	Vendor	Red Hat, Inc.	Version	6.2	Override	Detected By a Scanner
Asset Weight	8						

Port	Service	OSVDB ID	Name	Description	Risk / Severity	Last Seen	First Seen
22	unknown	729	SSH Protocol 1.5 Session Key Disclosure	The SSH protocol 1 is not secure. Ey capturing and logging the packets transmitted between a client and a server, an opponent could make use of a captured encrypted session key to launch a Bleichenbacher attack together with a simple timing attack. If the session key is successfully decrypted, the saved packets can easily be decrypted in a uniform manner.	2	2009-09-28 13:15:13 (Active)	2009-09-28 13:15:13 (Active)
80					1	2009-09-29 05:30:07 (Passive)	2009-09-25 22:45:09 (Fassive)

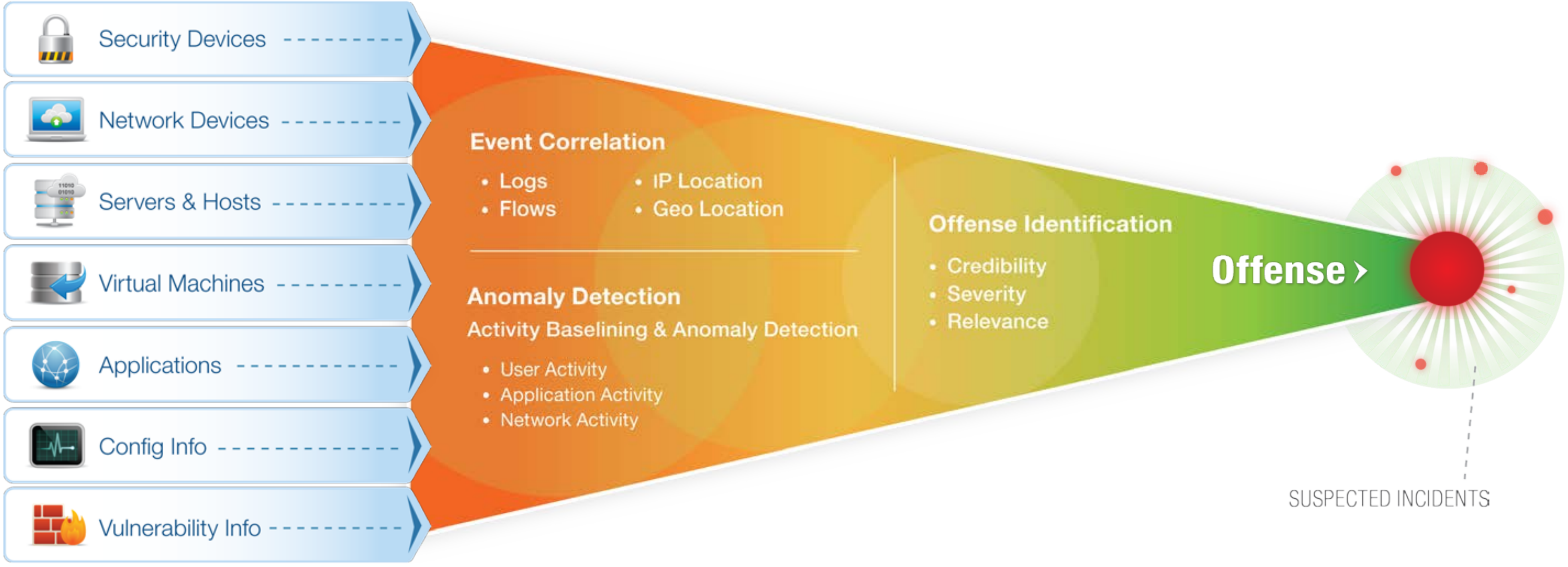
Protect Against Threats

- Assume Existing Defense Infrastructure
- Determine Vulnerability Status
  - Vulnerability Scan
  - Actual vs Baseline (policy)
- Determine Configuration Status
  - Periodic or event-driven
  - Automated policy rules
- Scoring & Reporting



Sources / Standards:
NVD, SCAP, CVE, CPE, CPP, OVAL, OCIL , XCCDF, CVSS/CCSS , NCP/USGCB, DISA STIG, CIS FDCC, etc

