Q1 Labs

Total Security Intelligence

True in Depth Security through Next Generation SIEM

Ray Menard
Senior Principal Security Consultant
Q1 Labs

Q1Labs.com

Q1 Labs
Total Security Intelligence

"Electronic intelligence, valuable though it is in its own way, serves to augment the daunting volume of information which is directed at headquarters from satellite and aerial reconnaissance, intelligence-gathering ships, optical observation, special forces, armoured reconnaissance teams, and the interrogation of prisoners. Nowadays the commander is confronted with too much information, rather than too little, and it is his informed judgment which ultimately decides what is relevant and important." [NATO, The Warsaw Pact and the Superpowers, 2° ed. p. 33

Hugh Farringdon

Q1 Labs
Total Security Intelligence

"Network and security information, valuable though it is in its own way, serves to augment the daunting volume of information which is directed at network and security practitioners from firewalls and IDS/IPS, sever logs, application logs, syslog servers, proxy servers and virus scanners. Nowadays the security practitioner is confronted with too much information, rather than too little, and it is his informed judgment which ultimately decides what is relevant and important."

Ray Menard plagiarized from Hugh Farringdon

Q1 Labs
Total Security Intelligence

Focus on Prevention

- Network and security professionals focus tends to be on preventing bad things from happening on the network.
- Gartner reported worldwide security software market revenue totaled 13.5 billion in 2008
- There is a significant amount of spending on tools designed to prevent bad things from getting in the network
- When things go bad, it is because the network and security practitioner doesn't know what they don't know.

Q1 Labs
Total Security Intelligence

Prevention is not enough

"This principle doesn't mean you should abandon your prevention efforts. As a necessary ingredient of the security process, it is always preferable to prevent intrusions than to recover from them. Unfortunately, no security professional maintains a 1.000 batting average against intruders. Prevention is a necessary but not sufficient component of security."

(Bejtlich, 2004)

Q1 Labs
Total Security Intelligence

Compliance Violations and Data Loss

- Story of two Universities
  - A: An old time QRadar Customer
  - B: QRadar not deployed, at least at the time
- University A
  - Host is compromised and detected by security administrator.
  - Host is identified as a critical system in accounting with student personal information
  - Flows were used to track all data sent two and from the host during the compromise and proved the only data the was transferred was not personal information but was copyright material uploaded by attacker
  - Host was cleaned up and no one outside was ever notified
- University B
  - Host is compromised and detected at some point after the attack
  - Host contains personal information
  - It cannot be proved what was removed so the university had to notify students of the possible loss of privacy and setup a call center to answer questions … this cost a serious amount of money.

Q1 Labs
Total Security Intelligence

"In the future everyone will be world-famous for fifteen minutes“

Andy Warhol

Q1 Labs
Total Security Intelligence

Moving Towards Solution

Network and security professionals need:

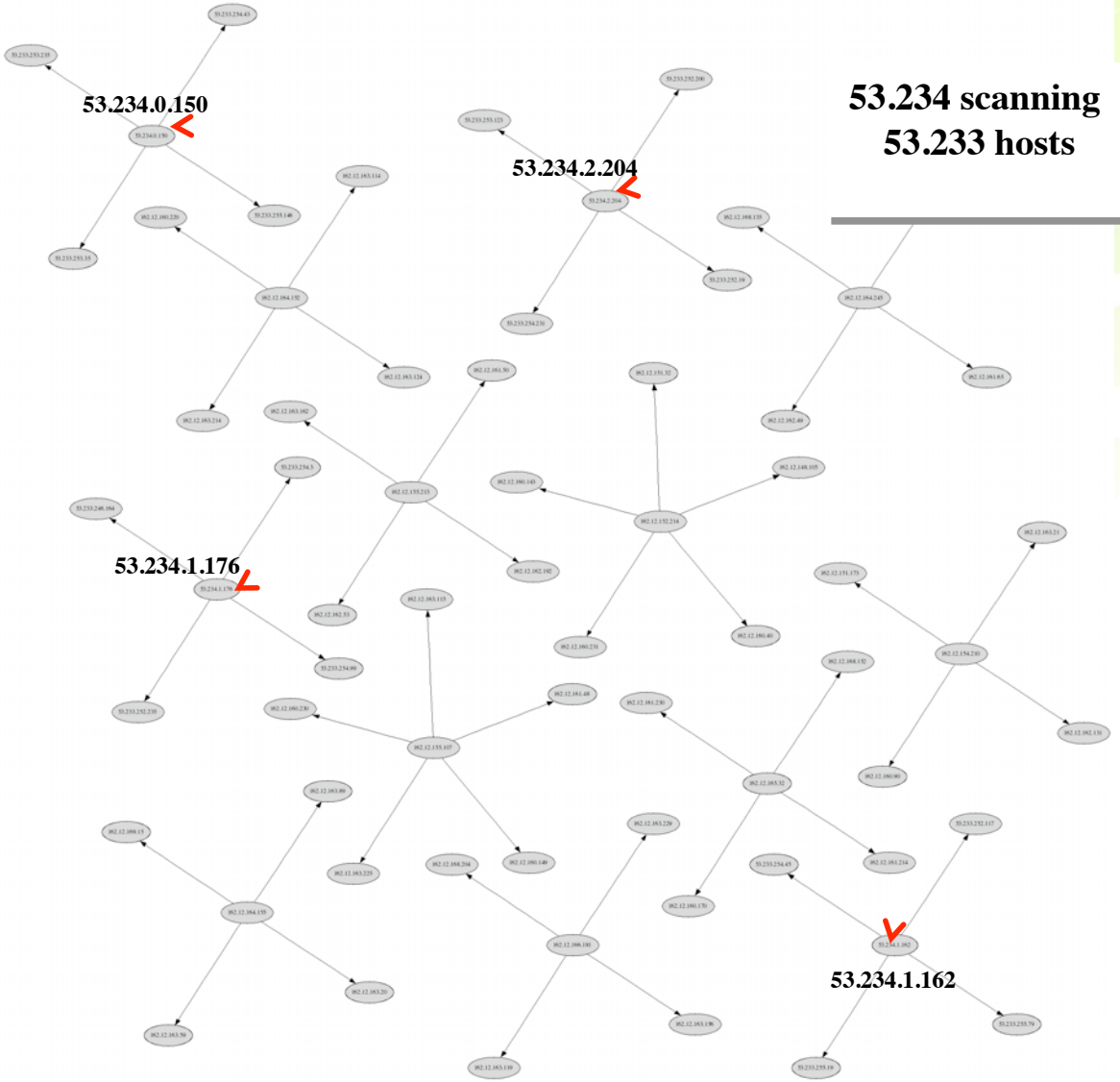
- Complete Network and Security Intelligence
- Ability to quickly and efficiently analyze large volumes of information, sorting the wheat from the chaff
- Flexibility to meet the ever changing more sophisticated threat
- Ability to do more with less as new requirements are identified
- Visibility and verification
- Time is an enemy!

