Training Intelligent Event Correlation Systems to Know Which Alerts Matter

Craig Chamberlain
Principal Security Consultant
Q1 Labs
craig@q1labs.com
http://www.q1labs.com

About Today's Presentation

- Slides should be available from Q1 Labs and my personal site
- More a technical talk than a sales presentation
- Not theoretical – all examples are real world
- Limited time – but I am available this week to meet and happy to discuss most any subject in great detail
- Please see me or contact me to schedule a meeting.

Agenda

- Observations on technological and human security workflow and process
- The state of security correlation today
- Correlation advances
- Introducing QRadar
- Real-world examples
- Q&A

Characteristics of Security Products

- IDS technologies evolved some time ago when processing power was less plentiful; processing atomic events was expedient and affordable approach
- IDS and log consoles often produce mountains of slow moving data containing very large numbers (billions and billions..) of alerts
- Analysts perform significant manual correlation between different products and their logs & alerts to produce timelines and incident stories

Characteristics of the Security Operator

- The human security analyst does not produce a daily report containing thousands of alerts or atomic events
- The human analyst sees the story in the alert data - even when the specific patterns vary - and assembles events into and incident report which tells the story
- The human analyst understands which alerts are important and which are noise, by considering the context (network terrain, history, and timelines)

State of Correlation Today

- "Red, yellow, green" technology – three mountains of alerts instead of one
- Intelligent decisions and coherent incident stories cannot be derived from atomic events
- Was the attack successful? What happened *after* the attack? What, if anything, was lost?

Intelligent Event Correlation

- The accuracy and relevance of correlated security data is roughly the square of the number of data sources
- Human analysts know how to correlate these to determine what really happened; why can't the machines "learn" to do some of this?
- We don't have thinking machines yet but intelligent decisions can be made, even by machines, by imitating analyst behavior

Intelligent Event Correlation

"Can you, like, learn stuff? So you can be, you know, more human..and not such a dork all the time?"

- John Connor, *Terminator 2*

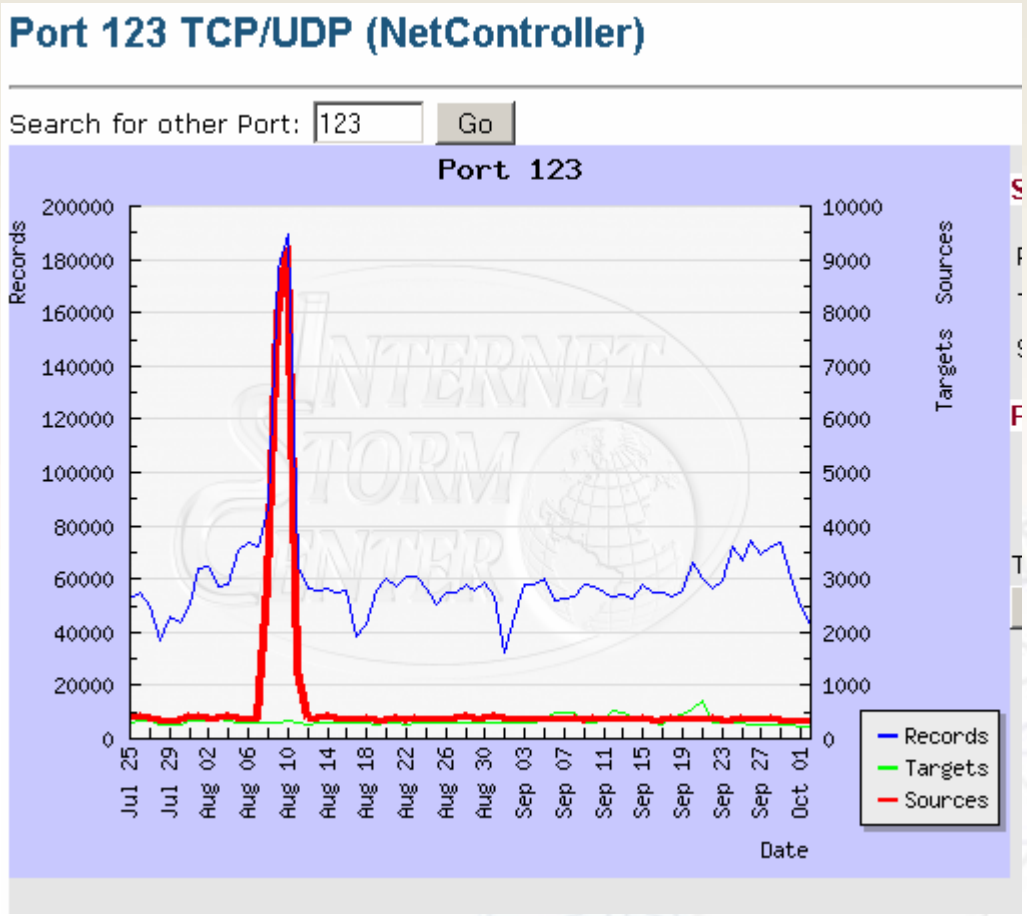
Intelligent Event Correlation

- All data sources – IDS, firewall logs, auth logs, behavioral & statistical detection have value; none are perfect
- Events can be correlated by source, destination, network, timelines and category
- Alert relevance can be increased by considering context, location and timeline

Why Behavioral Detection?

- Human analysts can often spot patterns of misuse they have not seen before
- Interestingly, behavioral detection algorithms can imitate this and sometimes find new activity patterns the coder had not thought of
- Behavioral detection example: malware traffic trying to look like NTP

Behavioral Detection Example: Detecting a Traffic Event



Behavioral Detection Example: Correlated Netflow Data

IP	Bytes In	Bytes Out	Packets In	Packets Out	Local Unique Ports	Remote Unique Ports	Host Count	Flow Count
0.0.120.156	0	5362560	0	59584	1	1	1062	22725

- The source port is 123 (local) and the destination port is 1230 (remote) ntp traffic should be using dest port 123. This could be an attempted method of hiding the traffic among legitimate ntp traffic.
- Ports aside, how do we know it's not ntp? Layer 7 inspection using application protocol signatures
- A spike in port 123 traffic coincided with this detect, as seen on previous slide.
- There are 1062 hosts and over 5 MB of traffic which works out to around 5K each which is a lot of ntp
- All of this happened within a 25 minute period starting at 9:07 that morning.

Behavioral Detection Example 2: Bot Detection

Here we see two behavioral bot traffic detections. Our bot has been detected two ways:

- The bot contacts a known botnet controller IP
- The bot directly query remote DNS servers to avoid DNS mitigation or contact controllers which are too new to be resolvable.