What’s Happening Right Now: Real Time Security Intelligence



Security Devices

Network Devices

Servers & Hosts

Virtual Machines

Applications

Config Info

Vulnerability Info

Event Correlation

- Logs
- Flows
- IP Location
- Geo Location

Anomaly Detection

Activity Baselining & Anomaly Detection

- User Activity
- Application Activity
- Network Activity

Offense Identification

- Credibility
- Severity
- Relevance

Offense ›

SUSPECTED INCIDENTS

Most Sources + Most Intelligence = Most Accurate & Actionable Insight

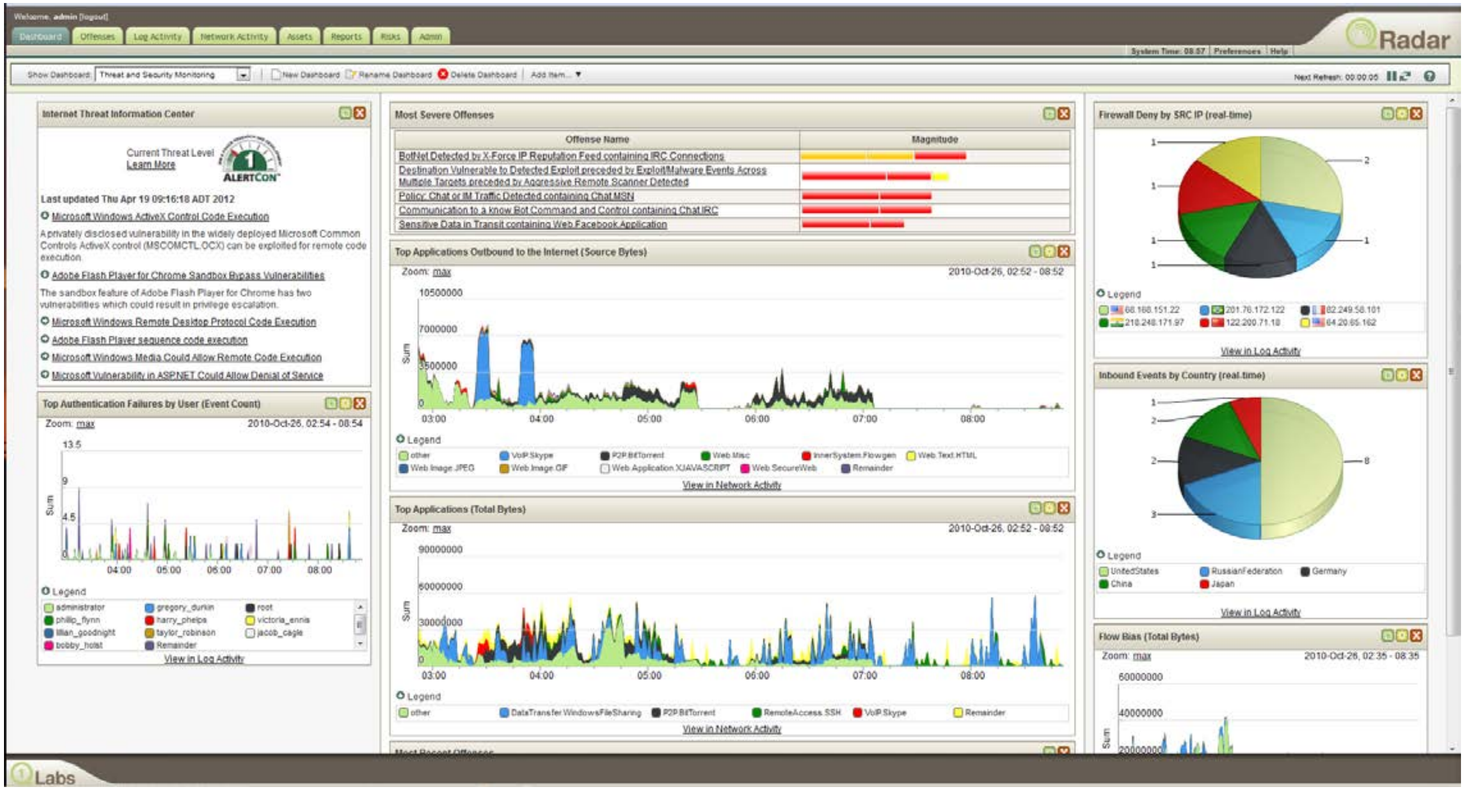
Monitor in Real Time & Determine the Impact

- Analysis—SIEM
  - De-duplication, correlating, searching
  - No discarding of information: store both raw & normalized data
  - Harmonization:

    IPS identifies attack; target vulnerable (VA scanner + patch not applied); but firewall blocking attack
- Packet Forensics
- Incident Response

Profile Activity & Behavior

- Profile activity on systems, applications, network
- Write policies and enforce them
- Helps detect day-zero attacks with no signature; provides visibility into attacker communications



Show Dashboard: Threat and Security Monitoring

Internet Threat Information Center

Current Threat Level
Learn More
1 ALERTCON

Last updated Thu Apr 19 09:16:18 ADT 2012

- Microsoft Windows ActiveX Control Code Execution

A privately disclosed vulnerability in the widely deployed Microsoft Common Controls ActiveX control (MSCOMCTL.OCX) can be exploited for remote code execution.