Q1 Labs
Total Security Intelligence

Customer blocked from Google…

- Customer is blocked trying to get to Google and all requests are asking for a validation before a search is completed
- Reason appears to be someone on customer site running an excessive number of requests to Google
- Flow data quickly identifies the offending system with a simple flow search.. Customer had been searching for hours

100 Seconds into Attack



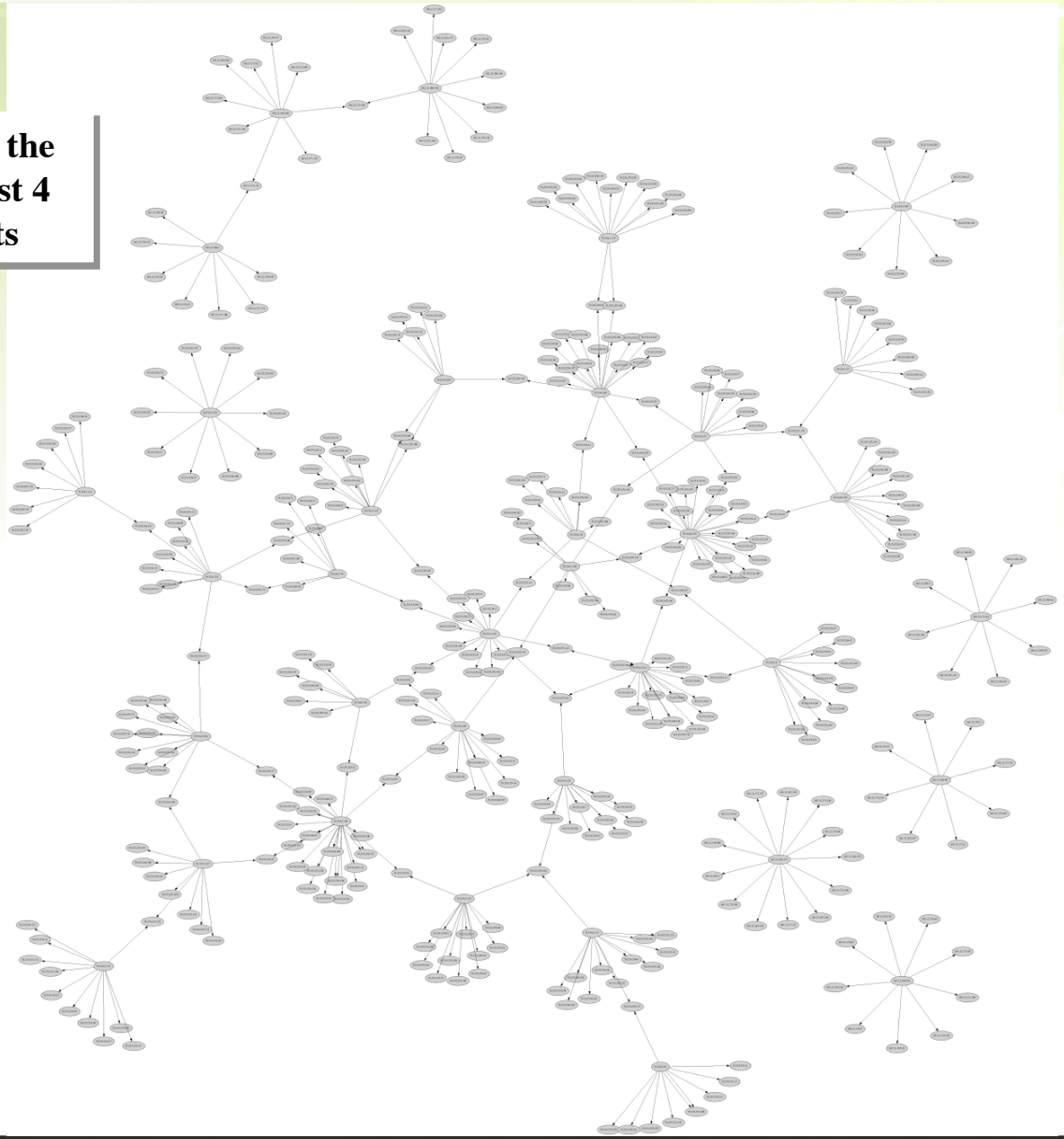
53.234 scanning
53.233 hosts

First hosts in 162.12_network to start scanning

- 162.12.152.214
- 162.12.154.210
- 162.12.155.107
- 162.12.155.213
- 162.12.164.152
- 162.12.164.155
- 162.12.162.245
- 162.12.165.32
- 162.12.166.181

