Dormant Malware Attacks – What's Next?

Daniel Frye
CedarCrestone, Inc.

Session ID: SP02-108
Session Classification: Advanced

Understanding the APT / dormant malware problem

Reality of APT / Dormant Malware

- The non-scientific definition of ‘advanced persistent threat’ is the same as ‘dormant malware’
  - *“Something’s in the system that’s quiet and malicious”*
- How is this different than any other virus, worm, backdoor, rootkit, Trojan, or malicious employee?
  - *Frankly… it’s not.*

World News

Malware Has Been Lurking on City College of San Francisco System for a Decade

January 16, 2012

Students, faculty, and staff at City College of San Francisco (California) are being urged to change their passwords, refrain from using computers at the school to conduct financial transactions or any activity that requires a password, and check their home computers for infection following the detection of malware on the school's computer system. It appears that at least seven different strains of malware have been on the system for years. The problem was detected in November 2011, when those responsible for monitoring network activity noticed anomalous traffic patterns. An investigation revealed that malware had been stealing data for more than a decade. The compromised information includes banking data.

http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/01/16/BA8T1MQ4E5.DTL

Input / Output

- Change in a ‘system’ relies on two things:
  - Input (I)
  - Output (O)
- Even internally to the ‘system’ we use (I) and (O)
  - Functions(), Procedures() at the code level
  - Queries, data files, network traffic at each successive level
- Theory: If you monitor all things (I) and (O) you can see all things affecting the ‘system’
  - *Corollary: If you see all things affecting the ‘system’ you have perfect intelligence*

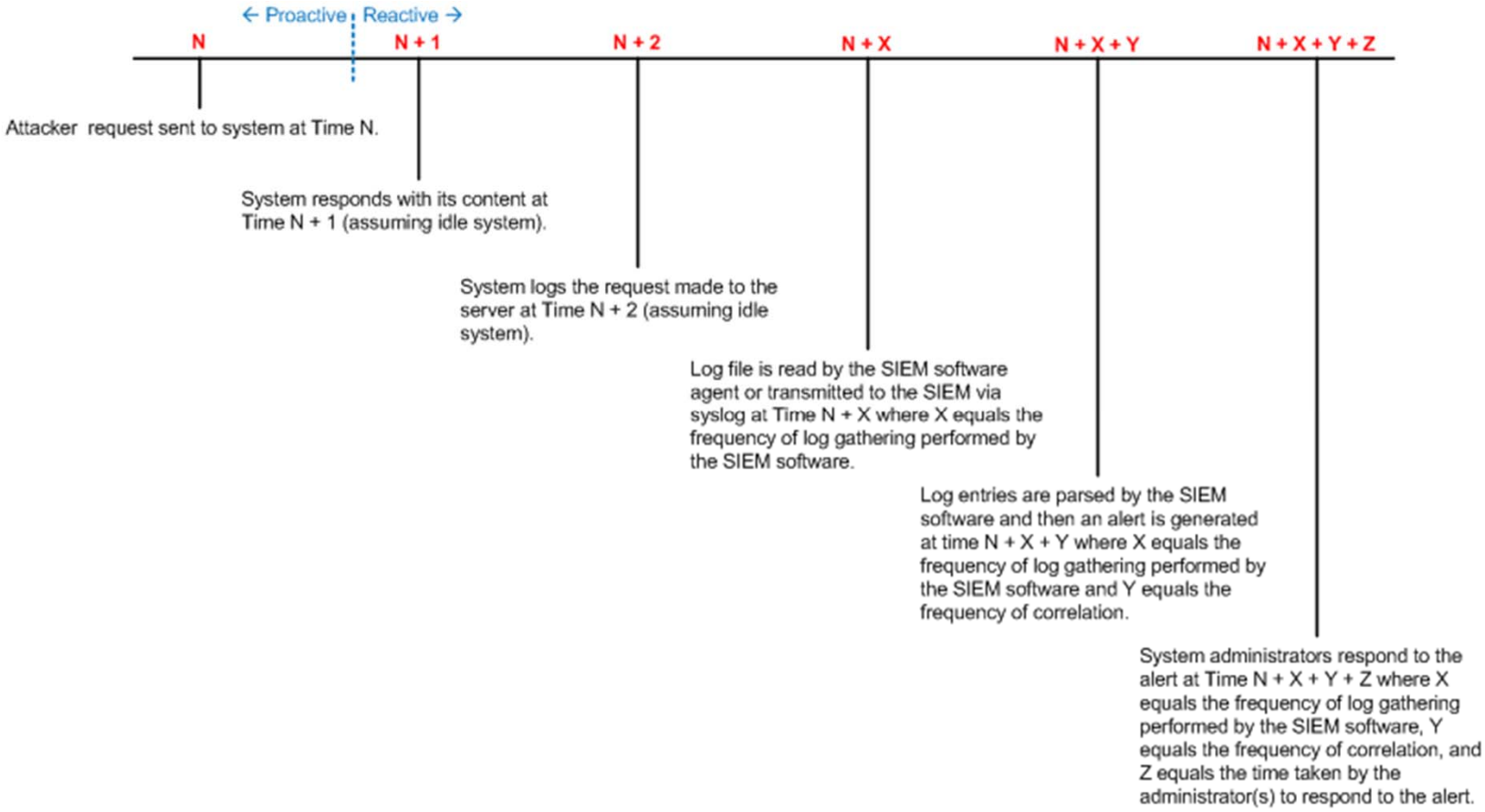
Attack detection

- Attacks are never invisible, but they may be hard to detect
  - Covert channels to C&C servers (network traffic)
  - New listening ports or processes being opened
  - System files modified (checksum)
  - Account modifications (additional rights granted)
- Attackers exploit a box by manipulating the I/O
  - Vulnerable port (worm, TCP/IP flaws, etc)
  - Vulnerable program (XSS, Sql_inj, PDF, etc)
- *Even Zero Days leave footprints somewhere!*

Manipulating Input / Output

- The point at which the attack is successful changes our defense from proactive to reactive
  - Events occur which indicate successful attack(s)
- Significant delays in detection impair response
  - Damage increased
  - Effectiveness of responders reduced
- Delays to response come in many forms
  - System
  - Human