Why are these useful? Bots using encryption or HTTP tunneling cannot be found by Internet Relay Chat (IRC) protocol detection (or where packet contne t inspection is otherwise unavailable)

Behavioral Detection Example 2: Bot Detection

Offense 35 — Summary | Targets | Categories | Annotations | Networks | Events | Flows | Actions

Magnitude				**Relevance**	3	**Severity**	6	**Credibility**	3
Description	Malware - External - Communication with BOT Control Channel preceded by Malware - External - Client Based DNS Activity to the Internet preceded by Potential Botnet Activity		**Event count**	39 events in 4 categories					
Attacker/Src	10.100.75.10		**Start**	2007-02-17 21:15:14					
Target(s)/Dest	10.100.50.16 Remote (2)		**Duration**	9m 48s					
Network(s)	Multiple (2)		**Assigned to**	Not assigned					
Notes									

Attacker Summary — Details

Magnitude		**User**	Unknown
Description	10.100.75.10	**MAC**	Unknown
Vulnerabilities	0	**Asset Weight**	0
Location	DMZ.Internal		

Top 5 Categories — Categories

Name	Magnitude	Local Target Count	Events	Last Event
Misc Malware		0	3	02-17 21:20:06
Potential Botnet connection		0	1	02-17 21:21:36
Misc flow		0	3	02-17 21:20:06
Firewall Deny		1	32	02-17 21:26:06

Top 5 Local Targets — Targets

IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
10.100.50.16		Unknown	No	Unknown	Unknown	Net_10_0_0_0	0

Top 10 Events — Events

Event Name	Magnitude	Device	Category	Destination	Start Time
Misc Malware - Event CRE		eventprocessor0 :: craig	Misc Malware	198.41.0.4:53	02-17 21:15:56
Misc Malware - Event CRE		eventprocessor0 :: craig	Misc Malware	198.41.0.4:53	02-17 21:15:14
Misc Malware - Event CRE		eventprocessor0 :: craig	Misc Malware	198.41.0.4:53	02-17 21:20:05
Firewall Deny command		Auto-discovered Pix at 10.100.150.9	Firewall Deny	10.100.50.16:0	02-17 21:15:27
Firewall Deny command		Auto-discovered Pix at 10.100.150.9	Firewall Deny	10.100.50.16:0	02-17 21:16:44
Firewall Deny command		Auto-discovered Pix at 10.100.150.9	Firewall Deny	10.100.50.16:0	02-17 21:16:18
Firewall Deny command		Auto-discovered Pix at 10.100.150.9	Firewall Deny	10.100.50.16:0	02-17 21:15:52
Firewall Deny command		Auto-discovered Pix at 10.100.150.9	Firewall Deny	10.100.50.16:0	02-17 21:17:09
Firewall Deny command		Auto-discovered Pix at 10.100.150.9	Firewall Deny	10.100.50.16:0	02-17 21:17:35

Behavioral Detection Example 2: Bot Detection

Top 5 Annotations Annotations

Annotation	Time	Weight
SENTRY Description: Malware - External - Communication with BOT Control Channel:Previously, the IP address being communicated with was a control channel for a BOTNET. The local machine may be infected with a bot and should be investigated.	02-17 21:22:06	7
SENTRY Description: Malware - External - Client Based DNS Activity to the Internet:Detects a host attempting to connect to a DNS server that is not defined as a local network. With the exception of your DNS servers or other hosts specifically configured to communicate with external DNS servers, this is suspicious activity and may be the sign of a bot net connection. If this is a false positive, add the external DNS server to the Q1-BB-HostDefinition: DNS Servers building block in custom rules.	02-17 21:16:05	7
[5] "Target/Event Analysis". The number of events this attacker generated during this attack, was deemed worth a value of 5 on a scale of 0-10, with higher values indicating high volumes of events generated, and lower numbers indicating a smaller grade attack.	02-17 21:27:06	6
"CRE Event". CRE Rule description: Detected a host connecting or attempting to connect to a DNS server on the Internet. This may indicate a host connecting to a Botnet. The host should be investigated for malicious code.	02-17 21:16:05	6

- The bot contacts a known botnet controller IP
- The bot directly query remote DNS servers to avoid DNS mitigation or contact controllers which are too new to be resolvable.

Behavioral Detection Example 3: SMTP-using malware

- Here we see a SPAMbot or mass mailing malicious program detect generating a large amount of SMTP traffic over a period of time
- Cannot be reliably done with atomic events. Requires profiling behavior over time to detect SMTP misuse while ignoring legitimate SMTP servers.

Behavioral Detection Example 3: SMTP-using malware

Offense 70 — Summary | Targets | Categories | Annotations | Networks | Events | Flows | Actions

Magnitude			**Relevance**	3	**Severity**	4	**Credibility**	3
Description	Local Mass Mailing Host Detected	**Event count**	361 events in 3 categories				
Attacker/Src	10.100.50.23	**Start**	2007-02-18 00:43:38				
Target(s)/Dest	Remote (12)	**Duration**	1m 52s				
Network(s)	other	**Assigned to**	Not assigned				
Notes							

Attacker Summary Details

Magnitude		**User**	Unknown
Description	10.100.50.23	**MAC**	Unknown
Vulnerabilities	0	**Asset Weight**	0
Location	Net-10-172-192.Net_10_0_0_0		