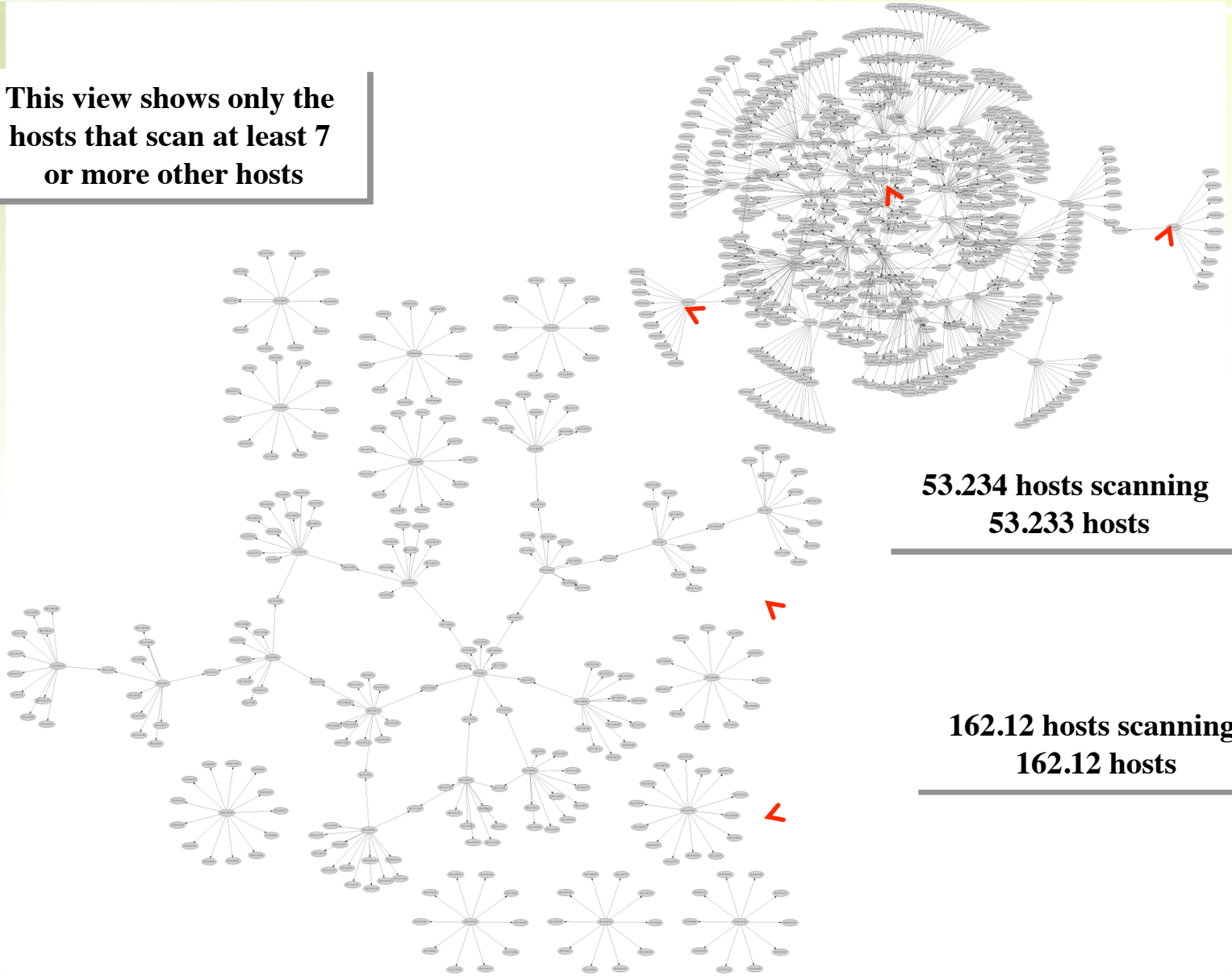
200 Seconds into Attack

This view shows only the hosts that scan at least 4 or more other hosts



300 Seconds into Attack

This view shows only the hosts that scan at least 7 or more other hosts

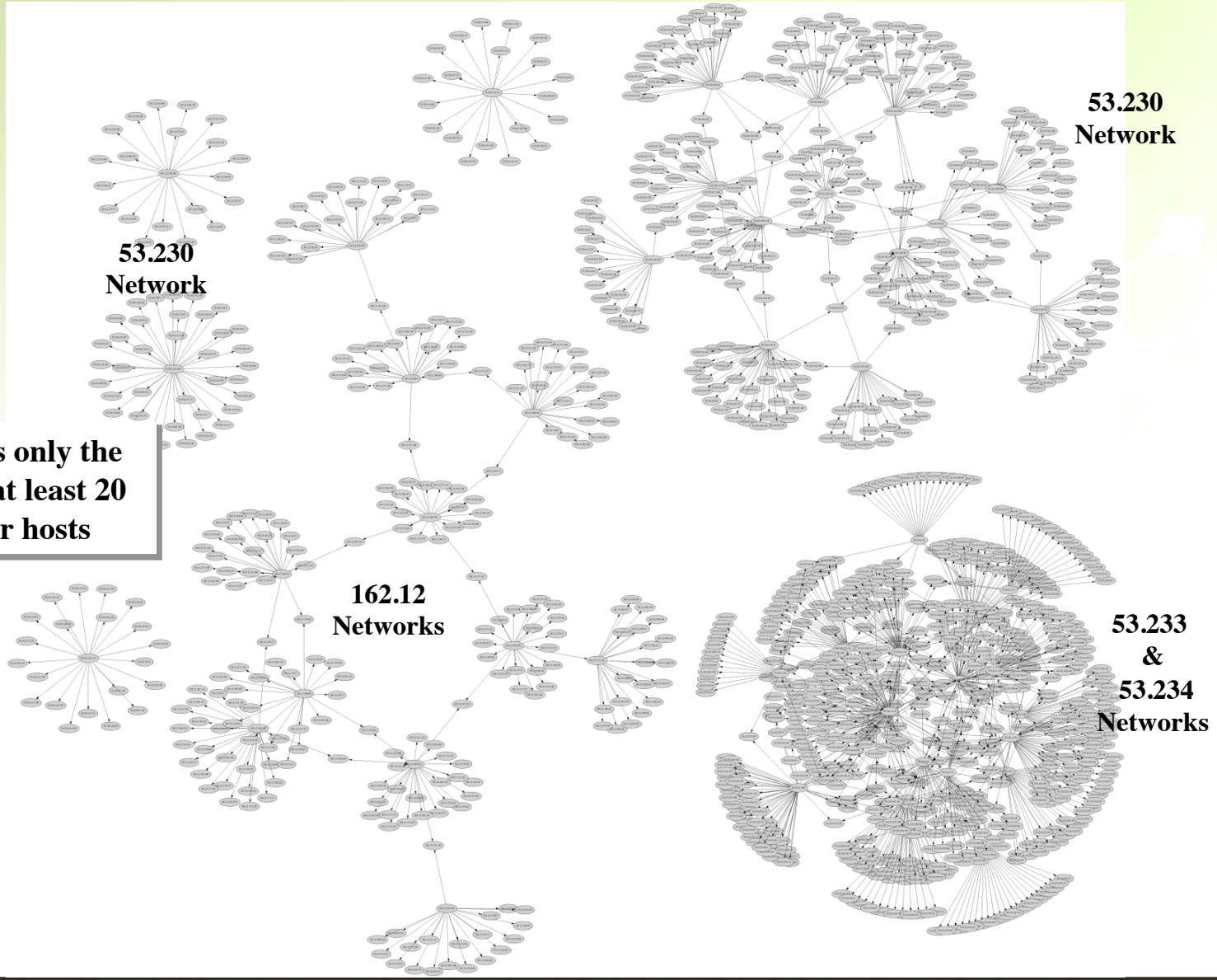


53.234 hosts scanning 53.233 hosts

162.12 hosts scanning 162.12 hosts

Q1 Labs
Total Security Intelligence