- Adobe Flash Player for Chrome Sandbox Bypass Vulnerabilities

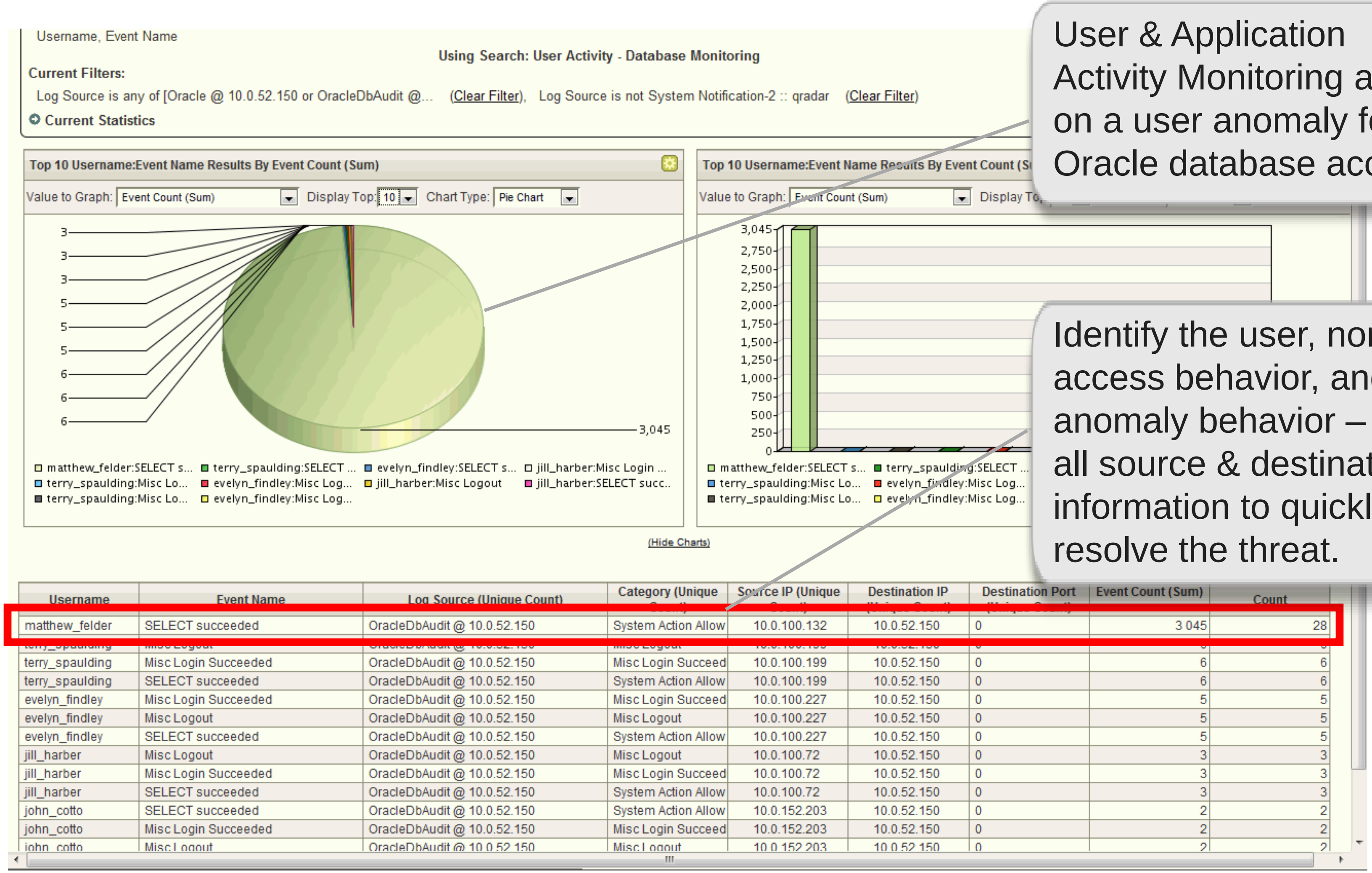
The sandbox feature of Adobe Flash Player for Chrome has two vulnerabilities which could result in privilege escalation.