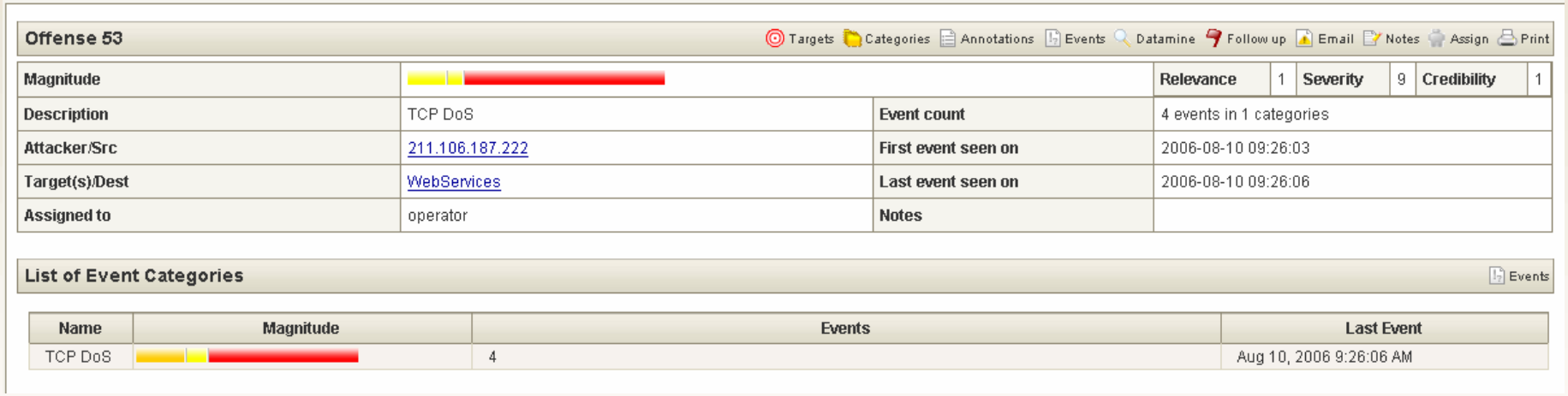
Top 5 Categories Categories

Name	Magnitude	Local Target Count	Events	Last Event
Mail Policy Violation		0	210	02-18 00:45:38
Firewall Deny		0	10	02-18 00:45:38
IP Protocol Anomaly		0	141	02-18 00:45:38

Top 10 Events Events

Event Name	Magnitude	Device	Category	Destination	Start Time
Mail Policy Violation - Event CRE		eventprocessor0 :: craig	Mail Policy Violation	216.55.168.215:25	02-18 00:43:58
Mail Policy Violation - Event CRE		eventprocessor0 :: craig	Mail Policy Violation	64.255.172.50:25	02-18 00:43:38
Mail Policy Violation - Event CRE		eventprocessor0 :: craig	Mail Policy Violation	65.54.244.136:25	02-18 00:43:42
Mail Policy Violation - Event CRE		eventprocessor0 :: craig	Mail Policy Violation	64.255.172.50:25	02-18 00:43:46
Mail Policy Violation - Event CRE		eventprocessor0 :: craig	Mail Policy Violation	64.4.33.7:25	02-18 00:44:02
Mail Policy Violation - Event CRE		eventprocessor0 :: craig	Mail Policy Violation	69.147.112.160:25	02-18 00:44:00
Mail Policy Violation - Event CRE		eventprocessor0 :: craig	Mail Policy Violation	72.51.27.51:25	02-18 00:45:25
Mail Policy Violation - Event CRE		eventprocessor0 :: craig	Mail Policy Violation	216.55.168.215:25	02-18 00:45:28
Mail Policy Violation - Event CRE		eventprocessor0 :: craig	Mail Policy Violation	64.4.33.7:25	02-18 00:45:18
Mail Policy Violation - QRadar Class...		classify0 :: craig	Mail Policy Violation	216.55.168.215:25	02-18 00:43:58

Behavioral Detection Example 4: Denial of Service (DOS) Attack



Offense 53 — Targets | Categories | Annotations | Events | Datamine | Follow up | Email | Notes | Assign | Print

Magnitude			**Relevance**	1	**Severity**	9	**Credibility** 1
Description	TCP DoS	**Event count**	4 events in 1 categories				
Attacker/Src	211.106.187.222	**First event seen on**	2006-08-10 09:26:03				
Target(s)/Dest	WebServices	**Last event seen on**	2006-08-10 09:26:06				
Assigned to	operator	**Notes**					

List of Event Categories — Events

Name	Magnitude	Events	Last Event
TCP DoS		4	Aug 10, 2006 9:26:06 AM

- Here we see a denial-of-service attack (DOS) of a web server.
- Again, cannot be accomplished by processing atomic events

Behavioral Detection Example 5: SSH Tunnel on Nonstandard Port

Offense 55 — Summary | Targets | Categories | Annotations | Networks | Events | Flows | Actions

Magnitude				**Relevance**	4	**Severity**	9	**Credibility**	2
Description	Policy - Internal - SSH or Telnet Detected on Non-Standard Port containing Backdoor Detected - QRadar Classify Flow		**Event count**	4 events in 1 categories					
Attacker/Src	10.100.45.55		**Start**	2007-02-17 22:35:02					
Target(s)/Dest	10.100.100.208		**Duration**	2m 55s					
Network(s)	Net-10-172-192.Net_10_0_0_0		**Assigned to**	Not assigned					
Notes									

Attacker Summary — Details

Magnitude		**User**	dave.bolton@Q1LABS.INC
Description	10.100.45.55	**MAC**	
Vulnerabilities	0	**Asset Weight**	0
Location	VPN_Addresses_Space.VPN_Addresses_Space		

Top 5 Categories — Categories

Name	Magnitude	Local Target Count	Events	Last Event
Backdoor Detected		1	4	02-17 22:38:52

Top 5 Local Targets — Targets

IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
10.100.100.208		Unknown	No	Unknown	Unknown	Net_10_0_0_0	0

Top 10 Events — Events

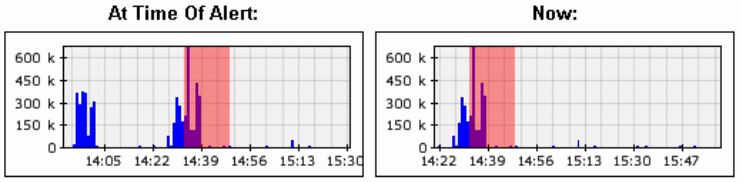
Event Name	Magnitude	Device	Category	Destination	Start Time
Backdoor Detected - QRadar Classify Flow		classify0 :: craig	Backdoor Detected	10.100.100.208:5000	02-17 22:35:58
Backdoor Detected - QRadar Classify Flow		classify0 :: craig	Backdoor Detected	10.100.100.208:5000	02-17 22:35:02
Backdoor Detected - QRadar Classify Flow		classify0 :: craig	Backdoor Detected	10.100.100.208:5000	02-17 22:36:58
Backdoor Detected - QRadar Classify Flow		classify0 :: craig	Backdoor Detected	10.100.100.208:5000	02-17 22:37:57

Behavioral Detection Example 7: Large Outbound File Transfer

Incident: Started At: Sun Feb 18 14:36:41 2007 Show All

Event: Outbound Bytes - Sun Feb 18 14:40:41 2007 Show All

View:	nets - Flows are classified by the defined n...
Object(s):	all
Network Location:	all
Layer:	Outbound Bytes
Event Number:	1
Response Number:	7 of Unlimited
Response:	Value above 30720.