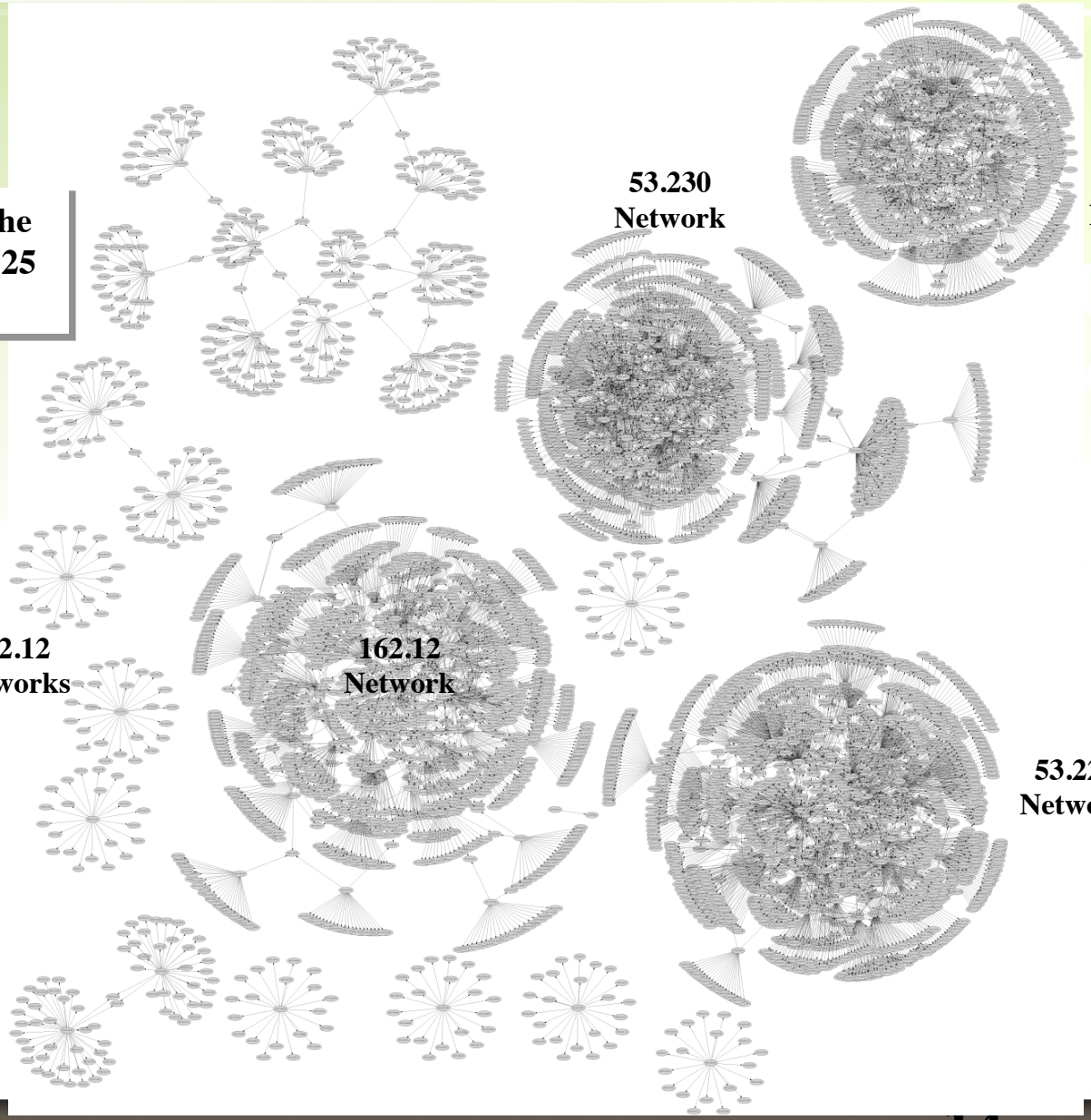
1 Hour into Attack



This view shows only the hosts that scan at least 20 or more other hosts

2 ½ Hours into Attack

This view shows only the hosts that scan at least 25 or more other hosts



Q1 Labs
Total Security Intelligence

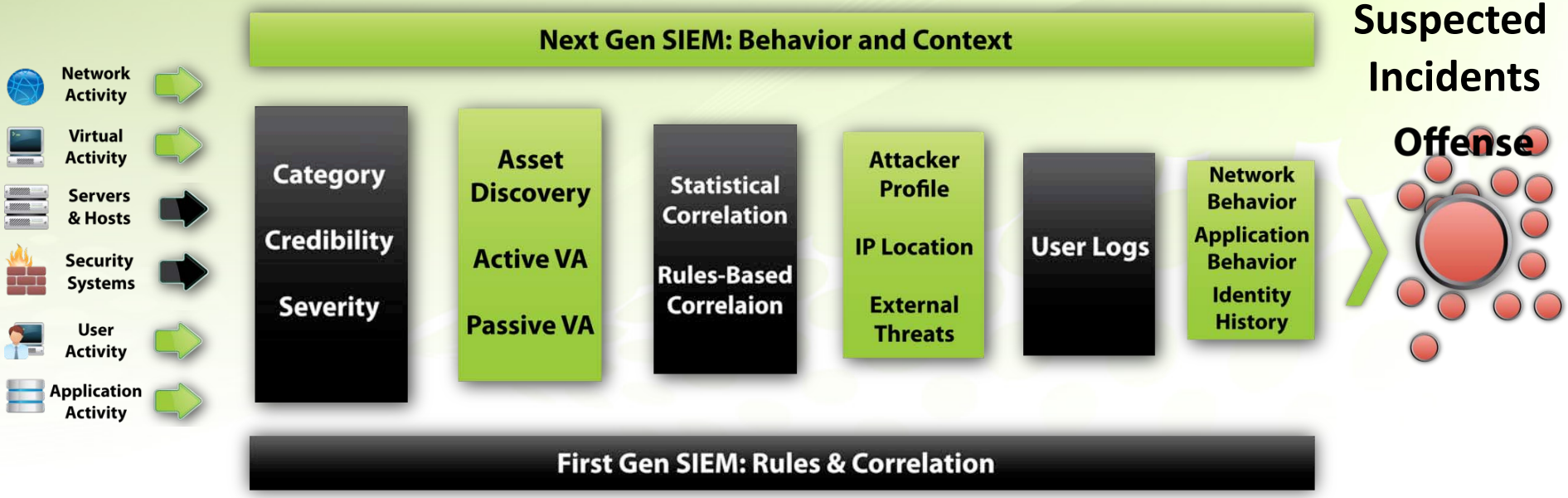
Restating The Problem

"One of the reasons why the state of information security is so bad is that it is built on a foundation of islands of point tools for protection against tactical threats. Managing these systems is an operational nightmare. What's more, most of these tools aren't integrated together, so getting a true picture of the security posture of the whole business is next to impossible, which may actually lead to additional security risks."