Effects of Correlation Time on Response



Developing your strategy for APT / dormant malware (also known as security)

Using Metrics

- Properly leveraged, metrics can tell you if you're doing better or worse
- Helps with…
  - Budget requests
  - Staffing levels
  - Choosing priorities
  - Finding process issues
  - Training needs
  - Technology issues

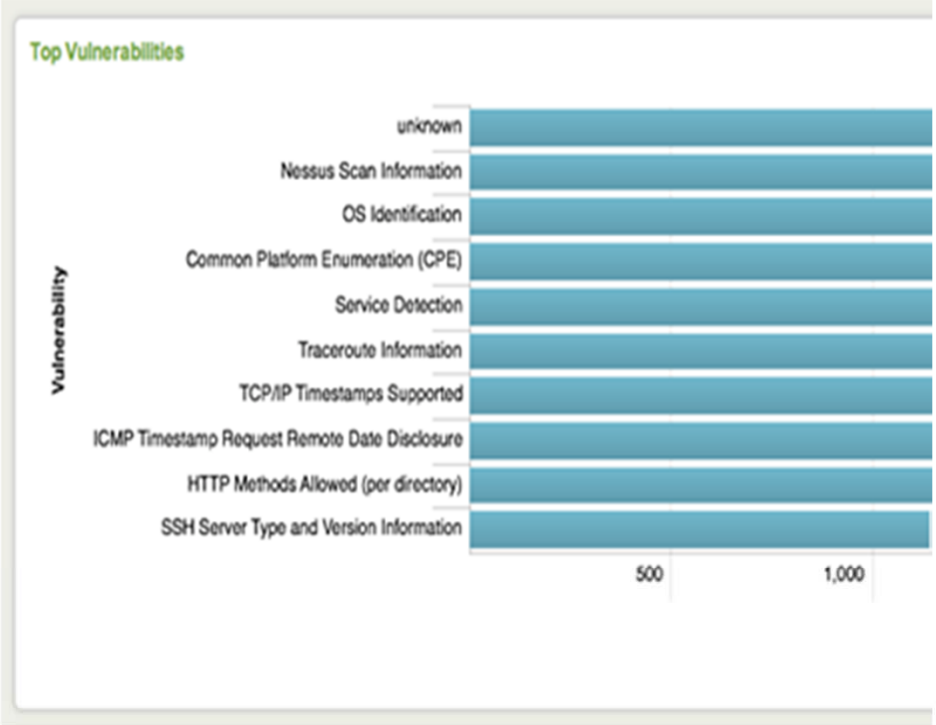
Types of Metrics

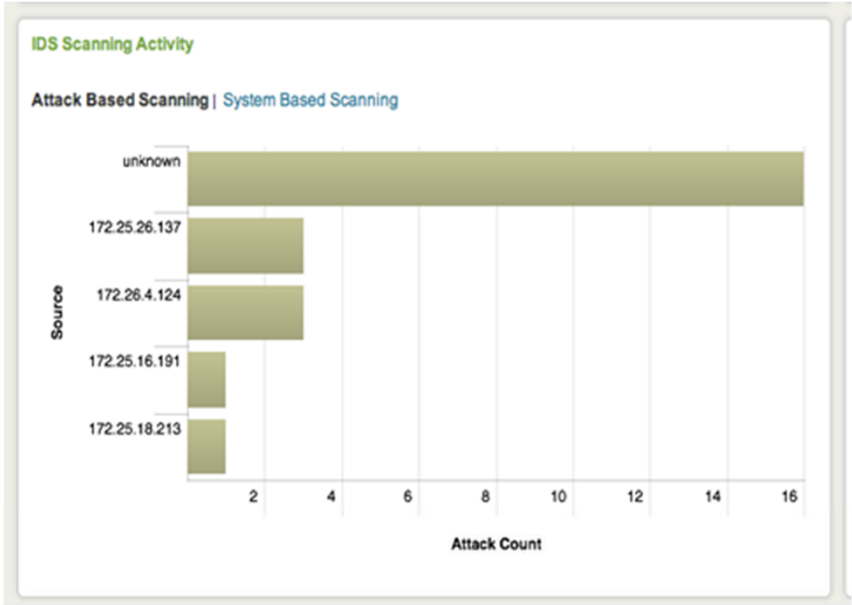
- Two types of Metrics
  - Digital Metrics
    - Discrete, repetitive, efficient measurements
      - Go get Andrew Jaquith's book *Security Metrics*
        - » http://www.amazon.com/Security-Metrics-Replacing-Uncertainty-Doubt/dp/0321349989
  - Analog Metrics
    - Trending, scenarios, probability… ***not*** discrete

"If you're presented with either/or… it's probably both."

Metrics limitations

- Must understand your limitations and the limitations of the system you're measuring!





Using Compliance Initiatives

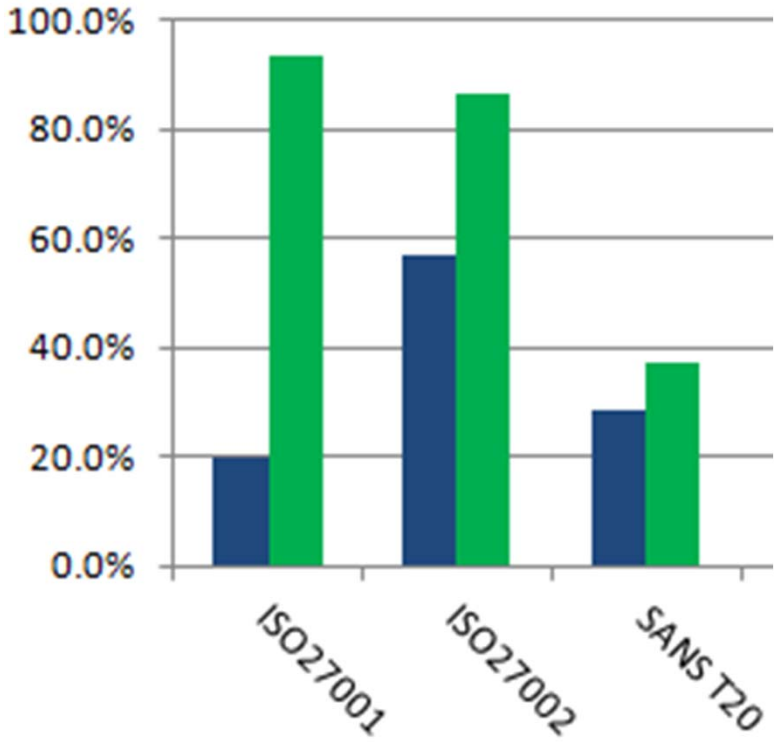
- PCI, HIPAA, ISO27000 series, etc can all be used to define your baseline
  - Not perfect, but can be used as an ‘analog’ metric
- Measure the following:
  - % of controls covered
  - Your ‘gut feeling’ of how effective that control is
  - Number of estimated man hours to implement control
  - Cost of control
- Net result is a SWOT diagram of your ISMS and the building block of your strategy