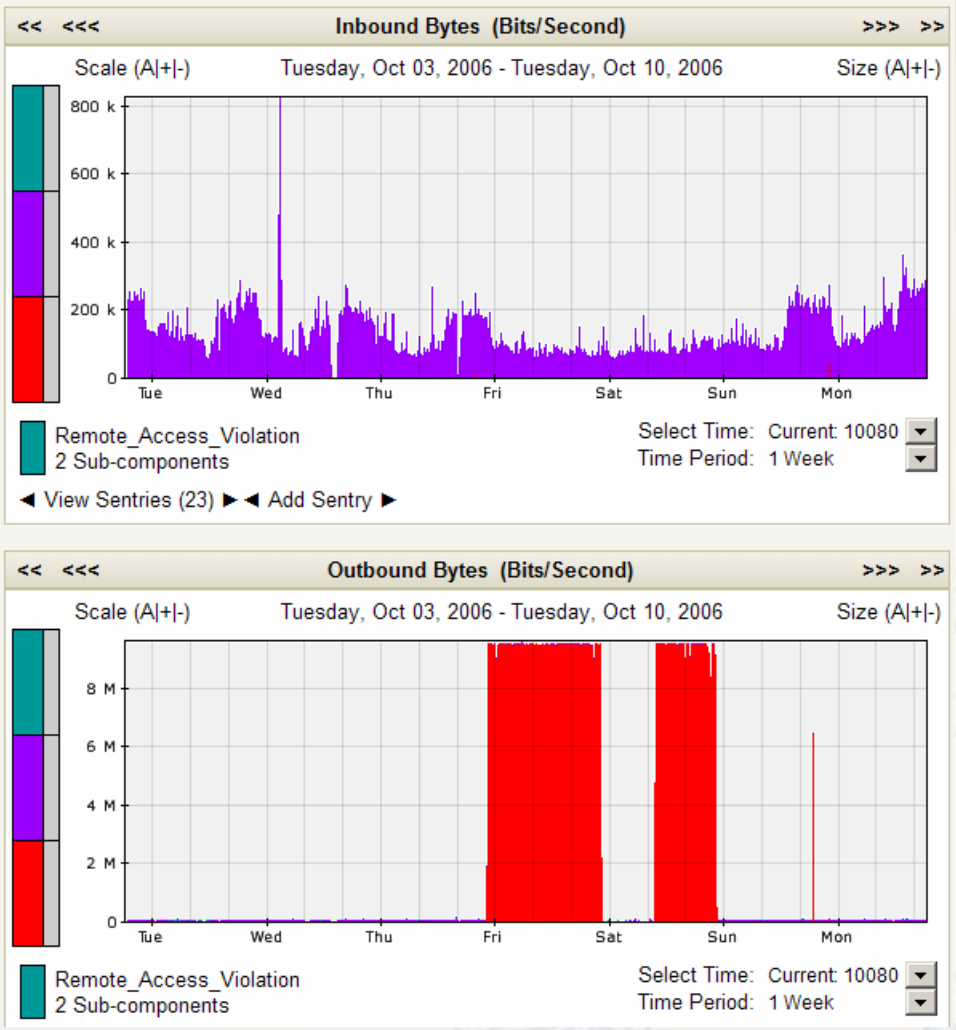
Sentry Description:
This could indicate and information leak.

Show Flows | Save Report | Email Report

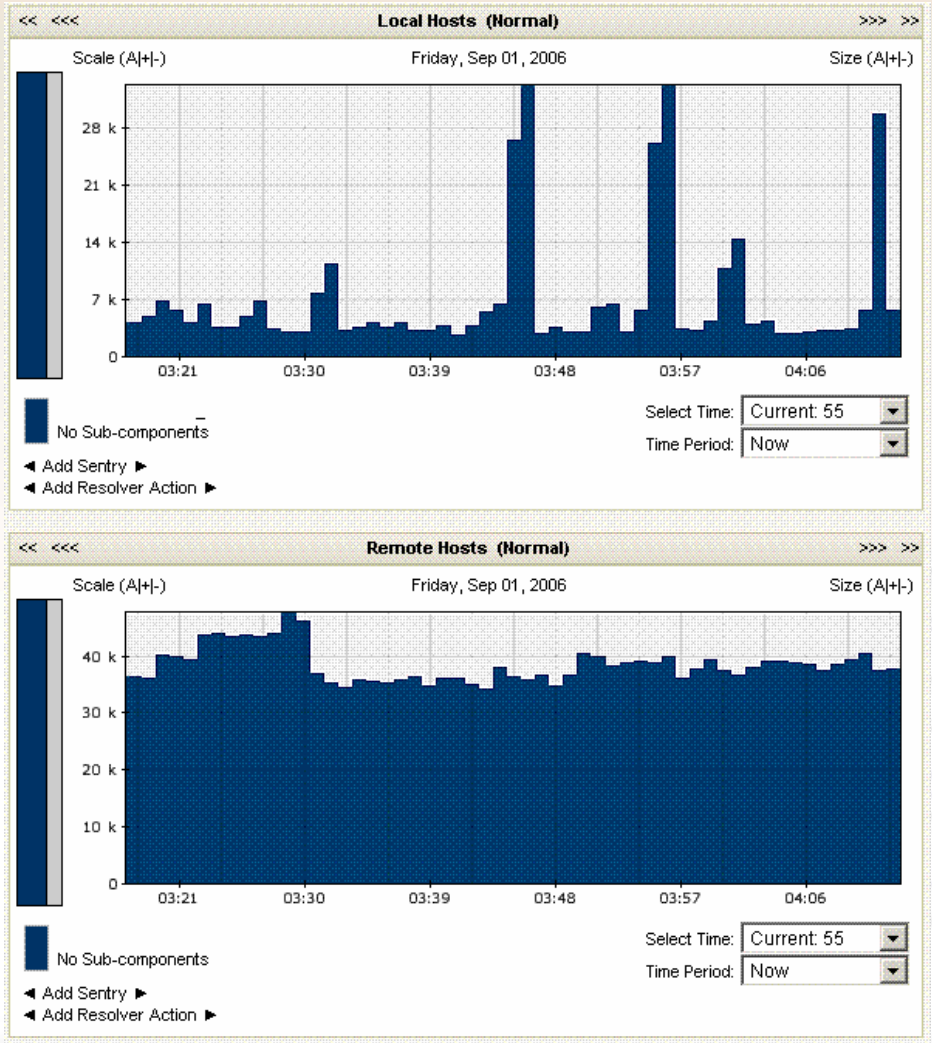
Results - Aggregates

AppID	Bytes In	Bytes Out ▼	Packets In	Packets Out	Local Unique Ports
SSH-Ports	1104	37884	15	36	1
HTTPWeb	60	19848	1	285	6
Web-Port	0	7608	0	108	24

Behavioral Detection Example 8: Large Outbound Information Leak



Behavioral Detection Example 8: Early Worm Activity Detection: Large Increase in Remote Host Count



Behavioral Detection Example 8: Zero-Day Worm Detection

Offense 64781 — Targets | Categories | Annotations | Events | Datamine | Follow up | Dismiss | Close | Email | Notes | Assign

Magnitude		**Relevance** 0	**Severity** 7	**Credibility** 2
Description	Aggressive Local Scanner Detected preceded by Remote UDP Scanner Detected preceded by Possible Local Worm Detected preceded by Local UDP Scanner Detected	**Event count**	104886 events in 3 categories
Attacker/Src		**First event seen on**	2006-10-26 07:31:07
Target(s)/Dest	Remote (58891)	**Last event seen on**	2006-10-26 11:08:03
Assigned to		**Notes**	Port 38293 sweep of the .x net - what is this?