- Microsoft Windows Remote Desktop Protocol Code Execution
- Adobe Flash Player sequence code execution
- Microsoft Windows Media Could Allow Remote Code Execution
- Microsoft Vulnerability in ASP.NET Could Allow Denial of Service

Most Severe Offenses

Offense Name	Magnitude
BotNet Detected by X-Force IP Reputation Feed containing IRC Connections	
Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Across Multiple Targets preceded by Aggressive Remote Scanner Detected	
Policy: Chat or IM Traffic Detected containing Chat.MSN	
Communication to a know Bot Command and Control containing Chat.IRC	
Sensitive Data in Transit containing Web.Facebook.Application	

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

□ 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

□ 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)

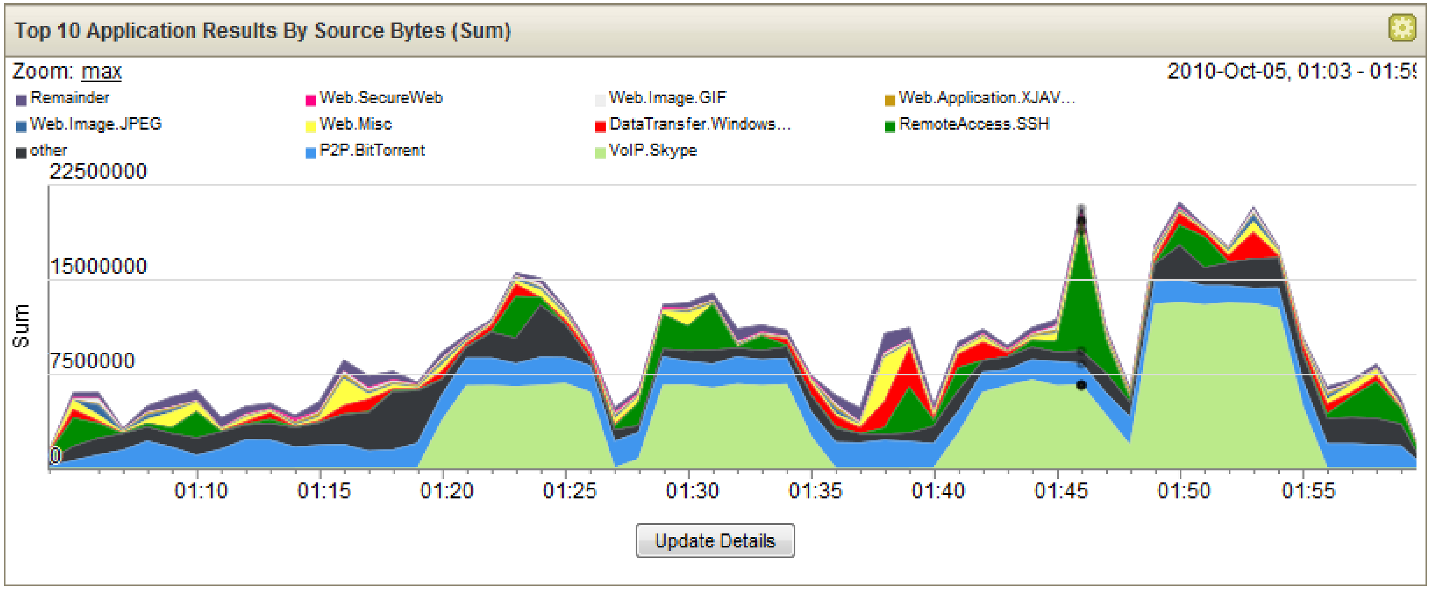
Username	Event Name	Log Source (Unique Count)	Category (Unique	Source IP (Unique	Destination IP	Destination Port	Event Count (Sum)	Count
matthew_felder	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.132	10.0.52.150	0	3 045	28
terry_spaulding	Misc Logout	OracleDbAudit @ 10.0.52.150	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.