Jon Oltsik ESG

Q1 Labs
Total Security Intelligence

Next-Generation SIEM: Total Intelligence



Threats and Fraud Detected That Others Miss

User correlation and application forensics enabled fraud detection prior to exploit completion

Liz claiborne

Massive Data Reduction

2Bn log and event records a day reduced to 25 high priority

Chevron

Q1 Labs
Total Security Intelligence

Detecting the undetectable

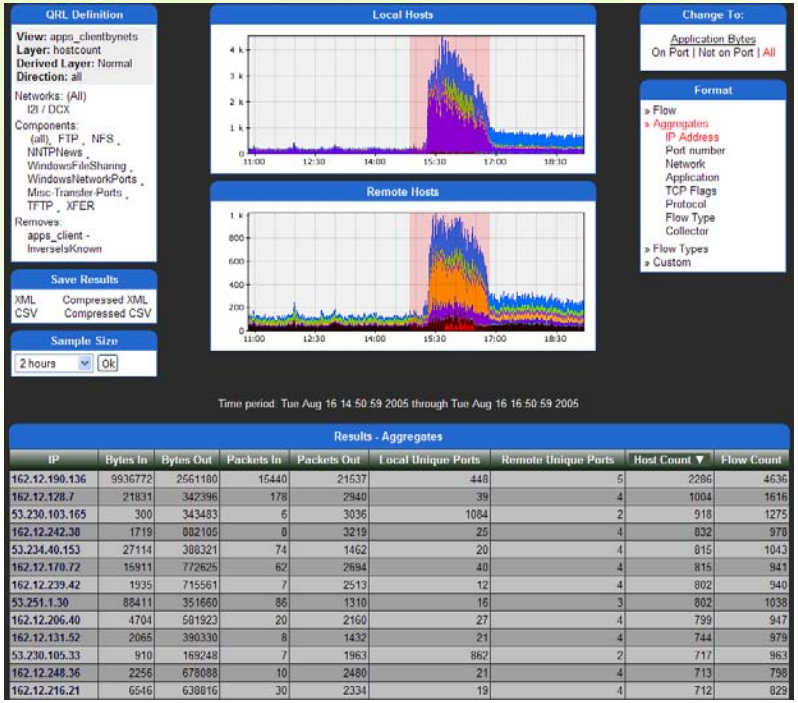
- QRadar has lots of rules that detect the infection and propagation of malware, worms, bots and issue dejour
- However, Sometime as many security measure as you put in place a host gets quietly compromised and goes undetected...
- Customer Eval: 3 hosts out of 80K+ make a web request to single address and transfer a 112 byte .gif image a couple of times a day.
- Those hosts make no other connections to any hosts even close to those and at some points in time, don't even appear to be in use during the request
- The 3 systems all have Anti-Virus/Anti-Malware which claim they are clean
- The host in question (where the.gif is downloaded from) is a know BOT Control Channel (as identified by QRadar's auto-update)
- Eval customer is aggressive and re-images the hosts...

Activity goes away....

Customer Proof Point

Large Auto Manufacturer –

Detected a worm outbreak affecting their production facility during evaluation using only flow data. This worm was not detected by exsiting signature based sources



IP	Bytes In	Bytes Out	Packets In	Packets Out	Local Unique Ports	Remote Unique Ports	Host Count ▼	Flow Count
162.12.190.136	9936772	2561180	15440	21537	448	5	2286	4636
162.12.128.7	21831	342396	178	2940	39	4	1004	1616
53.230.103.165	300	343483	6	3036	1084	2	918	1275
162.12.242.30	1719	882105	8	3219	25	4	832	970
53.234.40.153	27114	388321	74	1462	20	4	815	1043
162.12.170.72	15911	772625	62	2694	40	4	815	941
162.12.239.42	1935	715561	7	2513	12	4	802	940
53.251.1.30	88411	351660	86	1310	16	3	802	1038
162.12.206.40	4704	581923	20	2160	27	4	799	947
162.12.131.52	2065	390330	8	1432	21	4	744	979
53.230.105.33	910	169248	7	1963	862	2	717	963
162.12.248.36	2256	678088	10	2480	21	4	713	798
162.12.216.21	6546	630816	30	2334	19	4	712	829

53.229.21.68	0	53716	0	1033	632	1	422	690
53.229.21.105	0	62504	0	1202	705	1	421	765
53.230.105.225	0	116773	0	1256	524	2	419	556
53.229.23.165	0	54819	0	1041	638	3	412	682
53.234.0.150	0	53975	0	980	630	1	409	685
53.230.17.36	7948	165803	37	622	13	4	408	490
53.234.1.188	3600	160910	20	623	18	4	400	474
53.229.21.252	0	64064	0	1232	754	1	399	817
53.234.40.26	60434	155564	53	598	14	3	393	467
53.229.23.71	0	57616	0	1108	641	1	383	676
53.229.26.48	0	50960	0	980	642	1	383	683