List of Event Categories — Events

Name	Magnitude	Events	Last Event
UDP Reconnaissance		3428	Oct 26, 2006 11:07:02 AM
Potential worm activity		340	Oct 26, 2006 11:07:02 AM
Network Sweep		101118	Oct 26, 2006 11:08:04 AM

- Behavioral detection of early scanning activity preceding a zero-day worm targeting a desktop antivirus client vuln (October, 2006)
- Behavioral detection provided a valuable early warning system
- Effective where signatures are not available

Why Behavioral Detection?

- Behavioral detection is a powerful application for event correlation
- Behavioral detection can help fill in the blanks in an incident profile
- Behavioral detection can be customized to find things other methods cannot

Intelligent Event Correlation

- Did the target of an attack or event respond? Does the target exist?
- Did a scan precede an attack or is it background noise?
- Was the attack well targeted or scattershot?
- Did the target of an attack become the source of another attack? – offense chaining
- What happened next? –need session data

Correlation Example 1

Offense 92 — Targets | Categories | Annotations | Events | Datamine | Follow up | Email | Notes | Assign | Print

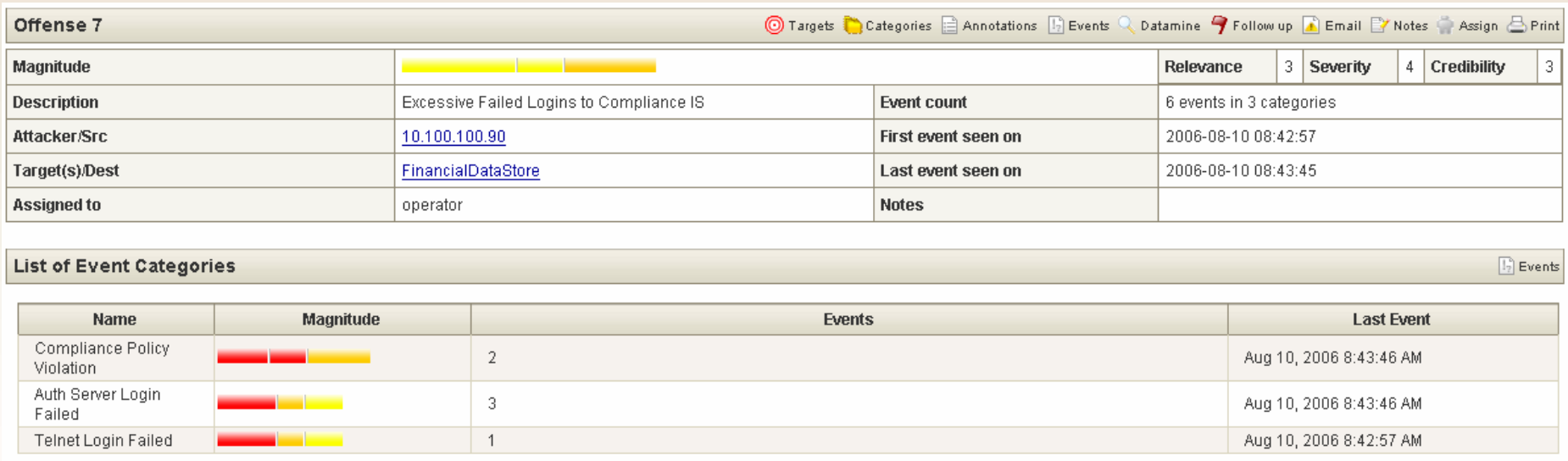
Magnitude		**Relevance** 4	**Severity** 6	**Credibility** 3
Description	Privilege Escalation Failed preceded by IP Protocol Anomaly preceded by Host Query preceded by ICMP Reconnaissance	**Event count**	93 events in 5 categories
Attacker/Src	10.100.50.5	**First event seen on**	2006-08-10 11:24:38
Target(s)/Dest	Multiple (7)	**Last event seen on**	2006-08-11 03:39:36
Assigned to	admin	**Notes**	

List of Event Categories — Events

Name	Magnitude	Events	Last Event
IP Protocol Anomaly		8	Aug 11, 2006 3:39:36 AM
Buffer Overflow		15	Aug 10, 2006 5:50:01 PM
Host Query		44	Aug 10, 2006 5:50:12 PM
ICMP Reconnaissance		22	Aug 10, 2006 5:50:01 PM
Privilege Escalation Failed		4	Aug 10, 2006 1:15:59 PM

- Privilege escalation attempt, followed by recon, followed by an exploit, followed by failed connection attempts

Correlation Example 2: Tracking An Incident



Offense 7 — Targets | Categories | Annotations | Events | Datamine | Follow up | Email | Notes | Assign | Print