Sample Strategy Plan Using PCI

	Requirement 10: Track and monitor all access to network resources and cardholder data.	4.0%	88.0%	Total Hours	Security	Unix	Network	WinServer
	Requirement 10: Track and monitor all access to network resources and cardholder data.			3236	886	362	282	282
10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	No	No	72	40	4	4	4
10.2	Implement automated audit trails for all system components to reconstruct the following events:	No	Yes	2750	750	250	250	250
10.2.1	All individual accesses to cardholder data	No	Yes	21	4	2	2	2
10.2.2	All actions taken by any individual with root or administrative privileges	No	Yes	21	4	2	2	2
10.2.3	Access to all audit trails	No	Yes	21	4	2	2	2
10.2.4	Invalid logical access attempts	No	Yes	21	4	2	2	2
10.2.5	Use of identification and authentication mechanisms	No	Yes	21	4	2	2	2
10.2.6	Initialization of the audit logs	No	Yes	21	4	2	2	2
10.2.7	Creation and deletion of system-level objects	No	Yes	21	4	2	2	2
10.3	Record at least the following audit trail entries for all system components for each event:			21	4	2	2	2
10.3.1	User identification	No	Yes	21	4	2	2	2
10.3.2	Type of event	No	Yes	21	4	2	2	2
10.3.3	Date and time	No	Yes	21	4	2	2	2
10.3.4	Success or failure indication	No	Yes	21	4	2	2	2
10.3.5	Origination of event	No	Yes	21	4	2	2	2
10.3.6	Identity or name of affected data, system component, or resource.	No	Yes	21	4	2	2	2
10.4	Synchronize all critical system clocks and times.	Yes	Yes	0	0	0	0	0
10.4.1	Critical systems have the correct and consistent time.	No	Yes	0	0	0	0	0
10.4.2	Time data is protected.	No	Yes	0	0	0	0	0
10.4.3	Time settings are received from industry-accepted time sources.	No	Yes	0	0	0	0	0
10.5	Secure audit trails so they cannot be altered	No	Yes	0	0	0	0	0

Performance of Plan

- Measurements
  - Starting % coverage
  - Current % coverage
- Review increase or decrease per unit of time (month / year) with Executives
- Are we on target?
  - If not, why?



Being Proactive

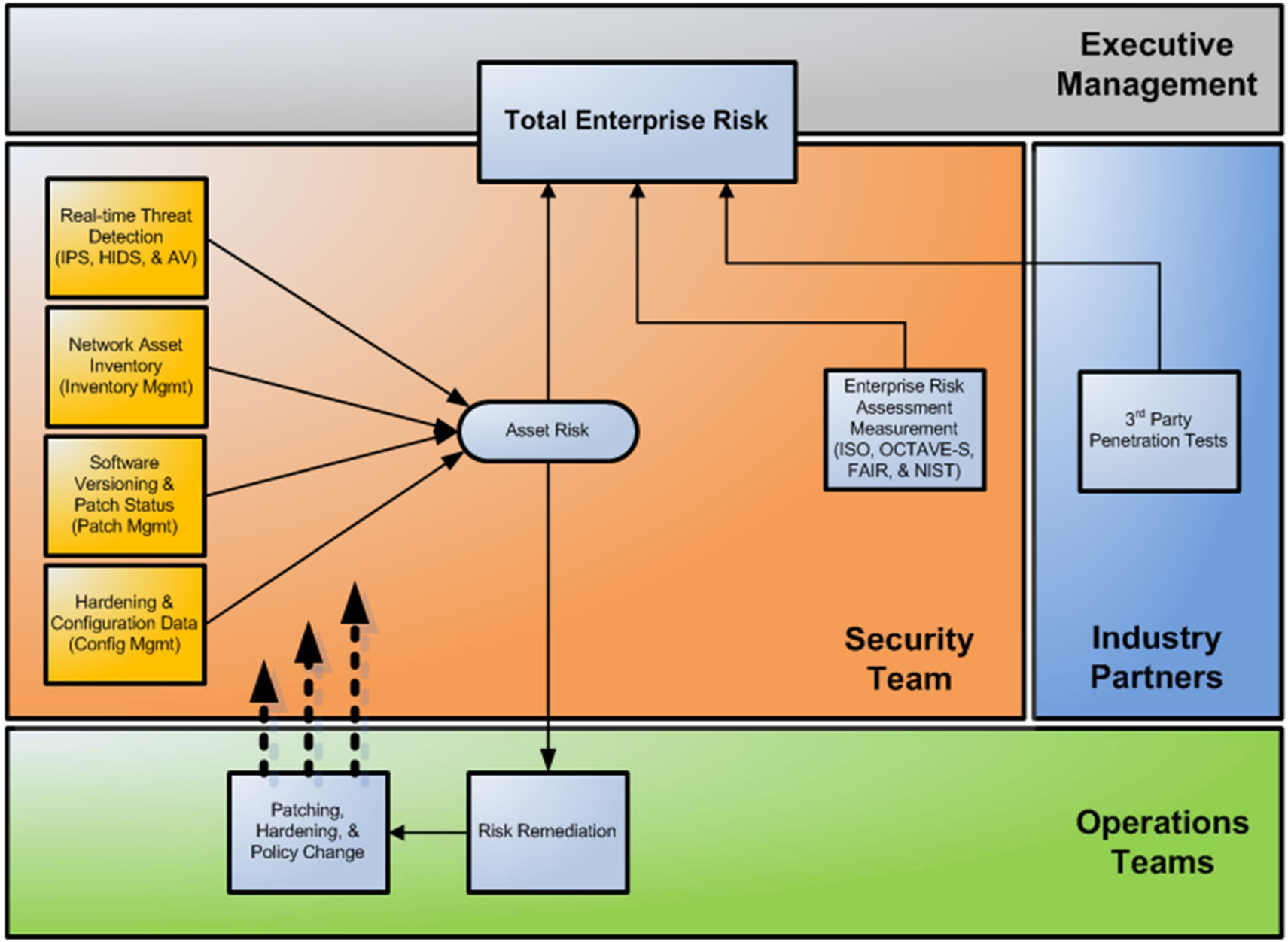
- Risk Assessment != Risk Management
  - What can happen to this ‘system’?
  - What is our “real time”[ish] threat and vulnerability stance?
  - Risk Management is an ongoing proactive process
- We are not all knowing… ask someone else
  - Finding your weaknesses is a “blacklist” approach; *you don’t know what you don’t know!*
  - Properly leveraging penetration testing techniques is a proactive approach to managing risk