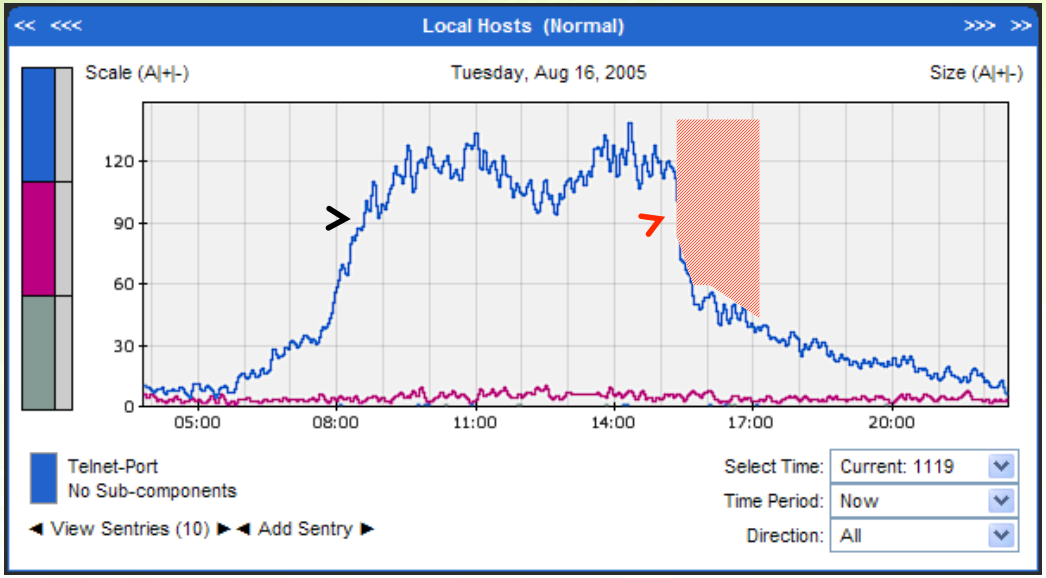
Showing 1 to 50 of 70850 ►►►

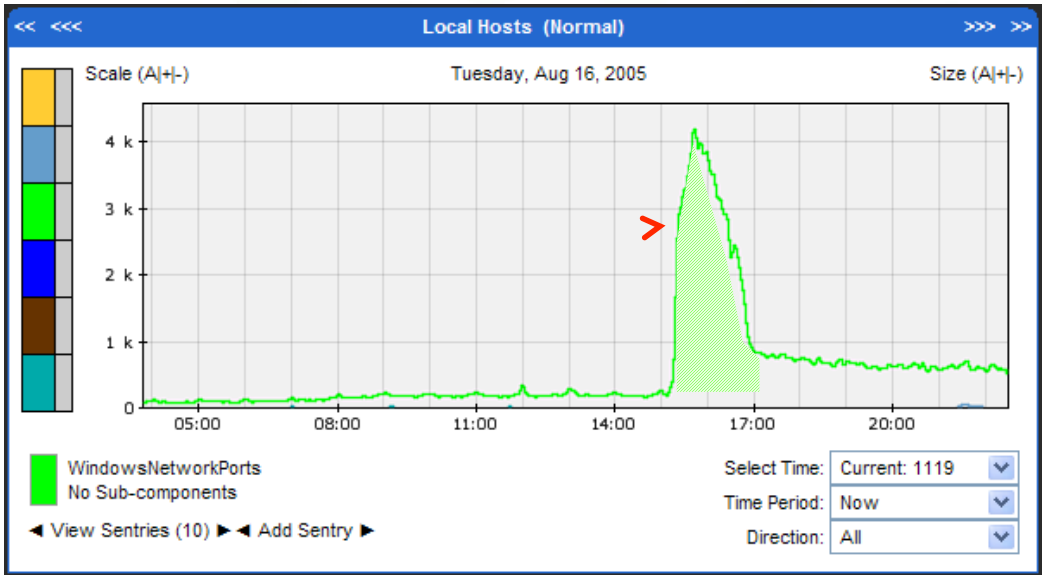
Impact on Applications

Telnet sessions prior to attack

Telnet sessions on local hosts going down during attack

Worm outbreak using Windows Network Ports to launch attack





QRadar Offense Management

Clear & concise delivery of the most relevant information …

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 Illustra … on 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	8
Misc Exploit		3	3
Network Sweep		716	1417

How many targets involved?

How valuable are they to the business?

Top 5 Local Targets — Targets

IP/DNS Name	Mag…	Vulnerable	Chained	User	MAC	Location	Weight
Windows AD Server		Unknown	No	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	Adm…	…7	main	10
10.101.3.11		Unknown	No	DC…	…7	main	0

Are any of them vulnerable?

Top 10 Events — Events

Event Name	Magnitude		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 :: qra…		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qra…		10.101.3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qra…		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qra…		10.101.3.15	445	09-29 16:05:01

What is the Supporting evidence?

Q1 Labs
Total Security Intelligence

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

Q1 Labs
Total Security Intelligence

Malware Activity

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

View flows for this offense

Magnitude		Relevance	0 / 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 enables detection of a covert channel.