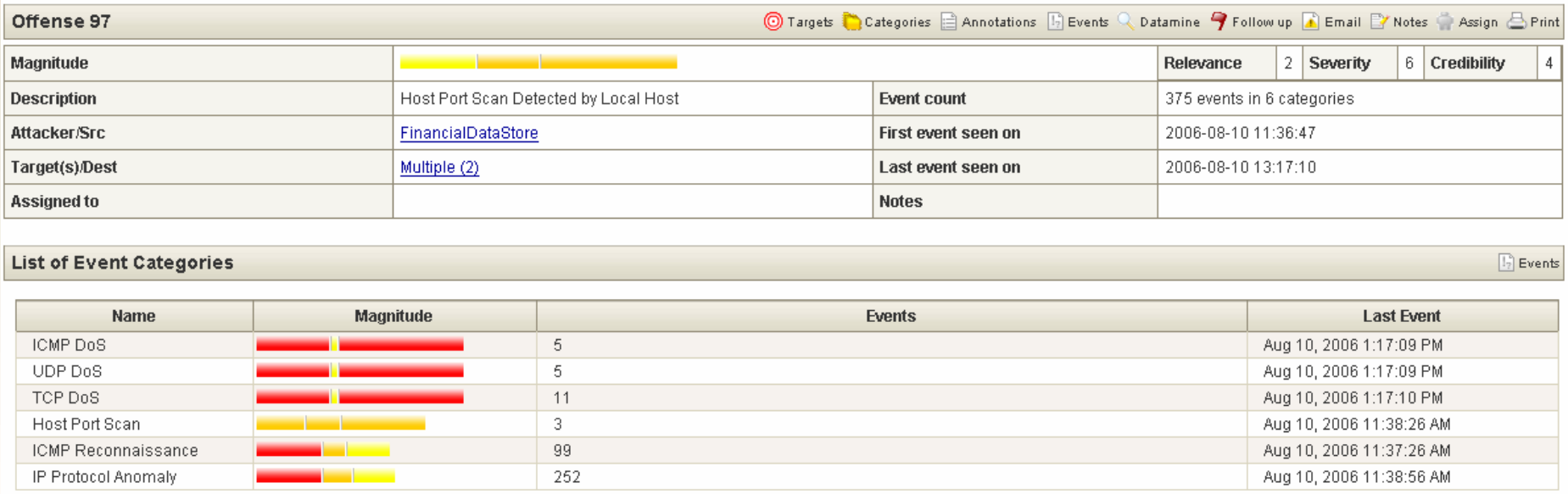
Magnitude			**Relevance**	3	**Severity**	4	**Credibility**	3
Description	Excessive Failed Logins to Compliance IS	**Event count**	6 events in 3 categories				
Attacker/Src	10.100.100.90	**First event seen on**	2006-08-10 08:42:57				
Target(s)/Dest	FinancialDataStore	**Last event seen on**	2006-08-10 08:43:45				
Assigned to	operator	**Notes**					

List of Event Categories — Events

Name	Magnitude	Events	Last Event
Compliance Policy Violation		2	Aug 10, 2006 8:43:46 AM
Auth Server Login Failed		3	Aug 10, 2006 8:43:46 AM
Telnet Login Failed		1	Aug 10, 2006 8:42:57 AM

- Here we see repeated failed attempts to logon to a sensitive server.

Correlation Example 2: Tracking An Incident



Offense 97 — Targets | Categories | Annotations | Events | Datamine | Follow up | Email | Notes | Assign | Print

Magnitude				**Relevance**	2	**Severity**	6	**Credibility**	4
Description	Host Port Scan Detected by Local Host	**Event count**	375 events in 6 categories					
Attacker/Src	FinancialDataStore	**First event seen on**	2006-08-10 11:36:47					
Target(s)/Dest	Multiple (2)	**Last event seen on**	2006-08-10 13:17:10					
Assigned to		**Notes**						

List of Event Categories — Events

Name	Magnitude	Events	Last Event
ICMP DoS		5	Aug 10, 2006 1:17:09 PM
UDP DoS		5	Aug 10, 2006 1:17:09 PM
TCP DoS		11	Aug 10, 2006 1:17:10 PM
Host Port Scan		3	Aug 10, 2006 11:38:26 AM
ICMP Reconnaissance		99	Aug 10, 2006 11:37:26 AM
IP Protocol Anomaly		252	Aug 10, 2006 11:38:56 AM

- The server then displays new behavior: new data connections, reconnaissance, and failed connections.

Correlation Example 2: Discussion

- Otherwise requires manual correlation of these events; significant time and effort
- Significant increase in coverage and efficiency of security detection
- What next?
  - Identify the user on the source workstation, using AD auth logs or tools
  - Profile the nature and destination of the anomalous traffic using session data (netflow, qflow, etc.)
  - Begin incident response

- Does the host exist? Did it respond?
- Are the services targeted running?
- Is the attack well targeted? Does the attack use a relevant exploit?
- If no, lower its importance. If yes, raise its importance.

Next Example: A Typical Nessus Scan of a Class C Network

Offense 69 — Summary | Targets | Categories | Annotations | Networks | Events | Flows | Actions

Magnitude			**Relevance**	4	**Severity**	5	**Credibility**	3
Description	Suspicious - Internal - Rejected Communication Attempts preceded by Multiple Exploit/Malware Types Targeting a Single Source preceded by Authentication: Repeated Login Failures Single Host preceded by Host Port Scan Detected by Local Host preceded by Suspicious - Internal - Unidirectional TCP Flows	**Event count**	283171 events in 37 categories				
Attacker/Src	10.100.100.128	**Start**	2007-02-18 00:40:21				
Target(s)/Dest	Local (80)	**Duration**	5h 8m 51s				
Network(s)	Multiple (2)	**Assigned to**	Not assigned				
Notes							

Attacker Summary — Details

Magnitude		**User**	Unknown
Description	10.100.100.128	**MAC**	Unknown
Vulnerabilities	0	**Asset Weight**	0
Location	Net-10-172-192.Net_10_0_0_0		

Top 5 Categories — Categories

Name	Magnitude	Local Target Count	Events	Last Event
Web Exploit		56	8589	02-18 05:47:12
Distributed DoS		20	72	02-18 05:47:12
Misc Exploit		45	274	02-18 05:47:12
Trojan Detected		25	112	02-18 05:45:42
Flow Context Response		15	15	02-18 03:44:11

Top 5 Local Targets — Targets

IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
10.100.100.208		Unknown	No	Unknown	Unknown	Net_10_0_0_0	0
10.100.50.21		Unknown	No	Unknown	Unknown	Net_10_0_0_0	0
172.16.150.40		Unknown	No	Unknown	Unknown	Net_172_16_0_0	0
172.16.150.145		Unknown	No	Unknown	Unknown	Net_172_16_0_0	0
172.16.150.143		Unknown	No	Unknown	Unknown	Net_172_16_0_0	0

Next Example: A Typical Nessus Scan of a Class C Network

Offense 69 — Summary | Targets | Categories | Annotations | Networks | Events | Flows | Actions

Magnitude		**Relevance** 4	**Severity** 5	**Credibility** 3
Description	Suspicious - Internal - Rejected Communication Attempts preceded by Multiple Exploit/Malware Types Targeting a Single Source preceded by Authentication: Repeated Login Failures Single Host preceded by Host Port Scan Detected by Local Host preceded by Suspicious - Internal - Unidirectional TCP Flows	**Event count**	283171 events in 37 categories
Attacker/Src	10.100.100.128	**Start**	2007-02-18 00:40:21
Target(s)/Dest	Local (80)	**Duration**	5h 8m 51s
Network(s)	Multiple (2)	**Assigned to**	Not assigned
Notes			