Dealing with the Unknown

- The most significant factor of a pentester successfully breaching your security is the skill of the person doing the testing…
- The most significant factor of an attacker successfully breaching your security is the skill of the person doing the attacking…
- Pentesters utilize the same tools / techniques as attackers
  - Results in an evaluation of things we 'don't know'
- If you're not using good testers, you should be!

Automating our Risk Metrics

- Risk broken down into:
  1. Operational Risk
     - Real-time Threats
     - Asset Discovery
     - Patch Management
     - Hardening & Configuration standards
  2. Enterprise Risk
  3. Unknown Risk
- Risk Assessment combined with Operations will "always probably" happen


Executive Management
Total Enterprise Risk
Real-time Threat Detection (IPS, HIDS, & AV)
Network Asset Inventory (Inventory Mgmt)
Software Versioning & Patch Status (Patch Mgmt)
Hardening & Configuration Data (Config Mgmt)
Asset Risk
Enterprise Risk Assessment Measurement (ISO, OCTAVE-S, FAIR, & NIST)
3rd Party Penetration Tests
Security Team
Industry Partners
Patching, Hardening, & Policy Change
Risk Remediation
Operations Teams

In Review…

- We need to detect changes & activity
- We need to measure our processes
- We need a strategy for our ISMS
- We need to evaluate Risk as an ongoing process
- We have to deal with ‘unknowns’ in our ‘system’

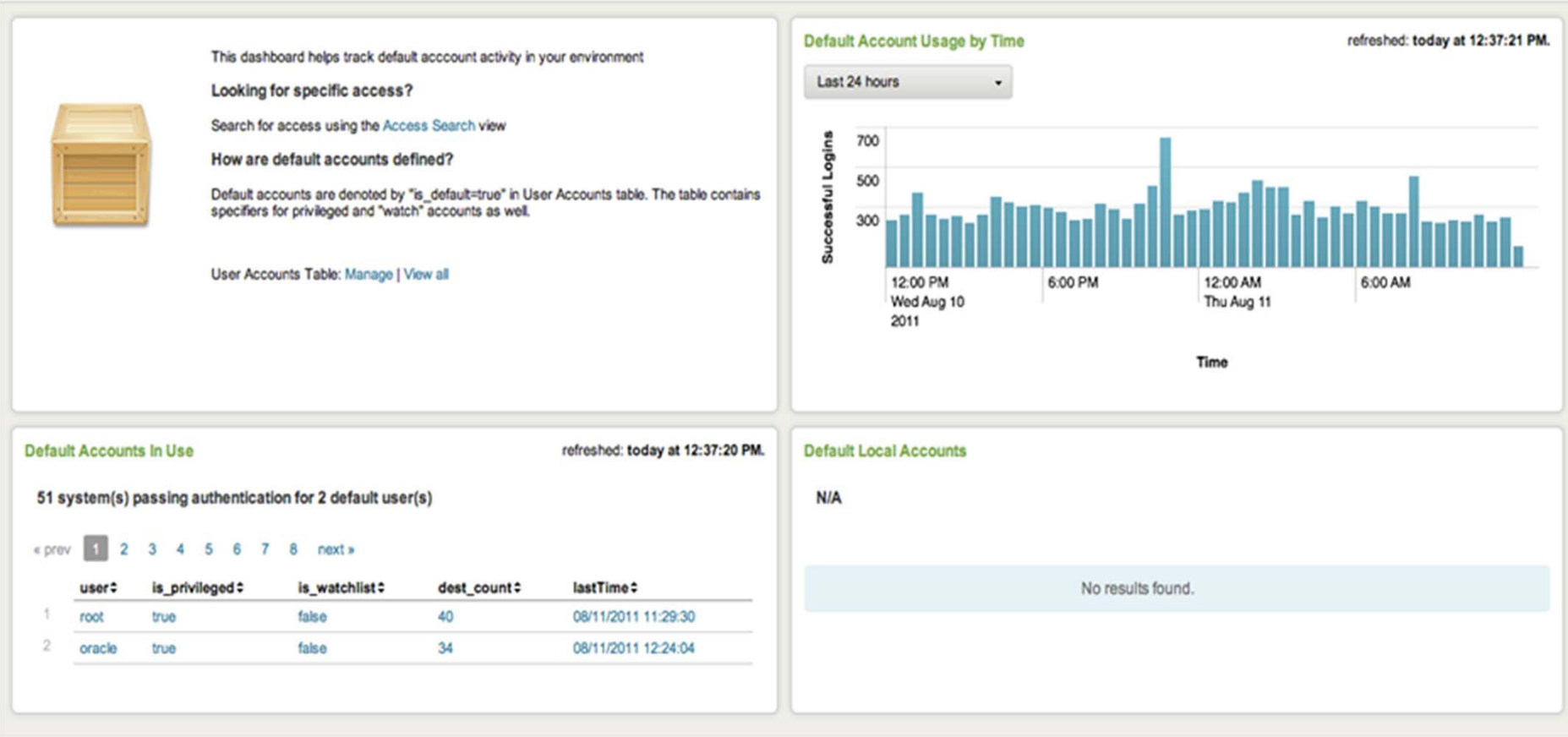
Building the tools we need

Flexibility

- The more complex the process, the more likely a custom solution is required
  - Windows event logs == easy
  - Web application logs from an ERP system == hard
- We need dashboard creation and user modifiable searches, graphs, and reports
  - No “developer” time
  - Every company presents and processes information differently

Default accounts

- These are still active? Really?