Network Activity Monitoring (Network Flows)

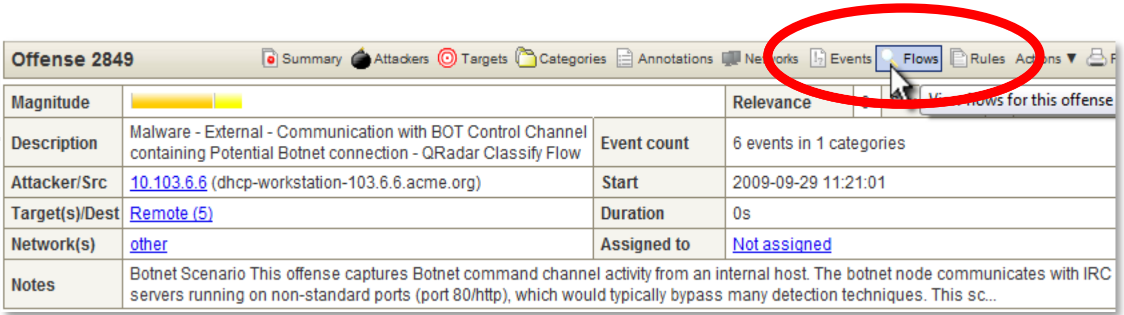
- Attackers can stop logging and erase their tracks, but can’t cut off the network
- Helps detect day-zero attacks with no signature; provides visibility into attacker communications
- Network activity can build up an asset database and profile assets
- Useful for non-security related issues as well



Application and Threat Detection with Forensic Evidence

Potential Botnet Detected?

This is as far as traditional SIEM can go

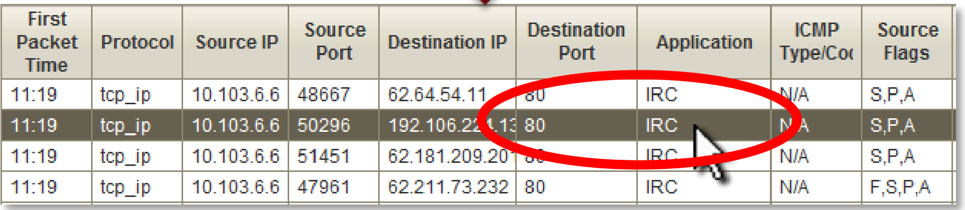


Offense 2849

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?

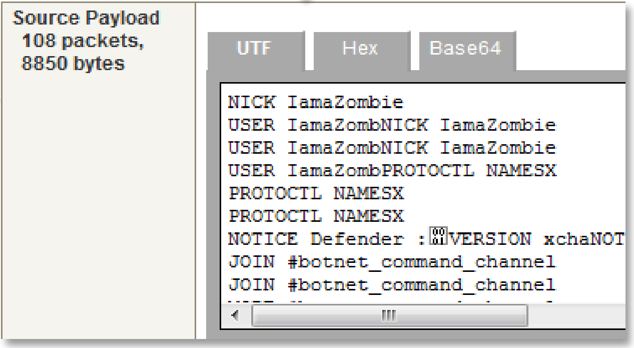
IBM Security QRadar QFlow detects a covert channel



First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Coi	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

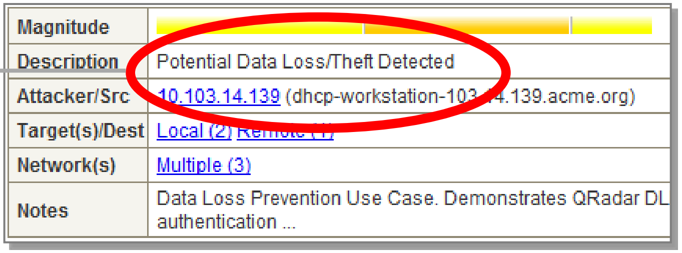
```
NICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombPROTOCTL NAMESX
PROTOCTL NAMESX
PROTOCTL NAMESX
NOTICE Defender :VERSION xchaNOT
JOIN #botnet_command_channel
JOIN #botnet_command_channel
```

Application layer flow analysis can detect threats others miss

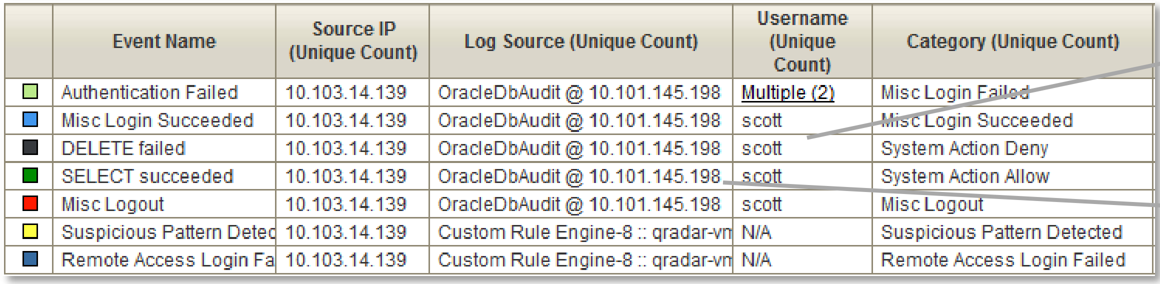
Detecting Insider Fraud and Data Loss

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 ...