List of Event Categories — Events

Name	Magnitude	Local Target Count	Events	Last Event
Firewall Session Closed		400	75417	02-18 05:50:13
IP Protocol Anomaly		331	63525	02-18 05:48:43
Potential Web Vulnerability		84	11954	02-18 05:48:43
System Action Allow		104	16071	02-18 05:48:43
Anomaly		238	2939	02-18 05:48:43
Firewall Session Opened		333	75133	02-18 05:48:43
Web Reconnaissance		72	17005	02-18 05:47:12
Web Protocol Anomaly		70	1429	02-18 05:47:12
Web Exploit		56	8589	02-18 05:47:12
Misc Exploit		45	274	02-18 05:47:12
Misc Recon Event		121	1969	02-18 05:47:12
Distributed DoS		20	72	02-18 05:47:12
NMAP Reconnaissance		36	809	02-18 05:47:12
Privilege Escalation Failed		24	102	02-18 05:45:42
System Error		38	210	02-18 05:45:42

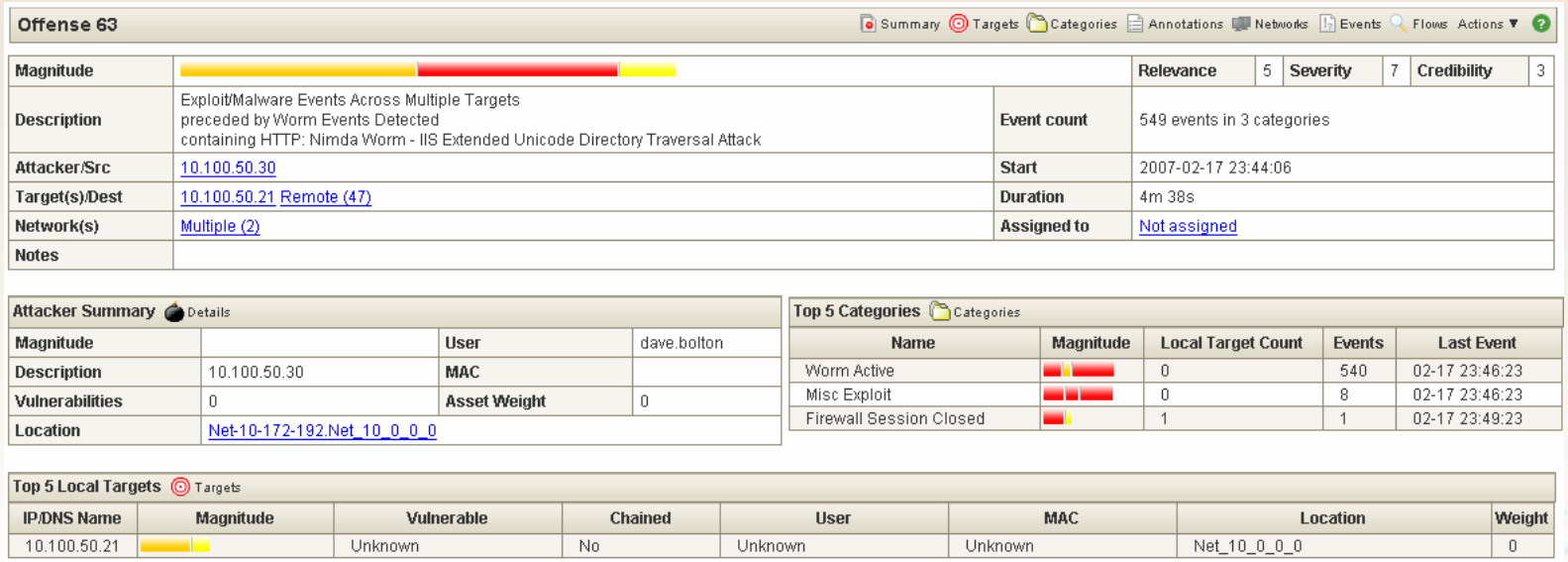
Contextual Awareness

- Source and destination are key in determining the severity of an event
- Many networks have an acceptable level of noise and misuse – scans may become background noise in perimeter networks
- Noise events – scans – drown out the important events

Reducing Noise: Suppress Alerting On Noise Events

- Attacks targeted at nonexistent vulnerabilities
- Worms of yesteryear
- “Script kiddies” or “ankle biters”
- Reconnaissance not followed by attack – the background radiation of the Internet
- Log these events; do not alert on those that have low impact

Worm example: Nimda wormscan



Offense 63 — Summary | Targets | Categories | Annotations | Networks | Events | Flows | Actions

Magnitude				**Relevance**	5	**Severity**	7	**Credibility**	3
Description	Exploit/Malware Events Across Multiple Targets preceded by Worm Events Detected containing HTTP: Nimda Worm - IIS Extended Unicode Directory Traversal Attack		**Event count**	549 events in 3 categories			
Attacker/Src	10.100.50.30		**Start**	2007-02-17 23:44:06			
Target(s)/Dest	10.100.50.21 Remote (47)		**Duration**	4m 38s			
Network(s)	Multiple (2)		**Assigned to**	Not assigned			
Notes							

Attacker Summary — Details

Magnitude		**User**	dave.bolton
Description	10.100.50.30	**MAC**	
Vulnerabilities	0	**Asset Weight**	0
Location	Net-10-172-192.Net_10_0_0_0		

Top 5 Categories — Categories

Name	Magnitude	Local Target Count	Events	Last Event
Worm Active		0	540	02-17 23:46:23
Misc Exploit		0	8	02-17 23:46:23
Firewall Session Closed		1	1	02-17 23:49:23

Top 5 Local Targets — Targets

IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
10.100.50.21		Unknown	No	Unknown	Unknown	Net_10_0_0_0	0

- Probably a permanent feature of the Net
- Do we want to alert on Internet worms of yesteryear? Probably not.
- Do we want to detect worm propagation internally? Probably (and if it's not a known worm, or it's a big event, raise the alert level even higher).