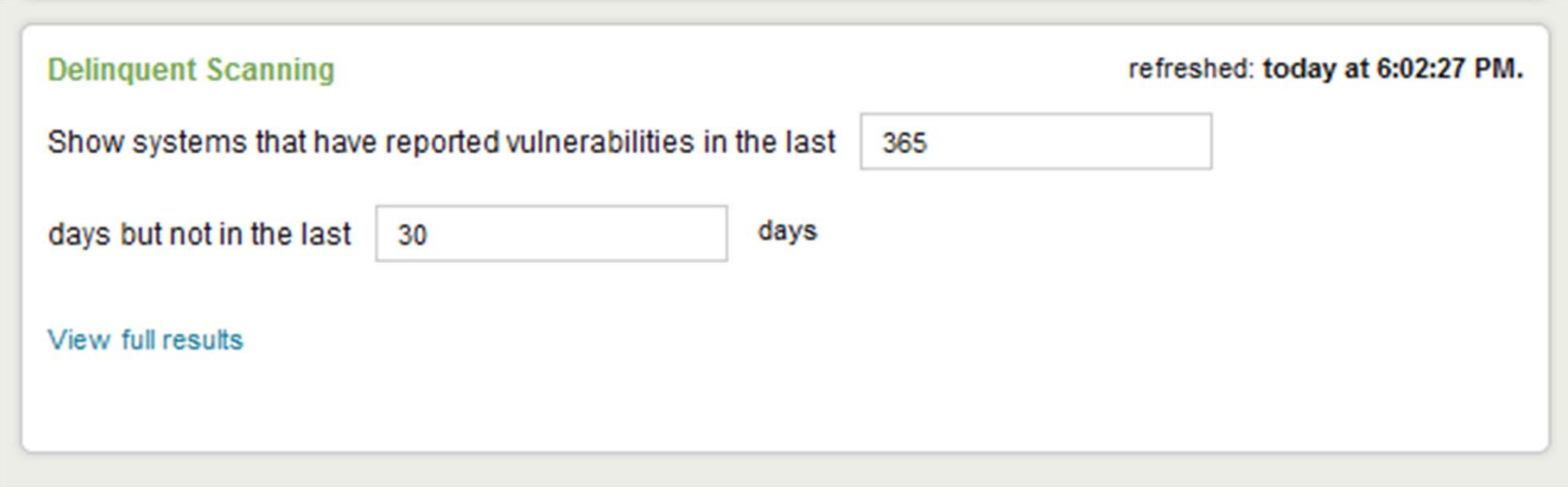
Tracking port activity

- **Monitoring external / internal IP Space**
  - What ports have changed over time?
  - Monitoring for services or ports that were unauthorized or misconfigured
  - Port changes over time to show growing external IP space, i.e. increased “Risk”

8	[redacted]	Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2|Microsoft Windows XP SP2 or SP3	80	tcp	open	http
			443	tcp	open	https
			5414	tcp	open	statusd
			6389	tcp	open	clariion-evr01
			13456	tcp	open	unknown
			60020	tcp	open	unknown
9	[redacted]	Sun Solaris 9 or 10 (SPARC)	21	tcp	open	ftp
			22	tcp	open	ssh
			111	tcp	open	rpcbind
			2049	tcp	open	nfs
			4045	tcp	open	lockd
			6389	tcp	open	clariion-evr01
			8089	tcp	open	unknown
			13722	tcp	open	netbackup
			13782	tcp	open	netbackup
			13783	tcp	open	netbackup
			32774	tcp	open	sometimes-rpc
10	[redacted]	Sun Solaris 9 or 10 (SPARC)	21	tcp	open	ftp
			22	tcp	open	ssh
			111	tcp	open	rpcbind
			4045	tcp	open	lockd
			6389	tcp	open	clariion-evr01
			8089	tcp	open	unknown

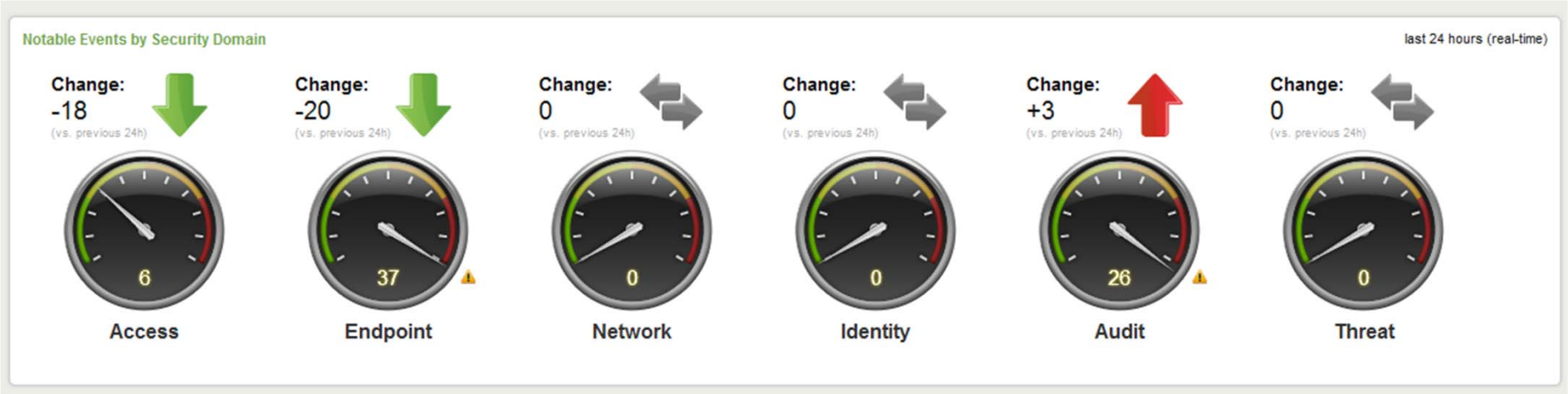
Vulnerability scanning mistakes

- Don’t look at data of what was scanned, but also consider what *wasn’t* scanned