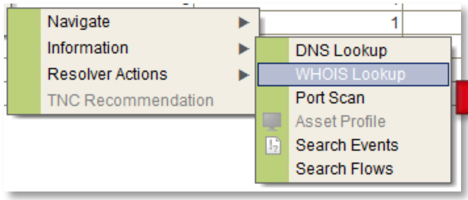
	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
🟩	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
🟦	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded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

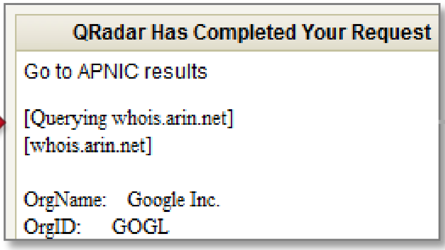
Who?

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

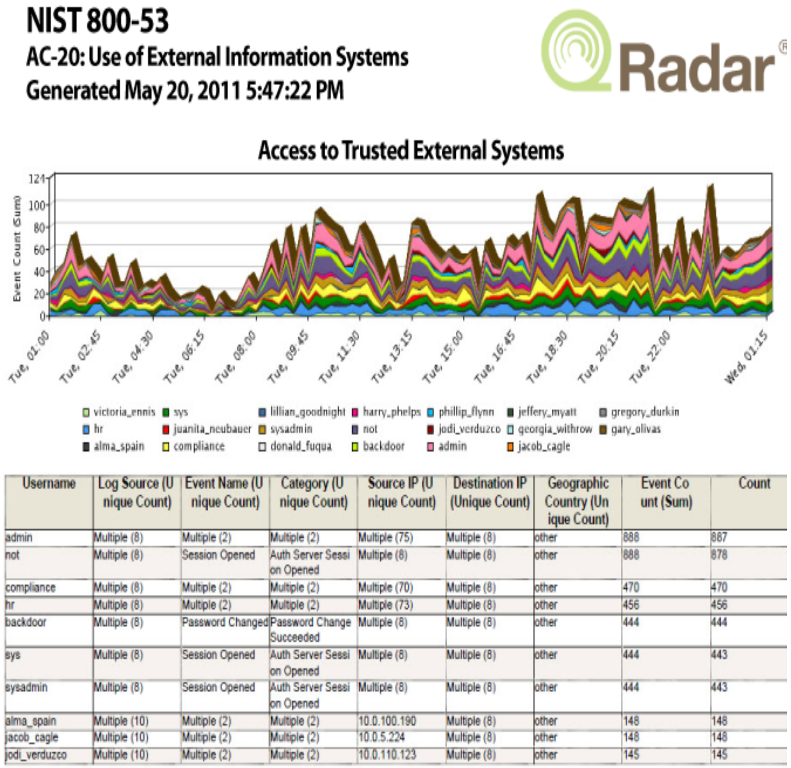
Where?