Multivariate Correlation Rules

- Correlation of vulnerability and attack data yields massive increase in accuracy of prioritization
- Correlation of authentication logs, firewall logs and session (e.g. netflow) data yields successful misuse detection
- Session and packet data can answer the question of what happened as a result of an incident

Multivariate Correlation: Marrying IDS Detects and Vulnerability Data

- Vuln data correlation only accurate when collected in advance and correlated at the time of the attack?
- “We saw an exploit alert this morning. I scanned and the host is not vulnerable.”
- Why? Intruders patch vulnerabilities to reinforce their position

Vulnerability / Exploit Correlation Example

Offense 3968

Magnitude			**Relevance**	5	**Severity**	6	**Credibility**	6
Description	Rule:[Vulnerable Target Exploit Attempt, Local Scanner Detected, Exploit/Malware events across multiple targets, Possible Local Worm Detected, Local Suspicious Probe Events Detected, SNMP Based Recon Detected, Aggressive Local Scanner Detected]	**Event count**	33250 events in 9 categories					
Attacker/Src	10.100.50.50	**First event seen on**	2006-01-25 13:33:28					
Target(s)/Dest	Multiple (6822)	**Last event seen on**	2006-01-25 14:55:55					

List of Annotations

Date	Annotation
2006-01-25 14:58:19	[10] "Target/Event Analysis". This attacker attemped to attack 10% of the IPs in the IP range defined by this network.
2006-01-25 14:58:19	[2] This attacker attempted to attack more hosts on the network then are known to exist. Approximatly 2% of the targets attacked, are thought to exist. The accuracy and scope of the attack is important to consider, as it may differentiate between a blind script-kiddie attack, and an accurate, intentional penetration attempt.
2006-01-25 14:58:19	[10] "Target/Event Analysis". The number of events this attacker generated during this attack, was deemed worth a value of 10 on a scale of 0-10, with higher values indicating high volumes of events generated, and lower numbers indicating a smaller grade attack.
2006-01-25 14:55:18	"Offense Chaining". This offense has 7 targets (destination IPs), which are the source (attacker) in other offenses
2006-01-25 14:54:20	[Vulnerable Target Exploit Attempt] "Offense Renamed". This offense has been renamed to "Vulnerable Target Exploit Attempt" by user request, based on an Event Rule that has fired. Typically this is done because a particular sequence of recognizable and important security events has been detected, and the offense has been named accordingly."
2006-01-25 14:54:20	"CRE Event". CRE Rule description: <Vulnerable Target Exploit Attempt> An attacker is attempting to exploit a local target. The target is known to exist, and the port being attacked is open, and have a vulnerability rating higher than 1.
2006-01-25 14:53:20	SENTRY: The traffic type detected was: 'Suspicious_IP_Protocol_Usage.Unidirectional_ICMP_Reply' from 'Threats', described as 'Flows were detected that were unidirectional ICMP Replies or Unreachables. Ordinarily an amount of this is to be expected. However, if there is an excessive quantity of these flows from a single source, this can indicate that host is scanning the network attempting to enumerate hosts.', fired from QRADAR Sentry 'Excessive unidirectional ICMP Responses detected'
2006-01-25 14:53:20	SENTRY Description: Excessive unidirectional ICMP Responses detected: Excessive unidirectional ICMP Responses from a single source were detected. This can indicate an attempt to enumerate hosts on the network, or can be an indicator of other serious network issues.
2006-01-25 14:52:20	[3] "Defense Perspective Analysis". Multiple devices (not necessarily different device types) reported events related to this offense. Because 3 devices reported events (not just one device) related to this offense, the credibililty of the offense has been raised to reflect added confidence.
2006-01-25 14:52:20	[3] "Defense Perspective Analysis". Multiple different device types (Enterasys Dragon and Snort would be 2 device types) reported events related to this offense. Because 3 different device types reported events (not just one device type, like Snort) related to this offense, the credibility has been raised to reflect added confidence. When more then one different device type reports the same, or related problems, chances lower that this may be a false positive.
2006-01-25 14:50:19	"CRE Event". CRE Rule description: <Exploit/Malware events across multiple targets> A source IP has been detected generating multiple (at least 5) exploit or malware events in the last 5 minutes. These events are not targeting hosts that are vulnerable, and may indicate false positives firing from a device.

Example Asset Profile With Vuln Data

Asset Profile

Name			
Description			
IP Address	10.100.100.16	**VA Risk Level**	0
Operating System	unknown	**How Threatening**	0
Host Name (DNS Name)	10.100.100.16	**How Threatened**	1
Asset Value	0		

Save Changes | Cancel

123	None	Open port	This port was detected open by configured VA scan	1	2006-08-10 13:15:48 (Active)	2006-08-10 13:15:48 (Active)
137	13577	Microsoft Windows NetBIOS Information Disclosure	Microsoft Windows contains a flaw that may lead to an unauthorized information disclosure. The issue is triggered when NetBIOS port 137 (UDP) is open by default, which will disclose sensitive information resulting in a loss of confidentiality.	1	2006-08-10 13:15:48 (Active)	2006-08-10 13:15:48 (Active)
139	None	Open port	This port was detected open by passive real time flow analysis	1	2006-08-10 14:00:00 (Passive)	2006-08-10 13:15:48 (Active)
443	None	Open port	This port was detected open by passive real time flow analysis	1	2006-08-10 11:30:00 (Passive)	2006-08-10 08:00:00 (Passive)
445	343	Multiple Product Version Disclosure	Many applications are designed to reveal their version number, configuration revision number or other such information. While helpful to administrators, this information is often valuable to would-be attackers in carrying out further, more focused attacks.	1	2006-08-10 13:15:48 (Active)	2006-08-10 13:15:00 (Passive)
445	300	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	Microsoft Windows contains a flaw that may lead to an unauthorized information disclosure. The issue is triggered when using the \PIPE\LANMAN transaction pipe, which will disclose lists of neighboring machines resulting in a loss of confidentiality.	1	2006-08-10 13:15:48 (Active)	2006-08-10 13:15:00 (Passive)
901	None	Open port	This port was detected open by configured VA scan	1	2006-08-10 13:15:48 (Active)	2006-08-10 13:15:48 (Active)

Introducing QRadar

- Unique hybrid SIM: correlates security detects (IDS, firewall, auth logs) with behavioral detection (netflow)
- Wide coverage of security devices, vendor-neutral
- Behavioral detection uses network session data (netflow / qflow) with layer 7 detection (app signatures)
- Netflow session data provides an audit trail to support network forensics

Introducing QRadar

- Extreme event correlation ++
- Massive event reduction (1 million low level: 40 high level incidents)
- Sophisticated post-processing; magnitude=credibility * severity * relevance
- Unique tuning capabilities (asset discovery, false positive tools)

Q & A

Craig Chamberlain
Principal Security Consultant
Q1 Labs
craig@q1labs.com
http://www.q1labs.com