Uncovering the Insider THREATS !!

Jude Pereira

Managing Director

NANJGEL Solutions

www.nanjgel.com

AGENDA :

1. The Insider Threat Battles
2. Types of Insider Threats
3. Detection of Insider Threats
4. The Framework for Insider Threat Detection & Remediation

1. The Insider Threat Battles

The Insider Threat Battles ???

- Humans will always make mistakes
- System and application vulnerabilities continue to emerge
- Malware detection will always lag

KrebsonSecurity
In-depth security news and investigation

27 Microsoft Warns of Attacks on IE Zero-Day

soft is warning Internet Explorer users about active attacks that attempt to ex

Vulnerabilities

Adobe Patches Flash Player Zero-Day Used in Watering-hole Attacks

e Lennon on April 28, 2014

infosecurity EUROPE

News

Cost of Data Breaches Spikes 15% in Last Year

06 May 2014

Topic: Security

Follow via:

Windows XP: Microsoft can't wash its hands of the security problem so easily

Summary: Microsoft might want to draw a line under Windows XP; hackers and users will be reluctant to let it off the hook.

ADVERTISEMENT

SEARCH

SCRIBE | LOG IN

R THE SITE

BER CENTER

Target CEO resigns as fallout from data breach continues

Harsh realities for CISOs

Attackers spend an estimated **243 days on a victim's network** before being discovered

In 2013, it took organizations **32 days** on average **to resolve a cyber-attack**

In 2012, **38%** of targets were **attacked again** once the original incident was remediated.

63% of victims **made aware** of their breaches **by an external organization**

Annual cost of cyber-crime in the U.S. now stands at **$11.56 million per organization**

Has our organization been compromised?

When was our security breached?

How do we identify the attack?

What type of attack is it?

What resources and assets are at risk?

How to avoid becoming a repeat victim?

THE CYBERCRIMINAL UNDERGROUND:

HOW CYBERCRIMINALS ARE GETTING BETTER AT STEALING YOUR MONEY

Your online activities make you a cybercriminal target.

Online Banking

Transactions get riskier as cybercriminals use cheaper, more sophisticated tools

Prices (in US$):

- 140 ▸ LATIN AMERICA: PiceBOT, crimeware kit for stealing banking data
- 2-25 ▸ RUSSIA: copies of credit cards, passports, work permits

Facts:

112,981 Online Banking Malware Victims in Q1 2013

US$ 225,334

Amount made by China's Topfox Case Gang on online banking theft

Email

Even with advanced spam filtering, you're still prone to spam

Prices (in US$):

- 30 ▸ Email spamming and flooding tool
- 3 ▸ Email fooding service per 1,000 emails
- 10 ▸ Spamming service per 1,000,000 emails

Facts:

5.2 BILLION

Spam messages sent every month worldwide

Online Gaming

The popularity of in-game purchases have made gamers prime cybercriminal targets

Facts:

5.3 BILLION

Game credentials stolen by China's Blandness Gang in 2009

US$225 M

Online game assets stolen by cybercrime groups in 2011

Bad Patching Practices

With how exploit kits are being traded, users who forgo patching put their data in danger

Prices (in US$):

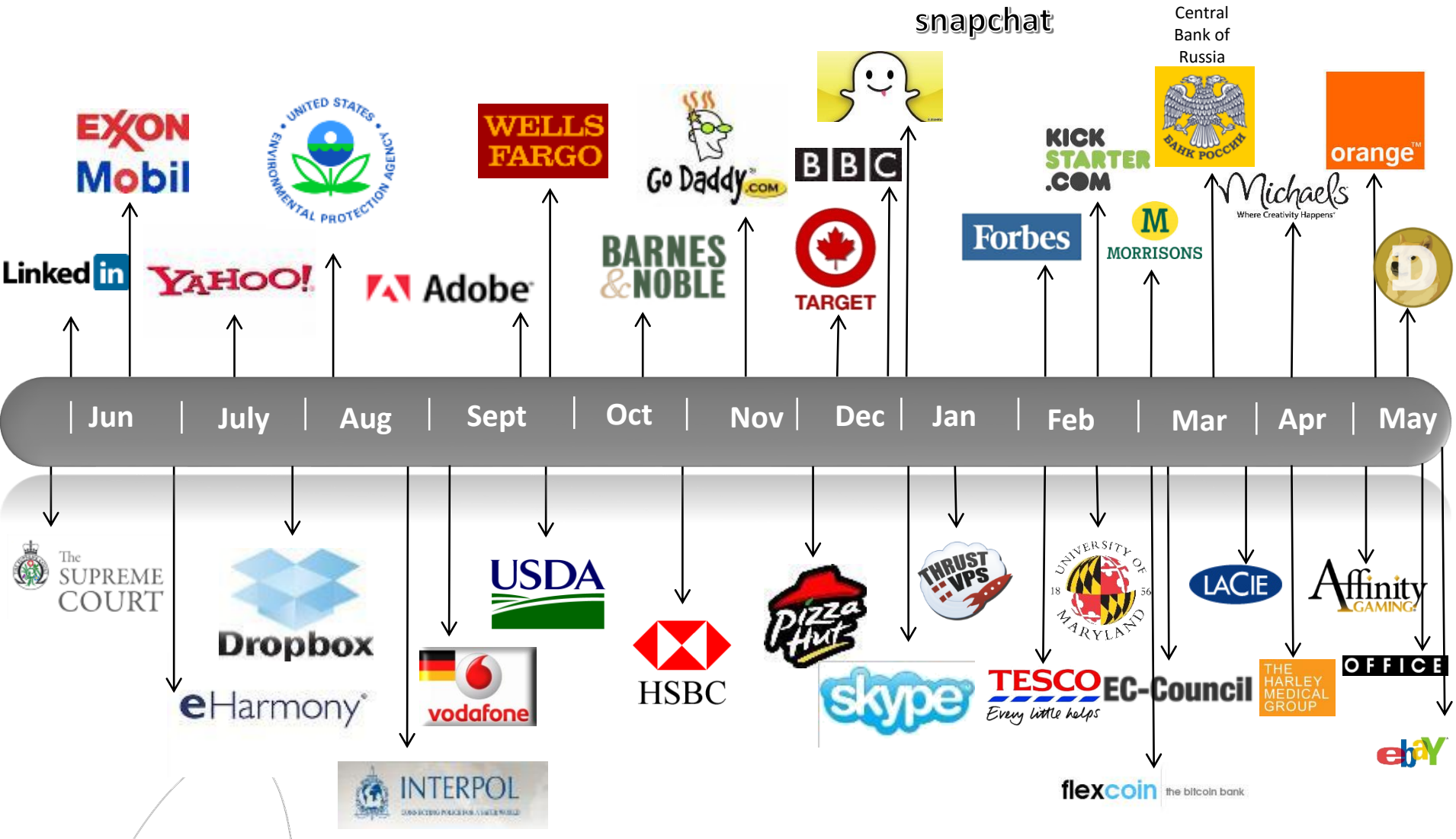
- 3,000 ▸ Rental of STYX Exploit Pack per month
- 25 ▸ Rental of exploit kit bundles per day
- 2,500 ▸ Minimum price for individual exploit kits

Facts:

JAVA Most targeted software platform in 2012

WINDOWS COMMON CONTROLS Most exploited vulnerability in targeted attacks in 2012

Sample of Breaches Last 12 Months



Post Breach Facts

100%

- Of victims had up-to-date AV

67%

- Of breaches were reported by third parties

100%

- Of breaches involved compromised credentials

229

- The median number of days an attacker was on the network

Source: Mandiant M-Trends 2014 report

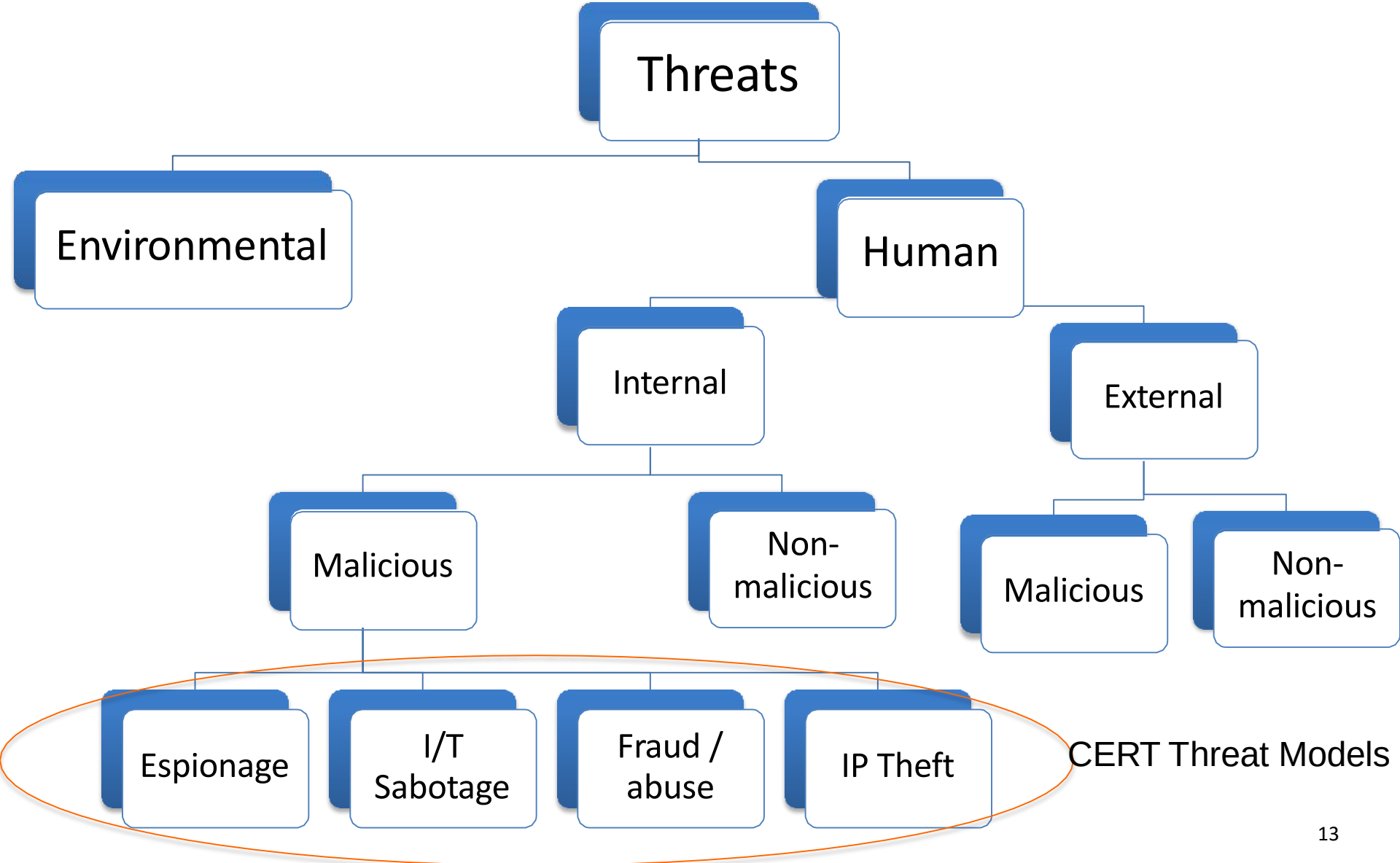
2. Types of Insider Threats

Insider Facts

- Insider threats are not hackers
- Insider threat is not a technical or "cyber security" issue alone
- A good insider threat program should focus on deterrence, not detection
- Detection of insider threats has to use behavioral based techniques
- The science of insider threat detection and deterrence is in its infancy

Source: *FBI*

The Threat Tree



Insider Threats

Definition

- An authorized user of a system who
  - Unwittingly aids or directly performs bad actions
  - Performs bad actions with the best possible intentions
  - Intentionally performs bad actions (motivation is irrelevant)
- Insider threat more insidious than external threats and may be harder to detect

Insider Threats

Perpetrators

- People with Privileged Access across the infrastructure
- Employees who share credentials ?
- Default use of vendor supplied passwords
- Inappropriate access to users
- Cowboys in the organization who consider themselves beyond any policy
- Remote or traveling users
- Disgruntled insiders
- Malicious Employees

Insider Threats

Inside Hacker Penetration

- Social engineering
  - Low tech but can be powerful
  - Mostly performed over the phone or e-mail
- Impersonation
  - Encrypt your authentication in transit
  - User credentials should not be emailed
- Hacker Penetration through Network
- Modems on the network
  - Direct connect to analog lines
  - Analog/digital converters
- Web capable phones
- Wireless LANs
- Portable Media (thumb drives)

Mo#va#on for Insider A0acks	Countermeasure
greed/financial need	?
revenge	disgruntlement mi2ga2on
terrorism	periodic background checks
ideology, poli2cal ac2vism, or radicalism	periodic background checks
coercion/blackmail	periodic background checks
social engineering/seduc2on	educa2on
narcissism/ego/need to feel important or smart, or to gain recogni#on	enlist & ego stroke hacker types
desire to prove that a warned about vulnerability or threat is real	take security professionals & their concerns seriously; welcome cri2cism
desire for excitement	?
mental illness?	periodic background checks?
inadvertent compromise of security via care--lessness, error, ignorance, laziness, arrogance	educate, mo2vate, reward, ~~punish~~


COULD YOU BE
TOMORROW'S
HEADLINE?
Ctrl

What Can You Do?

To Protect Data? Systems? Trust?

3. Challenges of Detecting Insider Threats

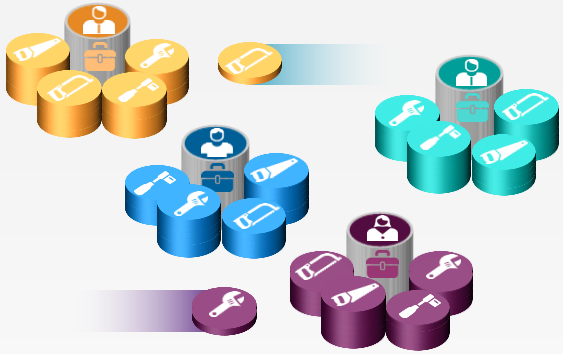
Today's threats require greater clarity to detect & resolve

Network Security	Detect unauthorized activities targeting critical assets, uncover the motivations and develop an understanding of the full scope of the risk
Insider Threat Analysis	Find the perpetrator, identify collaborators, pinpoint the systems compromised and document any data losses
Fraud and Abuse	Uncover sophisticated schemes involving multiple seemingly disparate interactions aiming to perform fraudulent or abusive transactions
Evidence Gathering	Compile evidence against malicious entities breaching secure systems and deleting or stealing sensitive data

The Detection Problem:
A Needle in a Stack of Needles

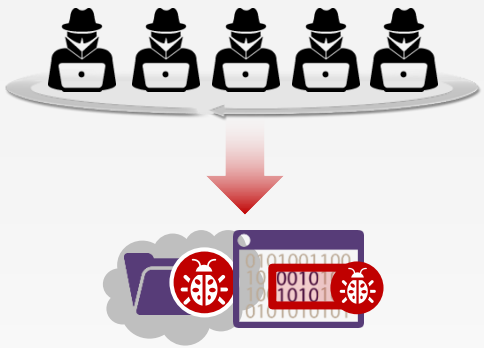
Do you have the right weapons?

Fragmented market with point products



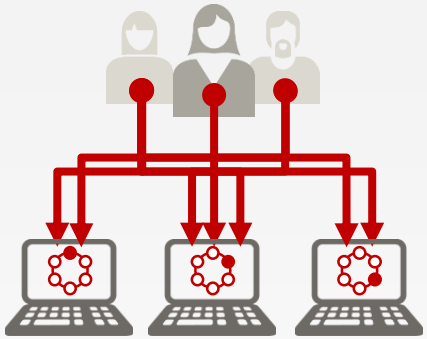
- Endpoint protection market is highly fragmented with many point solutions
  - e.g., Sandboxing, application control, whitelisting

Major security control gaps



- Existing products offer no controls for major attack vectors
  - e.g., Zero-day exploits, applicative Java attacks