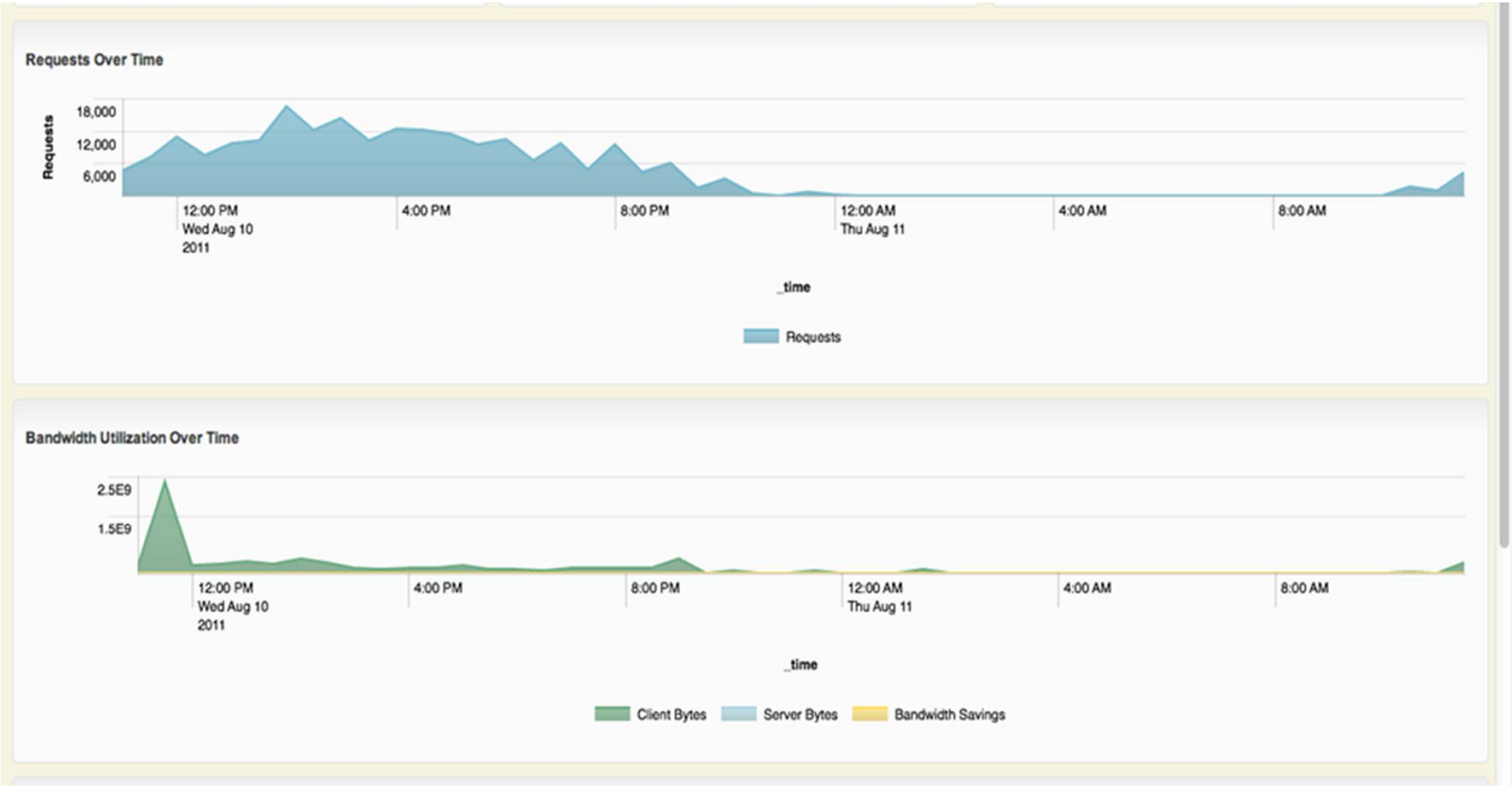


Tracking change of interesting events

- Dashboards used to track increase / decrease of event types
- Gives you ‘at-a-glance’ focus to problem areas



Network anomalies



Non-traditional areas of APT / Dormant malware

Dormant Malware in BYOT

- **Less control of the environment…**
  - Finding unprotected systems (missing A/V, no encryption, no PID scanning tools)
  - Making sure software versions are up-to-date
- **… means more probability of dormancy**
  - Less familiarity with operating patterns
  - Typically less ‘technical know-how’

- **Endpoint tool(s) fed through a ‘security intelligence’ tool can help build these tracking needs into your metrics**

Highly available systems

- **Less time to patch and maintain systems…**
  - SCADA / Water / Energy
  - Telco systems
  - Centrifuges
- **… means more probability of dormancy**
  - If something was infected, now what?

- **Gateway and network tools still carry the same types of traffic so our monitor / intelligence tools are still valid**

Unsupported systems / software

- **When there is no support…**
  - Legacy ERP systems
  - Workstation software which is End-of-Life
  - Test / lab equipment
- **… means more probability of dormancy**
  - More attack surface
  - Less emphasis on monitoring the security of the system

- **Anything on your network can still be a hidden access point for attackers**

Where you go from here

What to think about on the way home

- Look for areas where you traditionally don't have coverage
  - Systems "hiding" on your production network
  - Systems / software no longer under support
  - Systems not routinely connected to your network
- Find ways to measure the security machine; i.e. your *processes*
- 'Dormancy' is a breakdown of your *security processes*
- Security isn't done by just the SOC; give your admin's flexible tools (and data) they can use too

Contact Info / Q&A

Daniel Frye

AVP, Corporate Security

CedarCrestone, Inc.

dan.frye@cedarcrestone.com

Dormant Malware Attacks – What's Next?