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:1
```

Irrefutable Botnet Communication

Layer 7 data contains botnet command and control instructions.

Q1 Labs
Total Security Intelligence

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

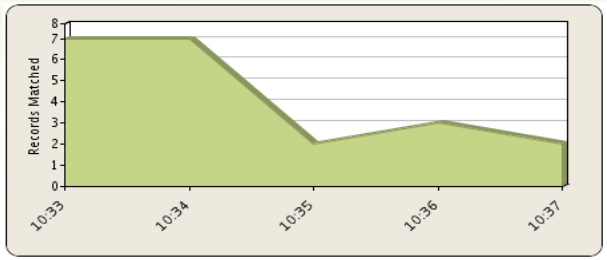
User Activity Monitoring

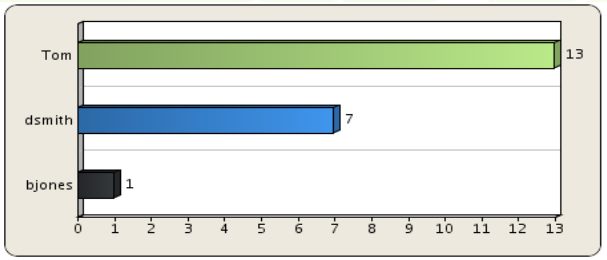
Offense 2834 Summary | Attackers | Targets | Categories | Annotations | Networks | Events | Flows | Rules | Actions ▼ | Print

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.

Q1 Labs
Total Security Intelligence

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

Q1 Labs
Total Security Intelligence

Complex Threat 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 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.

Q1 Labs
Total Security Intelligence

Compliance Monitoring

Problem Statement

- Validating your monitoring efforts against compliance requirements
- Ensuring that compliance goals align with security goals
- Logs alone don't meet compliance standards

Required Visibility

- Application layer visibility
- Visibility into network segments where logging is problematic

Q1 Labs
Total Security Intelligence

Compliance Visibility

Offense 2862 Summary | Attackers | Targets | Categories | Annotations | Networks | Events

Magnitude		**Relevance**	2
Description	Policy - Internal - Clear Text Application Usage containing Compliance Policy Violation - QRadar Classify Flow	**Event count**	1 events in 1 catego
Attacker/Src	10.103.12.12 (dhcp-workstation-103-12-12.acme.org)	**Start**	2009-09-29 15:09:0
Target(s)/Dest	10.101.3.30 (Accounting Fileserver)	**Duration**	0s
Network(s)	IT.Server.main	**Assigned to**	Not assigned
Notes	PCI Violation Use Case PCI DSS specifies that insecure protocols may not be used. This scenario der identify such activity. In this offense the system has captured cleartext network activity (telnet and FTP) b		

PCI Compliance at Risk?

Event Name	Log Source	Source IP	Source Port	Destination IP	Destination Port
Compliance Policy Violation - C	Flow Classification Engine-5 :	10.103.12.12	1482	10.101.3.30	23

Unencrypted Traffic

QFlow saw a cleartext service running on the Accounting server.

PCI Requirement 4 states: Encrypt transmission of cardholder data across open, public networks

Compliance Simplified

Out of the box support for all major compliance and regulatory standards.

Q1 Labs
Total Security Intelligence

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

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

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

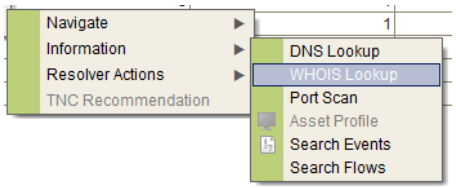
Who?

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

Q1 Labs
Total Security Intelligence

Network and Asset Discovery

Problem Statement

- Integration of asset information into security monitoring products is manual and labor intensive
- The assets you don't know about pose the greatest risk
- Asset discovery and classification is a key tenet of many compliance regulations
- False positive noise jeopardizes the effectiveness of the SIEM

Required Capability

- Real-time knowledge of all assets on a network
- Visibility into asset communication patterns
- Classification of asset types
- Tight integration into pre-defined rules is critical

Q1 Labs
Total Security Intelligence

Network and Asset Discovery

Port	Risk / Severity	Last Seen	First Seen
514	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
7676	1	2009-09-29 21:30:12 (Passive)	2009-09-28 02:30:11 (Passive)
7777	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
7778	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
8009	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)

Server Discovery

To discover servers (assets) in your deployment based on standard server ports, select the desired role in the Server Type drop-down list box and click 'Discover Servers'.

Server Type:	Database Servers All Assigned Unassigned
Ports:	1433, 1434, 3306, 66, 1521, 1525, 1526, 1527, 1528, 1529, 1571, 1575, 1630, 1748, 1754, 1808, 1809, 2481, 2482, 2484, 3872, 3891, 3938 Edit Ports
Server Type Definition:	Edit this BB to define typical database servers. This BB is used in conjunction with the Default-BB-FalsePositive: Database Server False Positive Categories and Default-BB-FalsePositive: Database Server False Positive Events building blocks. Edit Definition
Network:	Select an object...

Discover Servers

Matching Servers:

Approve	Name	IP	Network ▲
☐		10.101.139.151	Asia.Bridges.all
☐	Patient Records DB	10.101.139.156	Asia.Bridges.all
☐		10.101.144.76	Asia.Holloway.all
☐		10.102.150.115	Business.Staff
☑	CRM Database	10.101.145.198	IT.NetServers
☐		10.101.145.237	IT.NetServers
☐	CRM	10.101.3.32	IT.Server.main
☐		10.101.146.10	IT.other

- **Automatic Asset Discovery**
  QRadar creates host profiles as network activity is seen to/from
- **Passive Asset Profiling**
  QRadar identifies services and ports on hosts by watching network activity
- **Server Discovery**
  QRadar identifies and classifies server infrastructure based on these asset profiles
- **Correlation on new assets & services**
  Rules can fire when new assets and services come online

All made possible by Netflow & QFlow

Q1 Labs
Total Security Intelligence

"To lack intelligence is to be in the ring blindfolded."

Former Commandant of the Marine Corps, General David M. Shoup

Q1 Labs
Total Security Intelligence

Questions

Q1 Labs
Total Security Intelligence

Vielen Dank!