Gmail

Threat detection in the post-perimeter world

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

Security Intelligence & Continuous Monitoring



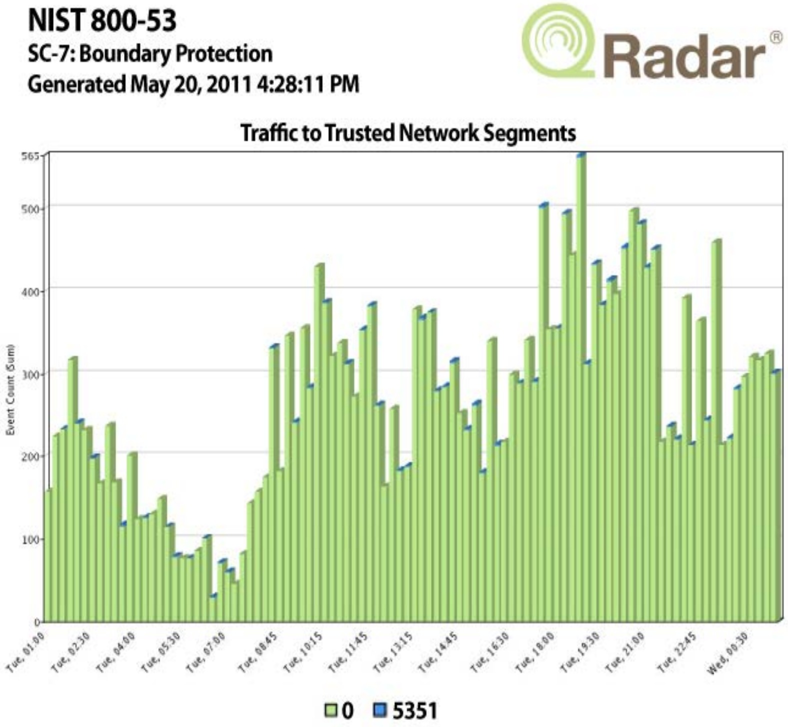
NIST 800-53

AC-20: Use of External Information Systems

Generated May 20, 2011 5:47:22 PM

Access to Trusted External Systems

Username	Log Source (Unique Count)	Event Name (Unique Count)	Category (Unique Count)	Source IP (Unique Count)	Destination IP (Unique Count)	Geographic Country (Unique Count)	Event Count (Sum)	Count
admin	Multiple (8)	Multiple (2)	Multiple (2)	Multiple (75)	Multiple (8)	other	888	887
not	Multiple (8)	Session Opened	Auth Server Session Opened	Multiple (8)	Multiple (8)	other	888	878
compliance	Multiple (8)	Multiple (2)	Multiple (2)	Multiple (70)	Multiple (8)	other	470	470
hr	Multiple (8)	Multiple (2)	Multiple (2)	Multiple (73)	Multiple (8)	other	456	456
backdoor	Multiple (8)	Password Changed	Password Change Succeeded	Multiple (8)	Multiple (8)	other	444	444
sys	Multiple (8)	Session Opened	Auth Server Session Opened	Multiple (8)	Multiple (8)	other	444	443
sysadmin	Multiple (8)	Session Opened	Auth Server Session Opened	Multiple (8)	Multiple (8)	other	444	443
alma_spain	Multiple (10)	Multiple (2)	Multiple (2)	10.0.100.190	Multiple (8)	other	148	148
jacob_cagle	Multiple (10)	Multiple (2)	Multiple (2)	10.0.5.224	Multiple (8)	other	148	148
jodi_verduzco	Multiple (10)	Multiple (2)	Multiple (2)	10.0.110.123	Multiple (8)	other	145	145