Challenging manageability and operations

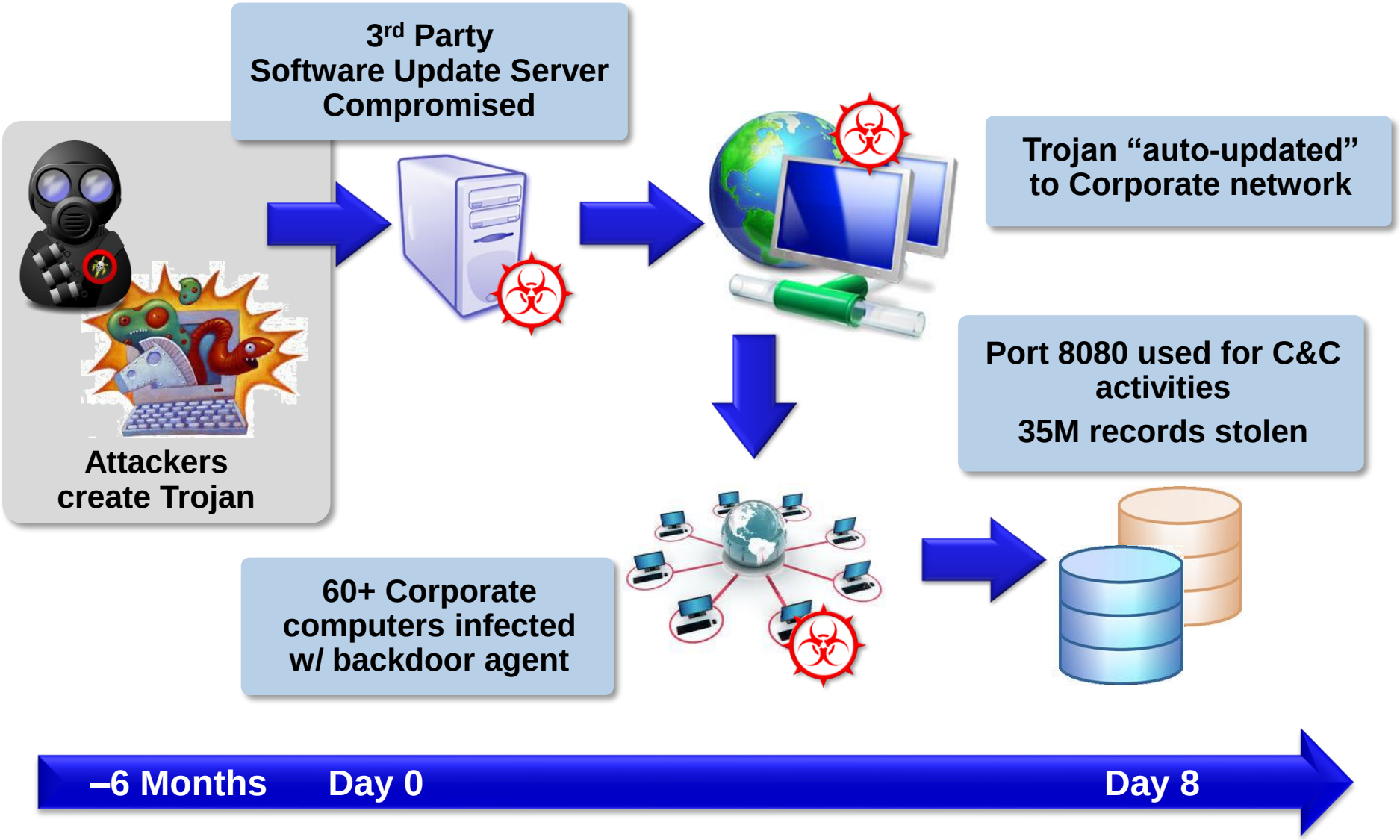


- Advanced threat solutions are difficult and costly to operate
- Difficult to scale manual remediation processes to thousands of enterprise endpoints
- High false positive rates
- Whitelisting processes on endpoints non-manageable

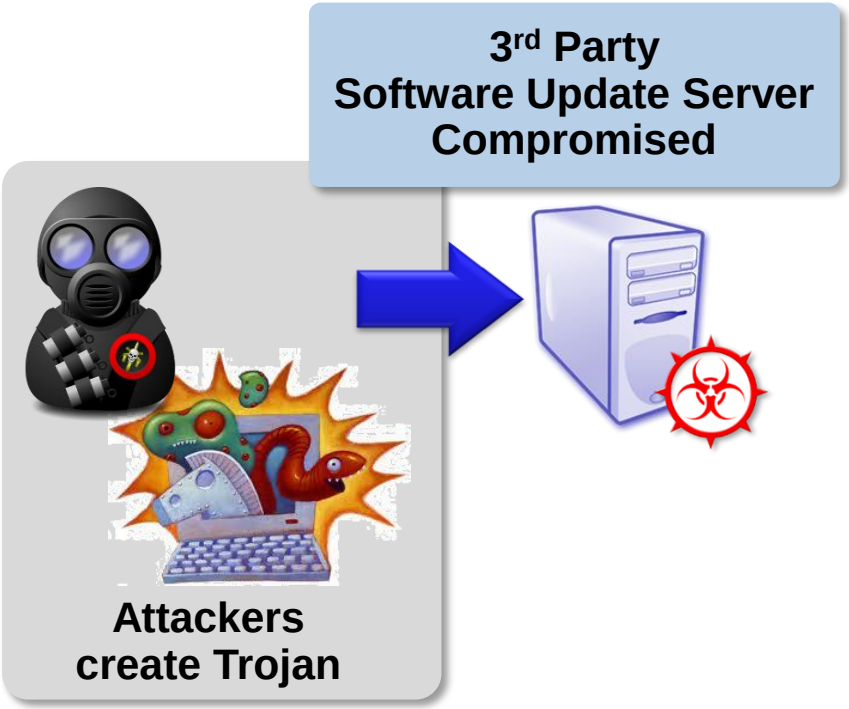
How do Inside Attackers Prepare?

- Scan the corporate website, Google, and Google News
  - Who works there? What are their titles?
- Search for LinkedIn, Facebook, and Twitter Profiles
  - Who do these people work with?
  - Fill in blanks in the org chart
- Who works with the information we want to target?
  - What is their reporting structure?
  - Who are their friends?
  - What are they interested in?
  - What is their email address?

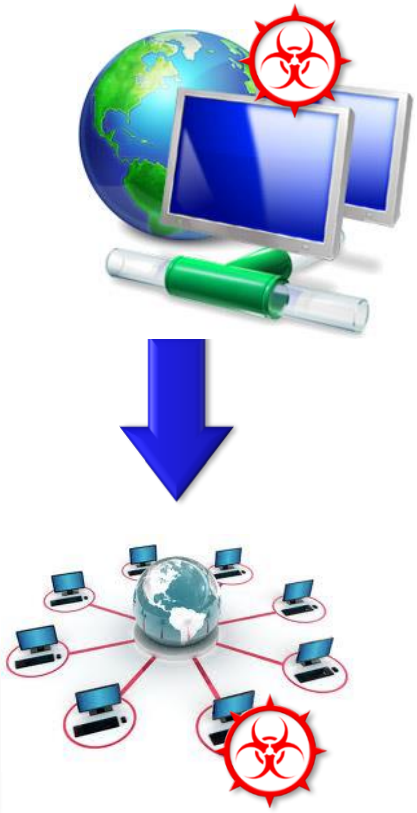
Anatomy of a THREAT – Leading Bank



Anatomy of a THREAT – Leading Bank



Anatomy of a THREAT – Leading Bank

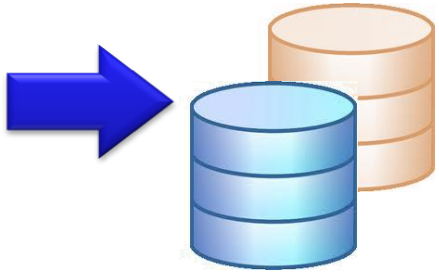


60+ Corporate computers infected w/ backdoor agent

Anatomy of a THREAT – Leading Bank

Port 8080 used for C&C activities

35M records stolen



Anatomy of a THREAT – Leading Bank

Bank lost the personal data of 35M+ users	How it could have been avoided
▪ Attackers exploited a 3rd party software provider to effectively "Auto-Update" a Trojan onto the bank's network ▪ Over a period of 8 days infected 60+ computers and gained access to bank network to learn how to compromise their databases ▪ Communicated with C&C on port 8080 (common alternate web port) ▪ According to analysis of the malware, it was compiled 6 months before the attack	▪ **Business Partner Security.** The partner should have examined the policies of the bank ▪ **Recon Detection.** During the 8 days of recon there were most likely many signs of the 60+ computers doing recon ▪ **Anomaly Detection.** During much of the time the Trojan was in place, a number of DNS based anomalies were present in DNS logs ▪ **Database Monitoring and Protection**

Malicious Activity

Problem Statement

- Distributed infrastructure
- Security blind spots in the network
- Malicious activity that promiscuously seeks ‘targets of opportunity’
- Application layer threats and vulnerabilities
- Silo’d security telemetry
- Incomplete forensics

Required Visibility

- Distributed detection sensors
- Pervasive visibility across enterprise
- Application layer knowledge
- Content capture for impact analysis

User Activity Monitoring

Problem Statement

- Monitoring of privileged and non-privileged users
- Isolating 'Stupid user tricks' from malicious account activity
- Associating users with machines and IP addresses
- Normalizing account and user information across diverse platforms

Required Visibility

- Centralized logging and intelligent normalization
- Correlation of IAM information with machine and IP addresses
- Automated rules and alerts focused on user activity monitoring

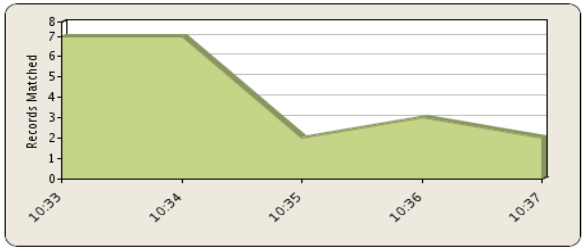
User Activity Monitoring (offense 2834 in the data set)

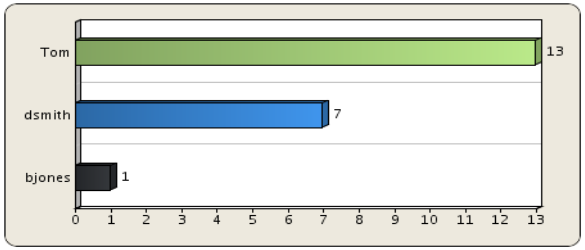
Offense 2834 Summary | Attackers | Targets | Categories | Annotations | Networks | Events | Flows | Rules | Actions ▼ | Print

Magnitude				**Relevance**	3	**Severity**	5	**Credibility**	3
Description	Single Host preceded by Login Failures Followed By Success preceded by Login failure to a disabled account. preceded by Authentication: Repeated Login Failures	**Event count**	36 events in 6 categories					
Attacker/Src	10.103.7.88 (dhcp-workstation-103-7-88.acme.org)	**Start**	2009-09-29 10:33:34					
Target(s)/Dest	10.101.3.10 (Windows AD Server)	**Duration**	4m 51s					
Network(s)	IT.Server.main	**Assigned to**	Not assigned					
Notes	Windows Authentication Use Case Demo data to demonstrate event-only Windows Authentication use case, including login failures, login attempt to disabled account, etc. This attack is comprised of : - Event(s): Multiple authentication attempts from ...							

Authentication Failures

Perhaps a user who forgot their password?