Paul Southerington
nTelos Wireless

Session ID: SP02-108
Session Classification: Advanced

RSA CONFERENCE 2012

Perspectives

Perspectives

- IT Assurance perspective
  - Security, Compliance, and Governance
  - then across IT
  - then across the Business
- New malware is part of a broader class of issue
  - Anomaly detection – similar to other areas:
    - Security and Compliance
    - Fraud Detection
    - On-Demand Investigations
  - Trend toward cascading failures

Toolset Challenges

- Multiple use cases
- Heterogeneous, distributed systems
  - Limited visibility across the whole stack
  - Poor consistency in data formats
  - Apps not designed for logging
- Highly dynamic environments
- Scalability/Performance
- Usability

Common Pitfalls

- Inflexible Schemas
  - Traditional DW approaches commit you to early decisions
  - Dependence on vendors for parsing logic
  - Poor support for custom / in-house apps
- Limited Reporting
  - Freedom to ask questions vs. fixed reports
- Poor Integration
  - Overdependence on vendor agents
- Lack of Customization
- Lack of Community

The Evolution of Monitoring

More Questions

- eCommerce
  - Customer logins from reseller IPs?
  - Multiple customers from same IP?
  - Account or voicemail reset attempts?
  - Unusual paths through the app (advanced modeling)
- Who is accessing customer data?
  - Authorized users
  - Third-party fraud monitoring firms
    - *“Who is watching the watchers”*

The Evolution of Monitoring

- Free exploration
- Blacklisting / Event Identification
- Whitelisting
- Trending and Alerting
- Visualization

- Phases may overlap or be skipped altogether

Open Exploration

- Often the starting point
  - Don’t knock it
- Inclusive searching
  - The usual starting point
- Exclusive searching
  - Search for everything
  - Start whittling out the expected
  - Leads into whitelisting

Blacklisting / Event Identification

- Define event types
  - Known events
  - Tag as “good” / “Bad” / “Noise”
- Transactional analysis
  - Roll-up and summarization

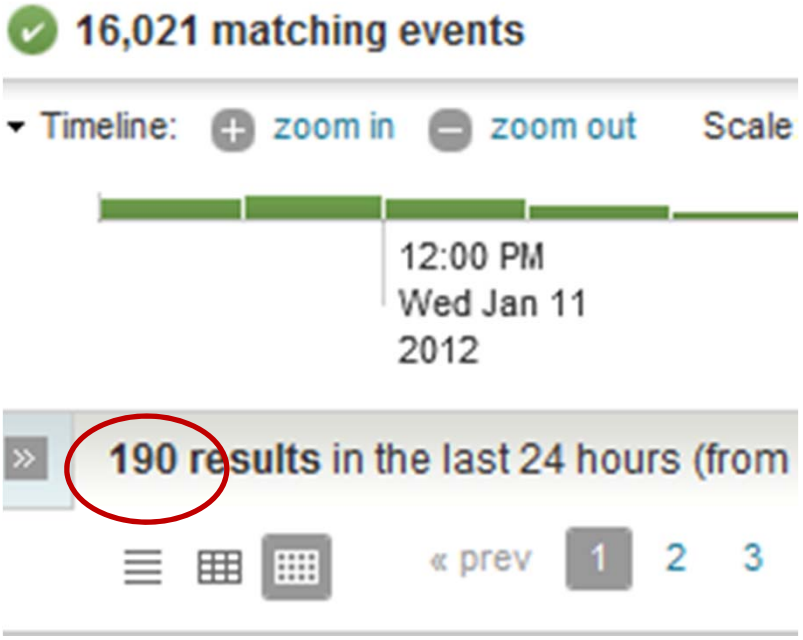
Whitelisting

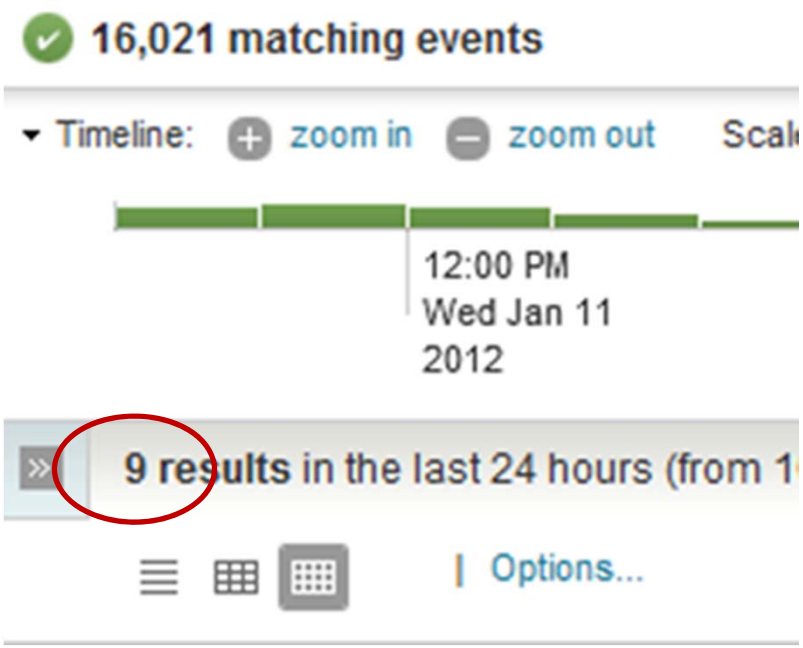
- Sounds simple enough
  - But systems do it poorly or don't scale
- Log everything, monitor "interesting"
- Data reduction :: Better monitoring
- Two broad types
  - Event typing – "The firewall blocked something"
  - Parametric – "Blocked *from X to Y*"

Whitelisting for Data Reduction

```
| stats count by src_ip, dest_ip, dest_port
| lookup ecom-asa-whitelist src_ip,dest_ip,dest_port OUTPUT whitelisted
| where whitelisted=0
```

Last 24 hours >





Trending Metrics

- Start building a metrics database
- Record metrics at least daily
- Define thresholds
  - Report/alert on deviations
- Multiple Levels
  - Fixed cutoff
  - Simple “dashboard”-style trending
  - Statistical tracking