NIST 800-53

SC-7: Boundary Protection

Generated May 20, 2011 4:28:11 PM

Traffic to Trusted Network Segments

Intelligent solutions provide the DNA to secure a Smarter Planet

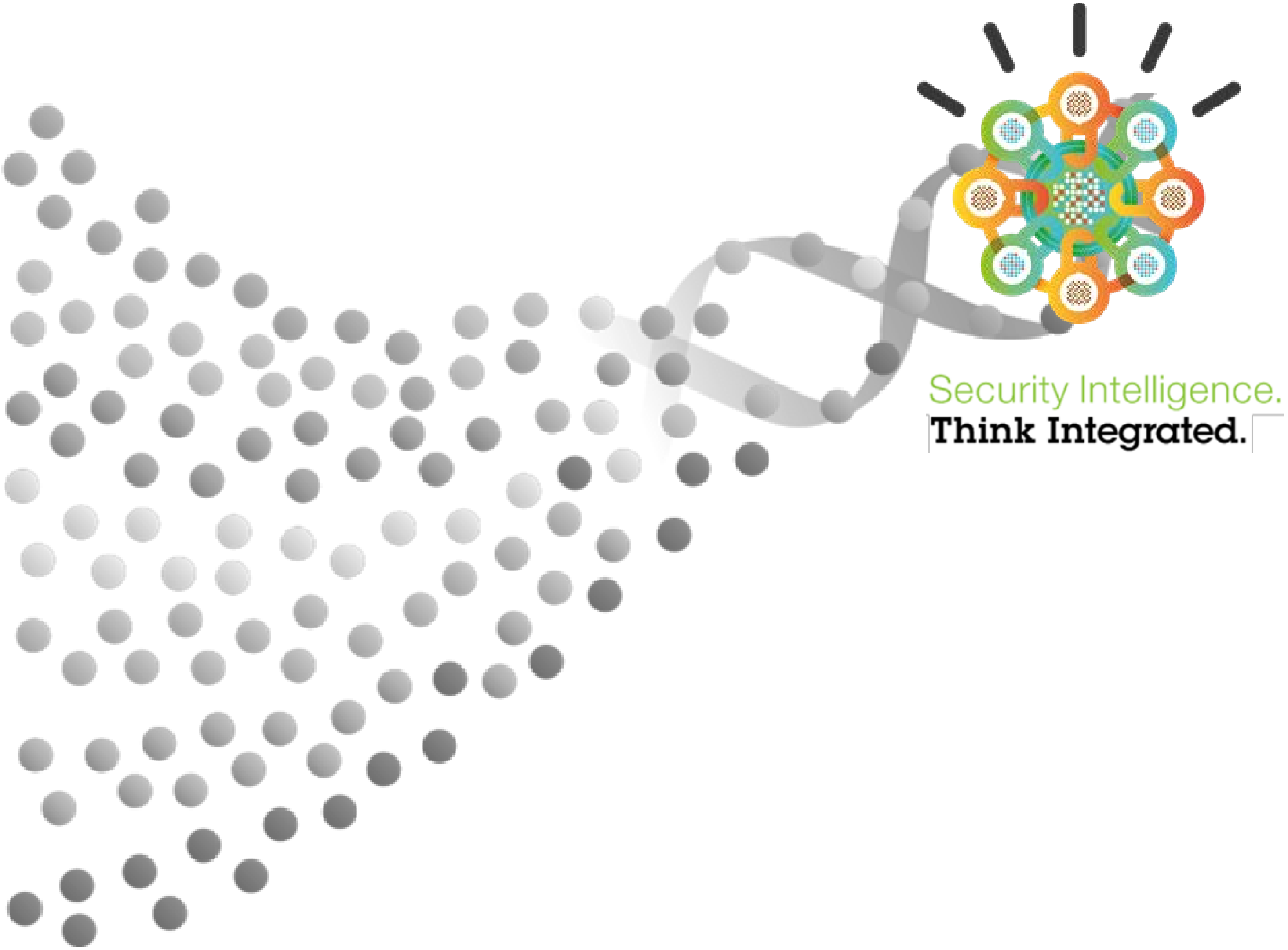
Security Intelligence, Analytics & GRC

People

Data

Applications

Infrastructure

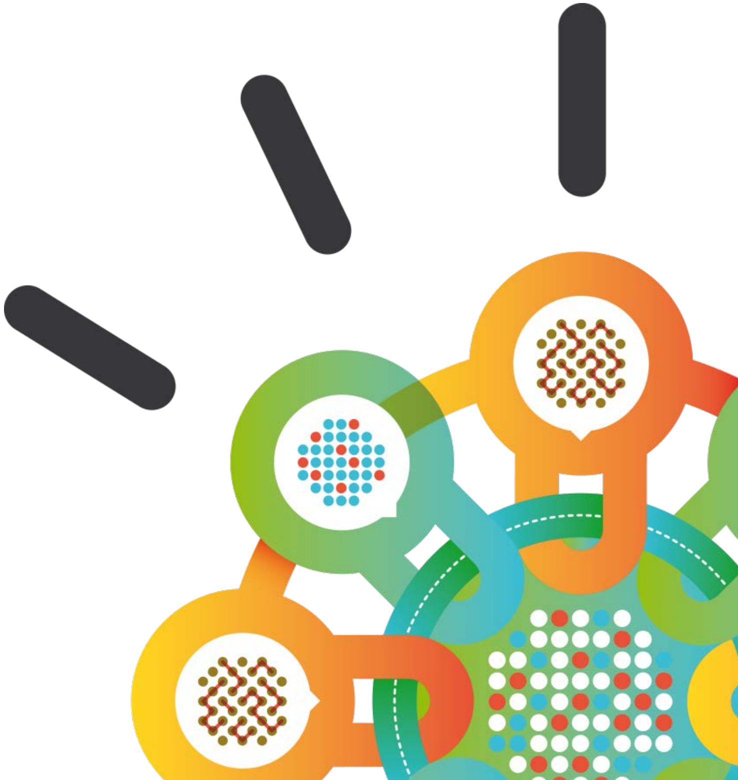


Security Intelligence.
Think Integrated.

Security Intelligence.
Think Integrated.

Don’t just comply with Continuous Monitoring; use it as an opportunity to:

- ✓ Create budget, and
- ✓ Put together the security program of your dreams



Thank You!

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.