(Hide Charts)

	Username	Source IP (Unique Count)	Destination IP (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Category (Unique Count)	Event Count (Sum)	Count ▼
	Tom	10.103.7.88	10.101.3.10	Multiple (4)	WindowsAuthSe...	Multiple (4)	19	13
	dsmith	10.103.7.88	10.101.3.10	Multiple (4)	WindowsAuthSe...	Multiple (3)	7	7
	bjones	10.103.7.88	10.101.3.10	Logon Failure - ...	WindowsAuthSe...	Host Login Failed	1	1

Brute Force Password Attack

Numerous failed login attempts against different user accounts.

Event Name ▲	Log Source	Source IP	Destination IP
Host Login Succeeded - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Host Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Host Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Remote Access Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Remote Access Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Suspicious Pattern Detected - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Suspicious Pattern Detected - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10

Host Compromised

All this followed by a successful login.

Automatically detected, no custom tuning required.

Complex Threat Detection

Problem Statement

- Finding the single needle in the 'needle stack'
- Connecting patterns across many data silos and huge volumes of information
- Prioritizing attack severity against target value and relevance
- Understanding the impact of the threat

Required Visibility

- Normalized event data
- Asset knowledge
- Vulnerability context
- Network telemetry

Complex Threat Detection (offense 3063 in the data

Offense 3063 Summary | Attackers | Targets | Categories | Annotations | Networks | Events

Magnitude		**Relevance**	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan	**Event count**	1428 events in 3 cate
Attacker/Src	202.153.48.66	**Start**	2009-09-29 16:05:01
Target(s)/Dest	Local (717)	**Duration**	1m 32s
Network(s)	Multiple (3)	**Assigned to**	Not assigned
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with I China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250). The first s		

Sounds Nasty…

But how to we know this?

The evidence is a single click away.

Network Scan

Detected by QFlow

Buffer Overflow

Exploit attempt seen by Snort

	Event Name	Source IP	Destination IP	Destination Port	Log Source	Low Level Category
	Network Sweep - QRadar Classify Flow	202.153.48.66	Multiple (716)	445	Flow Classification E	Network Sweep
	NETBIOS-DG SMB v4 srvsvc NetrpPathConon	202.153.48.66	Multiple (8)	445	Snort @ 10.1.1.5	Buffer Overflow

Port	Service	OSVDB ID	Name	Description	Risk / Severity
445	unknown	49243	Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution	Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that the flaw may allow remote code execution resulting in a loss of integrity.	3

Targeted Host Vulnerable

Detected by Nessus

Total Visibility

Convergence of Network, Event and Vulnerability data.

Fraud and Data Loss Prevention

Problem Statement

- Malicious activity against 'targets of choice'
- Privileged or knowledgeable users internal to the network
- Fraud patterns that are 'low and slow' by nature
- Associating suspicious patterns across network, security, application and host layers in the infrastructure

Required Visibility

- Ability to take and normalize telemetry across many diverse sources
- Correlation of host and asset profiles with IAM infrastructure
- Integration of 3rd party intelligence sources

Data Loss and Fraud Detection (offense 2853 in

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 ...

Attacker Summary Details			
Magnitude		User	scott
Description	10.103.14.139	Asset Name	dhcp-workstation-103.14.139.acme.org
Vulnerabilities	0	MAC	Unknown
Location	NorthAmerica.all	Asset Weight	0

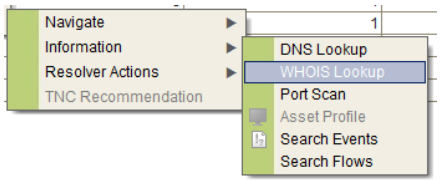
Who?

An internal user

	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

What?

Oracle data



QRadar Has Completed Your Request

Go to APNIC results

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

OrgName: Google Inc.
OrgID: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View

Where?

Gmail

Security Configuration Monitoring

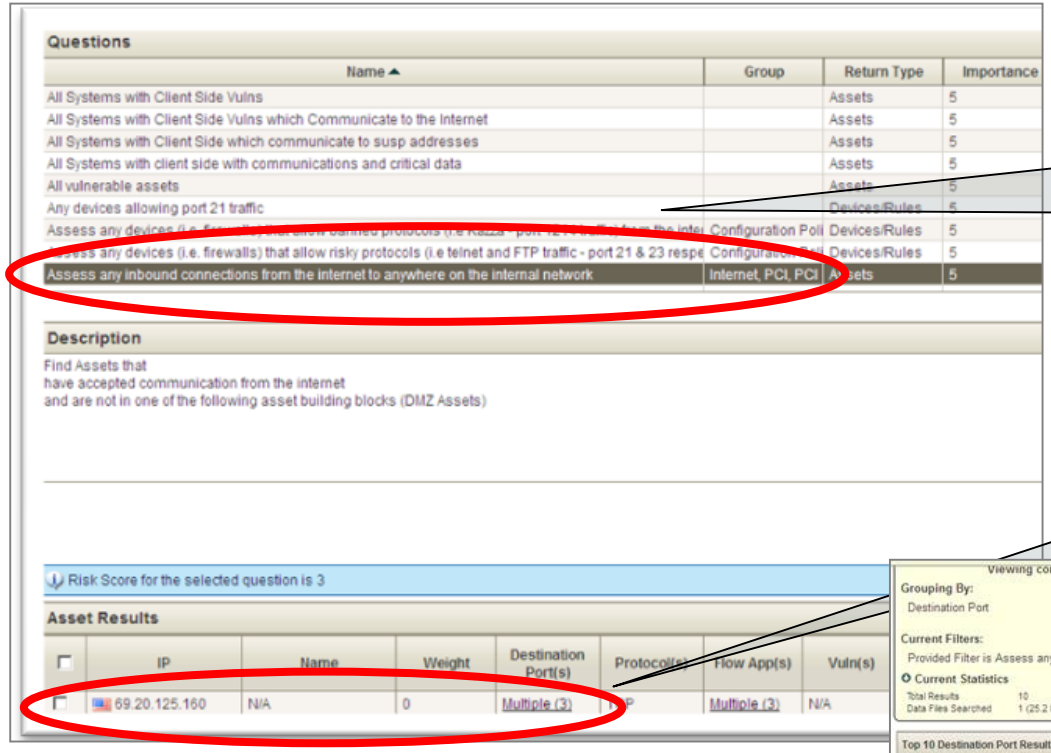
Challenges

- Identifying device misconfigurations that create gaping security holes
- Prioritizing security gaps by asset value and impact
- Investigating specific risks of concern to the business
- Continuously monitoring for new risks and remediating to prevent breaches

Required Capabilities

- Network flow collection with deep packet inspection
- Asset knowledge
- Vulnerability context
- Flexible querying & analysis
- Full workflow management

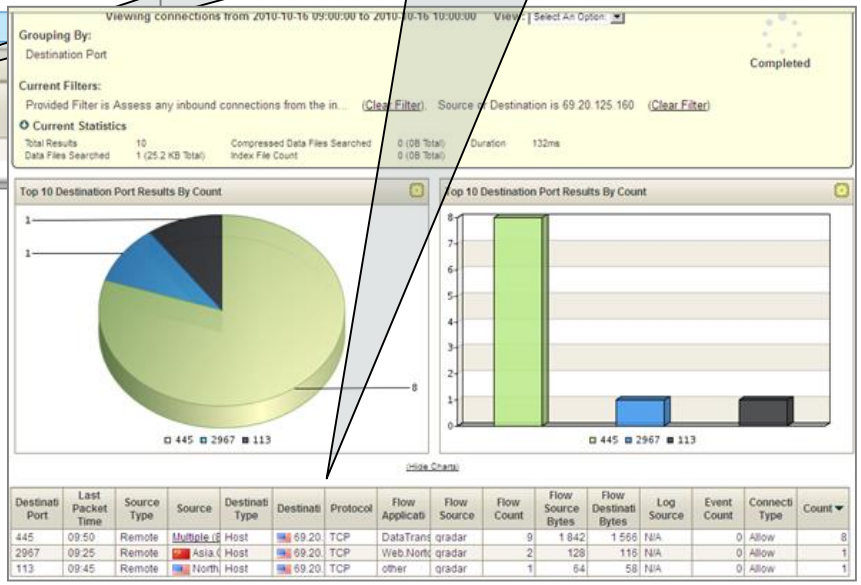
Security Configuration Monitoring



Find Devices with Risky Configuration Settings

Leverage knowledge of network traffic and vulnerabilities

Quickly Assess Risky Traffic and Drill Down

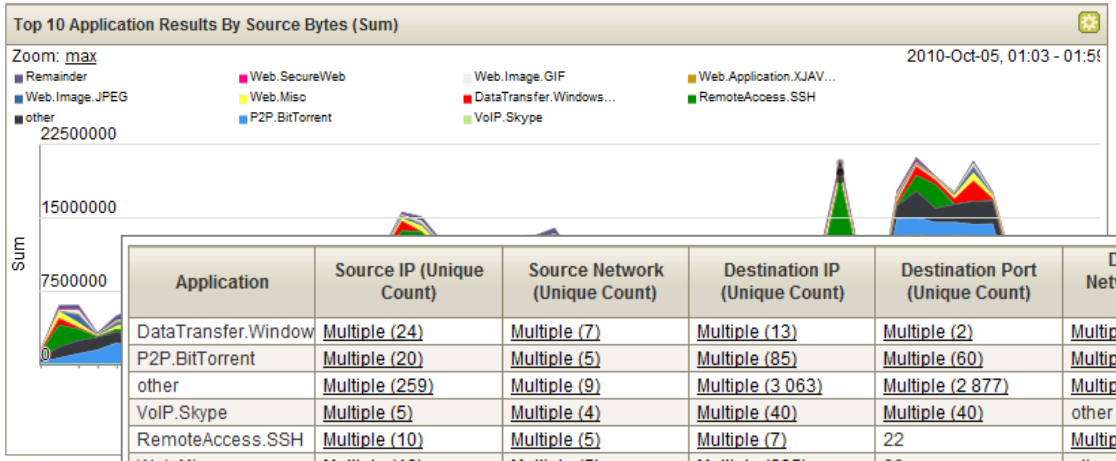


Find Gaps Before Your Adversaries Do

Continuous 360-degree visibility and monitoring

Flow Analytics & Network Anomaly Detection – Why

- **Network traffic doesn't lie.** Attackers can stop logging and erase their tracks, but can't cut off the network (flow data)
- Helps detect day-zero attacks that have no signature
- Detects anomalies that might otherwise get missed
- Provides definitive evidence of attack
- Enables visibility into all attacker communications



Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267
Web.Image.JPEG	Multiple (13)	Multiple (4)	Multiple (60)	80	other	2 418 857	18 538 204

Flow Analytics & Network Anomaly Detection – How

- Native flow collection from network infrastructure
- Deep packet inspection for Layer 7 data
- Full pivoting, drill-down and data mining on flow sources for advanced detection and forensic examination
- Anomaly detection: Identify by rule/policy, threshold, behavior or abnormal conditions across network (flow) and log activity

User Anomaly Detection (Activity Monitoring)

Challenges

- Monitoring of privileged and non-privileged users
- Isolating ‘Stupid user tricks’ from malicious account activity
- Associating users with machines and IP addresses
- Normalizing account and user information across diverse platforms

Required Capabilities

- Centralized logging and intelligent normalization
- Correlation of IAM information with machine and IP addresses
- Automated rules and alerts focused on user activity monitoring
- Behavior/activity baselining and anomaly detection

User Anomaly Detection (Activity Monitoring)

Rule Name	Group	Rule Category
Central American employee access from outside geography	IAM	Custom Rule
Contract Employee action followed by Privileged Employee actio...	IAM	Custom Rule
Privilege Escalation by Non-Privileged User	IAM	Custom Rule
Terminated Employee Access	IAM	Custom Rule
Contract Employee: Access to Sensitive Databases	IAM, Suspicious	Custom Rule

Integration with Identity & Access Management

Knowledge of user roles and group membership

Magnitude	
Description	Contract Employee action followed by Privileged Employee actions from the same Source IP
Source IP(s)	10.0.110.94
Destination IP(s)	Local (3)

Top 5 Users

Name	Events/Flows
SYSTEM	18
juanita_neubauer	5

Top 5 Categories

Name	Magnitude	Local Destination Count	Events/Flows
SSH Login Failed		1	1
SSH Login Succeeded		2	2
System Status		1	18
Privilege Escalation Succeeded		2	2
Remote Access		2	9

Top 10 Flows

Application	Source IP	Source Port
RemoteAccess.SSH	10.0.110.94	26216
RemoteAccess.SSH	10.0.110.94	26216
RemoteAccess.SSH	10.0.110.94	26216
RemoteAccess.SSH	10.0.110.94	26216
RemoteAccess.SSH	10.0.110.94	26216

Detect Suspicious Activity

Why is a privileged user taking action from a contractor's system?

Full Visibility at Your Fingertips

Users, Events, Flows – All Available for Drill-down

Reconnaissance Detection

Challenges

- Finding the single needle in the ‘needle stack’
- Connecting patterns across many data silos and huge volumes of information
- Prioritizing attack severity against target value and relevance
- Understanding the impact of the threat

Required Capabilities

- Normalized event data
- Flow collection with deep packet inspection
- Asset knowledge
- Vulnerability context
- Network telemetry

Reconnaissance Detection

Offense 3063 Summary | Attackers | Targets | Categories | Annotations | Networks | Events

Magnitude		Relevance	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan	Event count	1428 events in 3 cate
Attacker/Src	202.153.48.66	Start	2009-09-29 16:05:01
Target(s)/Dest	Local (717)	Duration	1m 32s
Network(s)	Multiple (3)	Assigned to	Not assigned
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with I China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250). The first s		

Sounds Nasty…

But how do we know this?

The evidence is just a single click away.

Network Scan

Detected by QFlow

Buffer Overflow

Exploit attempt seen by Snort

	Event Name	Source IP	Destination IP	Destination Port	Log Source	Low Level Category
	Network Sweep - QRadar Classify Flow	202.153.48.66	Multiple (716)	445	Flow Classification E	Network Sweep
	NETBIOS-DG SMB v4 srvsvc NetrpPathConon	202.153.48.66	Multiple (8)	445	Snort @ 10.1.1.5	Buffer Overflow

Port	Service	OSVDB ID	Name	Description	Risk / Severity
445	unknown	49243	Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution	Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that the flaw may allow remote code execution resulting in a loss of integrity.	3

Targeted Host Vulnerable

Detected by Nessus

Total Security Intelligence

Convergence of Network, Event and Vulnerability data

Stealthy Malware Detection

Challenges

- Distributed infrastructure
- Security blind spots in the network
- Malicious activity that promiscuously seeks ‘targets of opportunity’
- Application layer threats and vulnerabilities
- Siloed security telemetry
- Incomplete forensics

Required Capabilities

- Distributed detection sensors
- Pervasive visibility across enterprise
- Application layer knowledge (via Layer 7 flows)
- Content capture for impact analysis (Layer 7 flows)

Stealthy Malware Detection

Offense 2849 Summary | Attackers | Targets | Categories | Annotations | Networks | Events | Flows | Rules | Actions | Print

View flows for this offense

Magnitude		Relevance	3
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...		

Potential Botnet Detected?

This is as far as traditional SIEM can go.

First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Co	Source Flags	Destinat Flags	Source QoS	Destinat QoS	Flow Sourc
11:19	tcp_ip	10.103.6.6	48667	62.64.54.11	80	IRC	N/A	S,P,A	F,S,P,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	50296	192.106.224.13	80	IRC	N/A	S,P,A	S,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	51451	62.181.209.201	80	IRC	N/A	S,P,A	F,S,P,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	47961	62.211.73.232	80	IRC	N/A	F,S,P,A	F,S,P,A	Best Effor	Class 1	qradar

IRC on port 80?

QFlow detects a covert channel, using Layer 7 flows and deep packet inspection

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 :VERSION xchaNOTICE Defender :VERSION x
JOIN #botnet_command_channel
JOIN #botnet_command_channel
```

Destination Payload
70 packets,
5996 bytes

UTF | Hex | Base64

```
:Lexington.KY.US.AccessIRC.Net:Lexington.KY.US.AccessIRC.Net:
```

Irrefutable Botnet Communication

Layer 7 flow data shows botnet command and control instructions

Database Monitoring

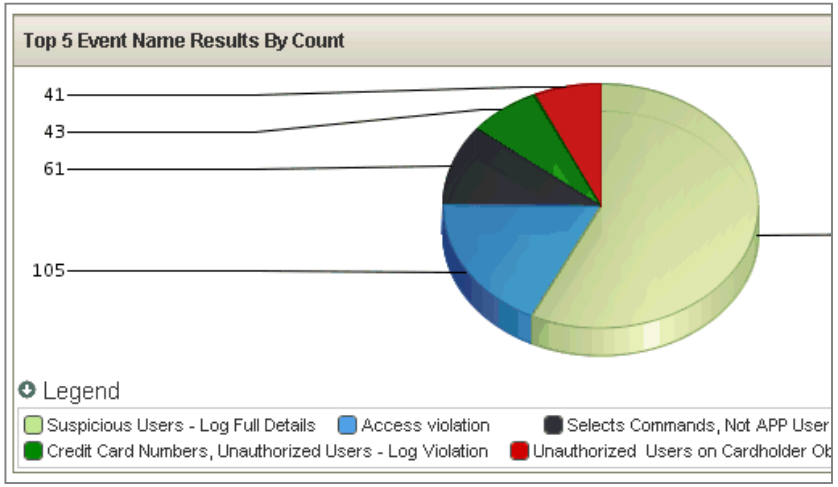
Challenges

- ‘Chameleons’: Patient attackers whose activity blends in with the environment
- Accurately identifying breaches with only partial information
- Analyzing data over long time periods
- Distinguishing attacks from abnormal but innocent activity
- Incomplete forensics

Required Capabilities

- Activity baselining and anomaly detection
- Correlation of data access with other network activity
- Content capture for threat determination (Layer 7 flows)

Database Monitoring



Visualize Data Risks

Automated charting and reporting on potential database breaches

Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Log Source
Suspicious Users - Log Full Details	10.10.9.56	10.10.9.56	Guardium @ g8
Access violation	10.10.9.56	10.10.9.56	Guardium @ g8
Selects Commands, Not APP User, Cardholder Objects -	10.10.9.56	10.10.9.56	Guardium @ g8
Credit Card Numbers, Unauthorized Users - Log Violation	10.10.9.56	10.10.9.56	Guardium @ g8
Unauthorized Users on Cardholder Objects - Alert	10.10.9.56	10.10.9.56	Guardium @ g8
Suspicious Users, Cardholder Objects - Log Info	10.10.9.56	10.10.9.56	Guardium @ g8

Correlate Database and Other Network Activity

Enrich database security alerts with anomaly detection and flow analysis

Event Name	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)
Suspicious Users - Log Full Details	Suspicious Activity	other	Multiple (4)
Access violation	Access Denied	other	SYSTEM
Selects Commands, Not APP User, Cardholder Objects -	nformation	other	Multiple (2)
Credit Card Numbers, Unauthorized Users - Log Violation	Unauthorized Access	other	system
Unauthorized Users on Cardholder Objects - Alert	Unauthorized Access	other	system
Suspicious Users, Cardholder Objects - Log Info	Suspicious Activity	other	system
SQL Error - Log	Error	other	Multiple (2)
Failed Login - Log Violation	General Authentication	other	Multiple (3)
Failed Login - Alert if repeated	General Authentication	other	Multiple (2)

Better Detect Serious Breaches

360-degree visibility helps distinguish true breaches from benign activity, in real-time

Fraud attack methods evolve quickly

Man-in-the Browser Malware

Malware injection of these fields created by criminals

Criminals

Fraud attack methods evolve quickly

Man-in-the Browser Malware

Fake fields created by criminals appear as bank request fields

Zeus BabyBerta

Malware injection of Personally Identifiable Information (PII) fields

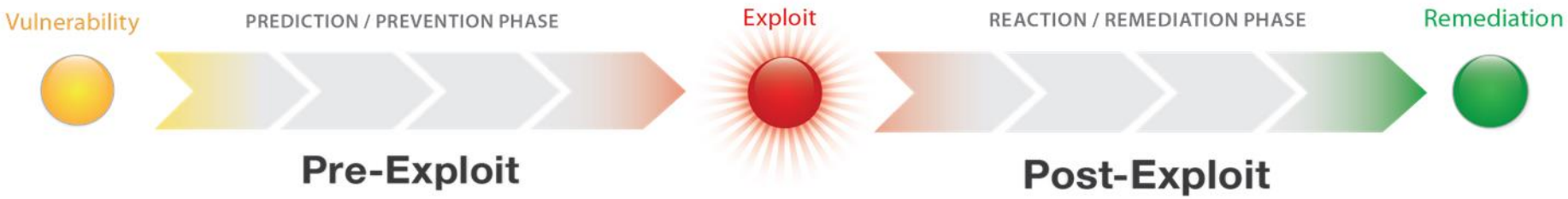
Citadel

Criminals

Fraud attack methods evolve quickly

Addressing full Security Intelligence Timeline

What are the external and internal threats? → Are we configured to protect against these threats? → What is happening right now? → What was the impact?



Pre-Exploit

Prediction & Prevention

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

Post-Exploit

Reaction & Remediation

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

1Labs®
Total Security Intelligence | An IBM Company

What Capabilities Can Help Protect Against Insider Threat ?

- 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

Can You Prevent An Insider Threat

Four key measures—

1. Whitelisting - (i.e., allowing only authorized software to run on a computer or network),
2. Very rapid patching of applications
3. Very rapid patching operating system vulnerabilities,
4. Restricting the number of people with administrator access to a system

85% of targeted intrusions can be prevented.

4. The Framework for Insider Threat Detection & Remediation

Risk Assessment

Risk Mitigation

Network Visibility

Discover All Wired & Wireless Infrastructure

Device Profiling

Detect and Classify Every Endpoint Device

Easy Onboarding

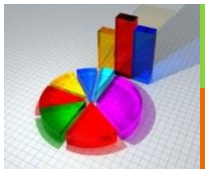
Simple and Powerful Device and User Onboarding

Endpoint Compliance

Pre-Connect Risk Assessment of Endpoint Devices

Network Provisioning

Safe Network Access Assignment



Analytics

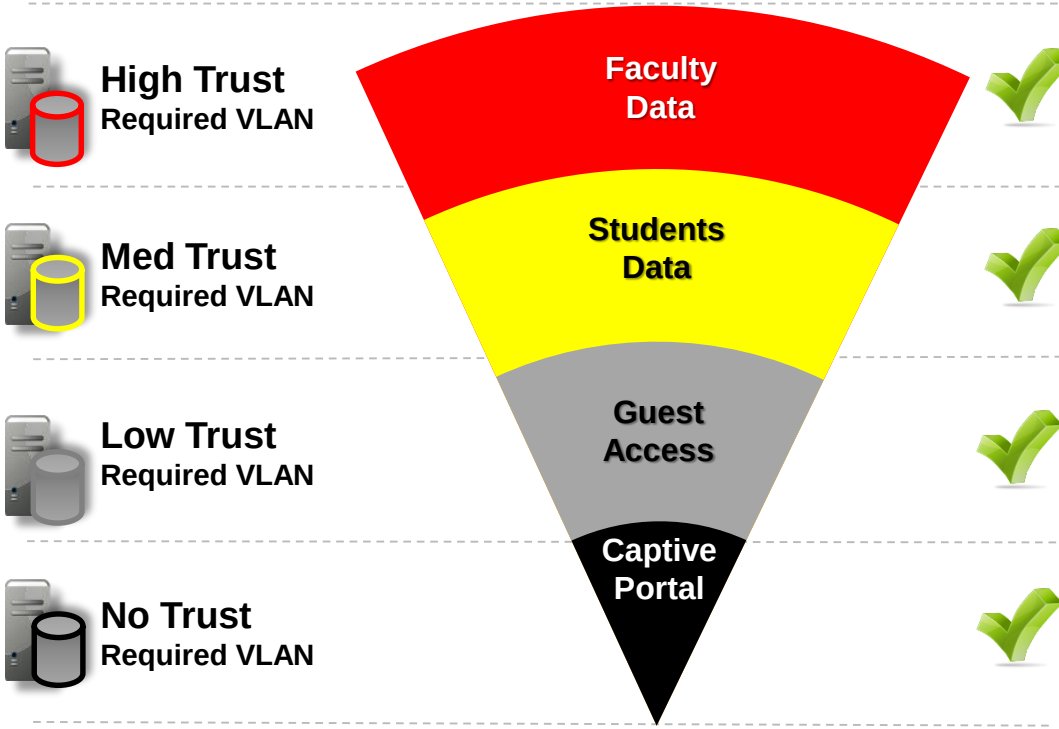
Historical Event Correlation and Trending

SmartEdge Platform Integrations

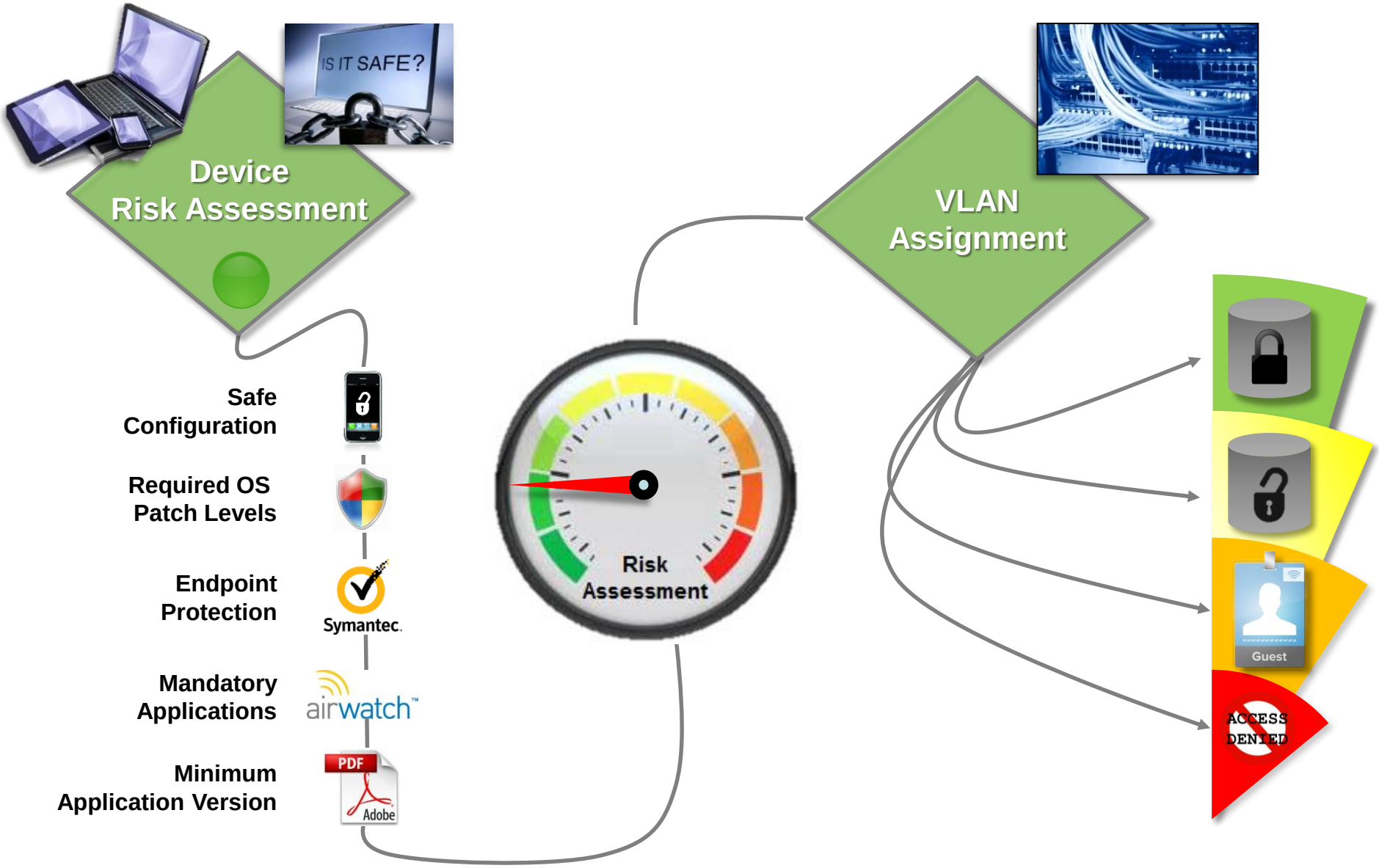
- Security
- Mobility
- Wired & Wireless

Safe Policy-Based Network Access

Single
Mgmt Appliance



Endpoint Compliance



Restricting Privilege Access – From Tin to Twitter

Server, Desktop & Network OS

- Administrator, Domain/Local
- Root, Super user, Admin, …

Databases (DBA + Apps)

- SA, Sysadmin
- SYS, …

Middleware

- Proxy Accounts
- Gateway Accounts, …

Mainframes

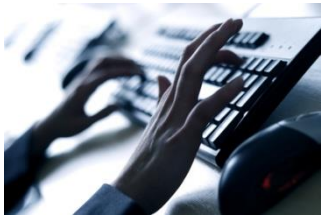
- UID=0, Line-of-business
- RACF Special, …

Applications

- Setup, Admin, App Local
- Web Service Accounts, …

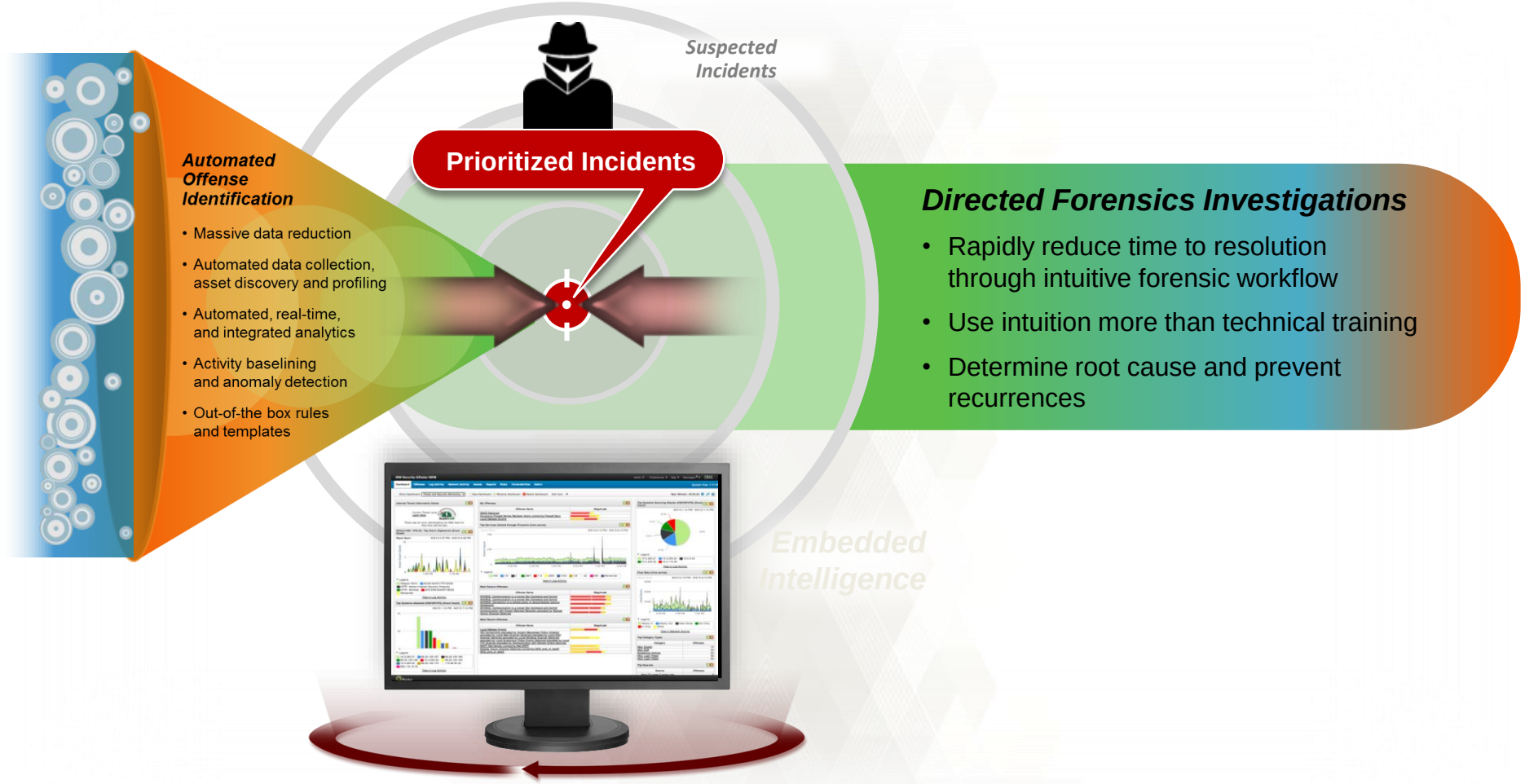
VM Environments

- Administrator
- Root





Extend clarity around incidents with in-depth forensics data



How network forensics is done

Full Packet Capture

- Capture packets off the network
- Include other, related structured and unstructured content stored within the network

Retrieval & Session Reconstruction

- For a selected security incident, retrieve all the packets (time bounded)
- Re-assemble into searchable documents including full payload displayed in original form

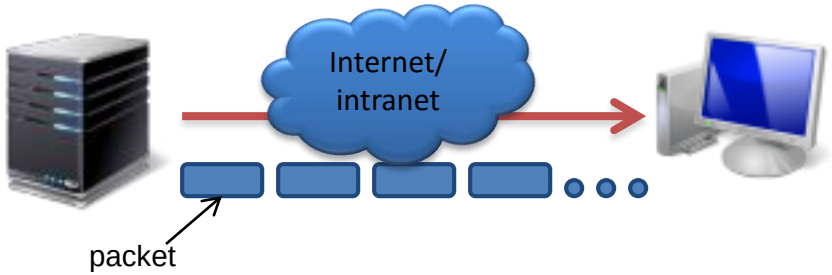
Forensics Activity

- Navigate to uncover knowledge of threats
- Switch search criteria to see hidden relationships

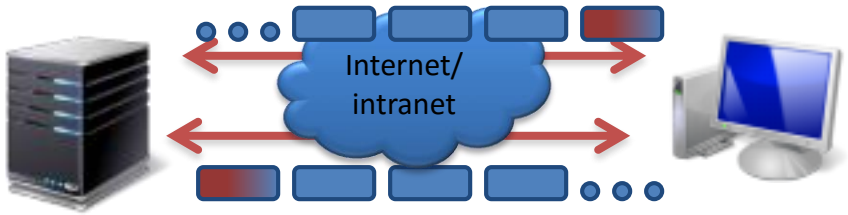
How Network Forensics is Works -

1	**Extension of Security Intelligence Platform**	• Built off high accuracy QRadar offense discovery • Improve efficiency of investigations
2	**Expands Data Available for Incident Forensics**	• Data-in-motion and data-at-rest • Structured and unstructured data
3	**Has Scalable Search Infrastructure**	• Index all the data • Correlate all the data • Prioritize search performance
4	**Builds Intelligence**	• Automated identification and assembly of identities • Automated distilling of suspicious content/activity • Content categorization informs data exclusion • Reveals linkages between entities
5	**Enables Intuitive Investigative Analysis**	• Simple search engine interface • Visual analytics • Retrace activity in chronological order with reconstructed content

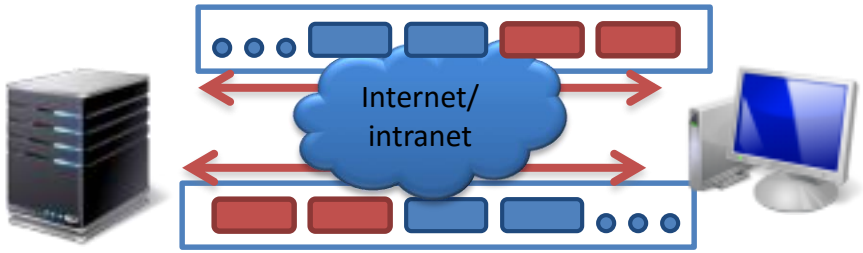
From NetFlow to QFlow to… …



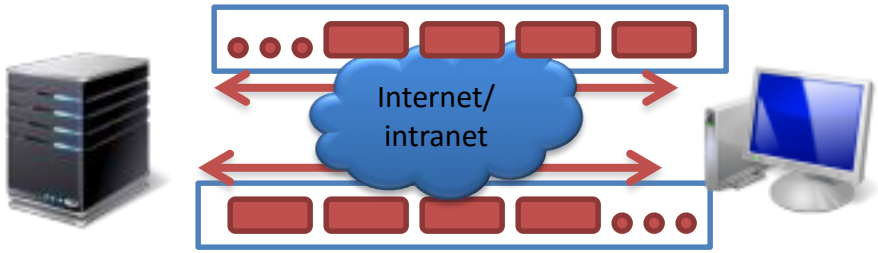
Netflow: packet oriented, identifies unidirectional sequences sharing source and destination IPs, ports, and type of service



QFlow: packet oriented, identifies bi-directional sequences aggregated into sessions, also identifies applications by capturing the beginning of a flow.



Competitive solutions: session oriented, some only capture a subset of each flow and index only the metadata—not the payload.



QRadar Incident Forensics: session oriented, captures all packets in a flow indexing the metadata and payload to enable fast search driven data exploration

Changing the dynamics of network forensics activities

Incident Forensics helps simplify the task, accelerate results, and ensure better results

Before

- Performed by technically trained forensics researchers
- Hunt for anomalous activities within specified time frame
- Identify threat actor and remediate malicious conditions

After

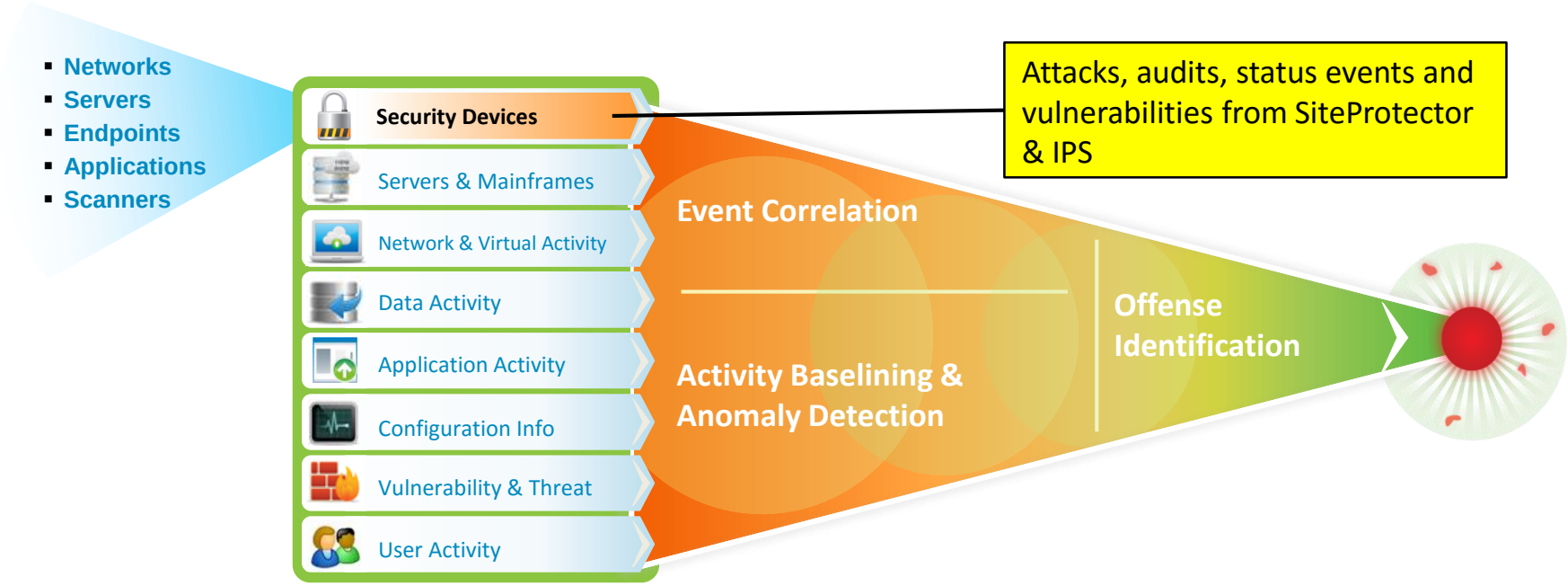
- Initiated using intuition with Internet search engine simplicity
- Follow security analytics or threat intelligence feed directives
- Retrace step-by-step movements for complete clarity

Benefit

- Address skills gap for forensics analysis
- Win race against time finding true threats and halting data loss
- Determine root cause and prevent breach recurrences

Improve your visibility and prevention against

THREAT PROTECTION



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

- Helps find threats other SIEMs might miss by combining Network Protection's Protocol Analysis Module signature analysis and QRadar's anomaly detection capabilities
- Enables immediate real-time threat awareness and powerful threat and offense prioritization capabilities to establish definitive evidence of attack and visibility into all attacker communications
- Integrates X-Force security content
- Outstanding coverage available within full SIEM solution or targeted Network Anomaly Detection offering

Clear, concise and comprehensive delivery of relevant info

Offense 3063 — Summary | Attackers | Targets | Categories | Annotations | Networks | Events | Flows | Rules | Actions | Print

Magnitude				Relevance	0	Severity	8	Credibility	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan		Event count	1428 events in 3 categories					
Attacker/Src	202.153.48.66		Start	2009-09-29 16:05:01					
Target(s)/Dest	Local (717)		Duration	1m 32s					
Network(s)	Multiple (3)		Assigned to	Not assigned					
Notes	Vulnerability Correlation Use Case Illustr… n of vulnerability data with IDS alerts An attacker originating from China (202… ng the Conficker worm exploit (CVE 2008-4250).								

What was the attack?

Was it successful?

Who was responsible?

Attacker Summary Details

Magnitude		User	Karen
Description	202.153.48.66	Asset Name	Unknown
Vulnerabilities	0	MAC	Unknown
Location	China	Asset Weight	0

Where do I find them?

Top 5 Categories Categories

Name	Magnitude	Local Target Count	
Buffer Overflow		8	
Misc Exploit		3	3
Network Sweep		716	1417

How many targets involved?

How valuable are the targets to the business?

Top 5 Local Targets Targets

IP/DNS Name	Ma…		Chained	User	MAC	Location	Weight
Windows AD Server				Unknown	Unknown	main	8
10.101.3.3		Unknown	No	Unknown	Unknown	main	0
10.101.3.4		Unknown	No	Unk…		main	0
DC106		Yes	No	Adn…		main	10
10.101.3.11		Unknown	No	DC…		main	0

Are any of them vulnerable?

Top 10 Events Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm	Misc Exploit	10.101.3.15	445	09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrpPathCo…		Snort @ 10.1.1.5	Buffer Overflow	10.101.3.10	445	09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrpPathCo…		Snort @ 10.1.1.5		10.101.3.15	445	09-29 16:06:33
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-v…		10.101.3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qr…		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qr…		10.101.3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qr…		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01

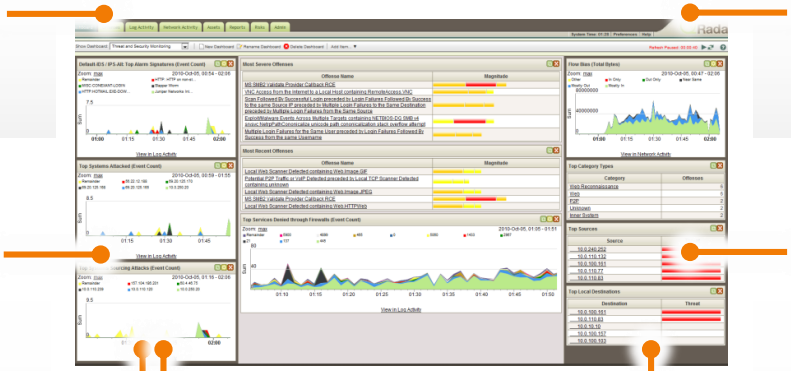
Where is all the evidence?

NG Multi Layered Security Framework

*Integrated **automated** capabilities delivered across a comprehensive security framework*

Detect, analyze, and prioritize threats	QRadar
Reduce fraud and malware	Trusteer
Manage users and their access	Identity and Access Management
Discover and harden valuable assets	InfoSphere Guardium
Secure critical business applications	AppScan
Protect infrastructure against attacks	Network and Endpoint Protection
Monitor and evaluate today's threats	IBM X-Force

All domains feed Security Intelligence

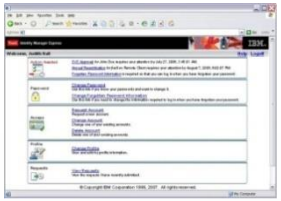


Correlate new threats based on X-Force IP reputation feeds

Hundreds of 3rd party information sources

Guardium

Database assets, rule logic and database activity information



Identity and Access Management

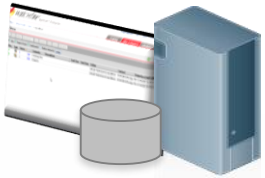
Identity context for all security domains w/ QRadar as the dashboard

Tivoli Endpoint Manager

Endpoint Management vulnerabilities enrich QRadar's vulnerability database

IBM Security Network Intrusion Prevention System

Flow data into QRadar turns NIPS devices into activity sensors



AppScan Enterprise

AppScan vulnerability results feed QRadar SIEM for improved asset risk assessment

Q: Why, given the variety of security technologies typically in place, do information assets remain at significant risk?

A: Traditional methods fail to capture and alert on a complete trail of information. With fraud detection software, you can solve this problem.

5 THINGS TO THINK ABOUT

1. When funds are gone, it's too late
2. Logs never tell the complete story
3. Focus on analysis, not just alerts.
4. Outdated methods waste time and money.
5. If you could find a way to "see" fraud before it starts, wouldn't you want to?

Questions?