[redacted] Agent Activity | Actions

Previous month

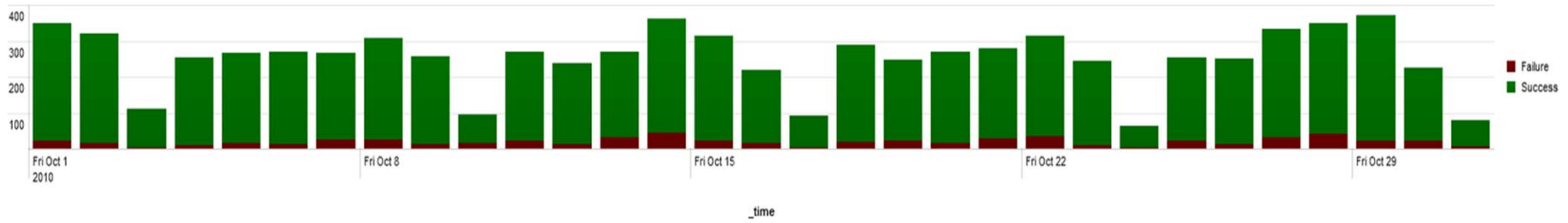
Indirect Login Success:

7,236

Indirect Login Failures:

598

Indirect Agent Login Activity

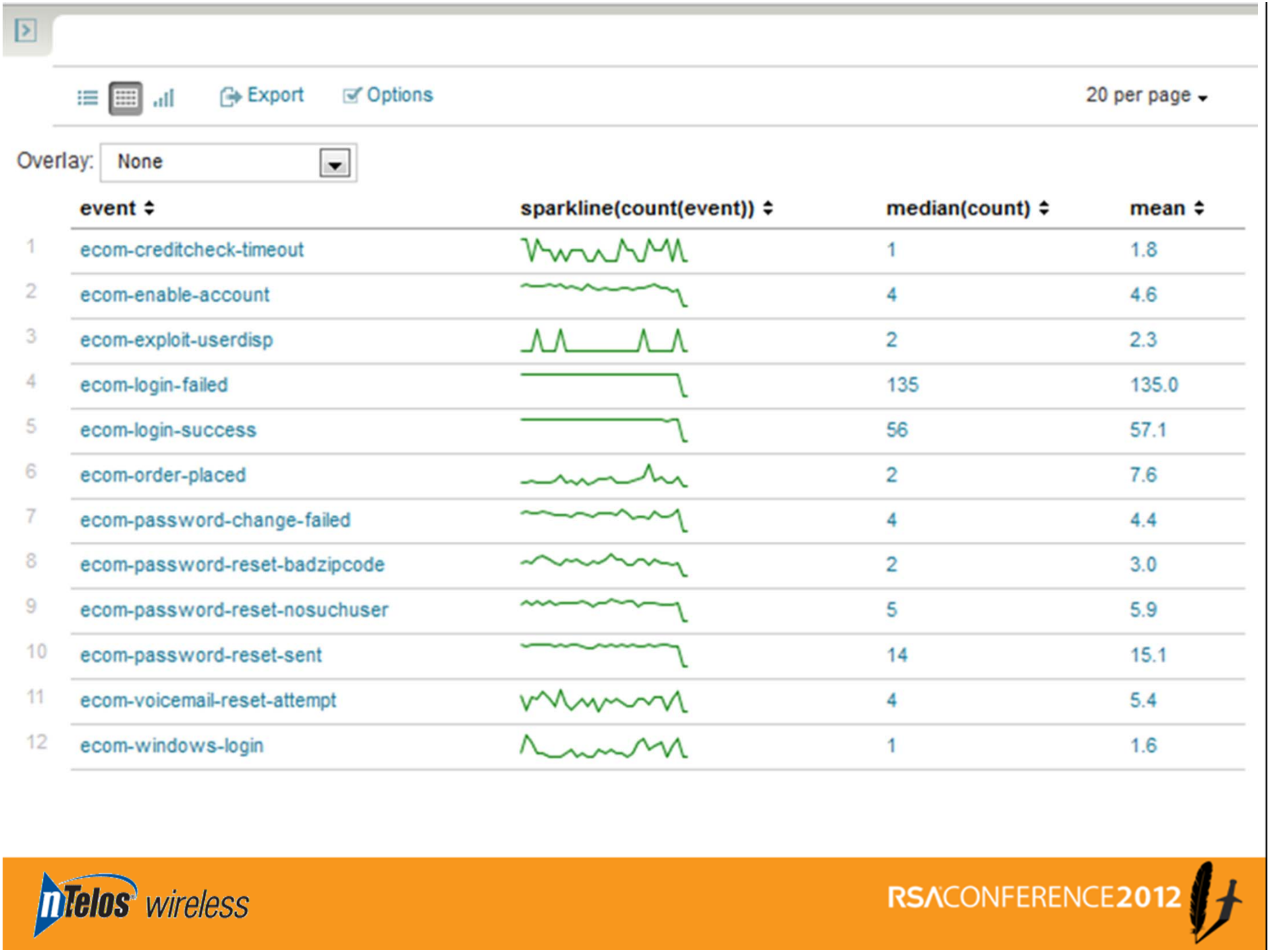


Top 10 Agents Attempting Login

	rits_lname	count	percent
1	[redacted]	371	4.768025
2	[redacted]	337	4.331063
3	[redacted]	262	3.367176
4	[redacted]	253	3.251510
5	[redacted]	225	2.891659
6	[redacted]	209	2.686030
7	[redacted]	197	2.531808
8	[redacted]	185	2.377586
9	[redacted]	163	2.094846
10	[redacted]	159	2.043439

Top 10 Agents With Login Failures

	rits_lname	count	percent
1	[redacted]	28	5.137615
2	[redacted]	27	4.954128
3	[redacted]	23	4.220183
4	[redacted]	23	4.220183
5	[redacted]	21	3.853211
6	[redacted]	21	3.853211
7	[redacted]	20	3.669725
8	[redacted]	20	3.669725
9	[redacted]	17	3.119266
10	[redacted]	16	2.935780



	event	sparkline(count(event))	median(count)	mean
1	ecom-creditcheck-timeout		1	1.8
2	ecom-enable-account		4	4.6
3	ecom-exploit-userdisp		2	2.3
4	ecom-login-failed		135	135.0
5	ecom-login-success		56	57.1
6	ecom-order-placed		2	7.6
7	ecom-password-change-failed		4	4.4
8	ecom-password-reset-badzipcode		2	3.0
9	ecom-password-reset-nosuchuser		5	5.9
10	ecom-password-reset-sent		14	15.1
11	ecom-voicemail-reset-attempt		4	5.4
12	ecom-windows-login		1	1.6

Trending Metrics – Statistical Tracking

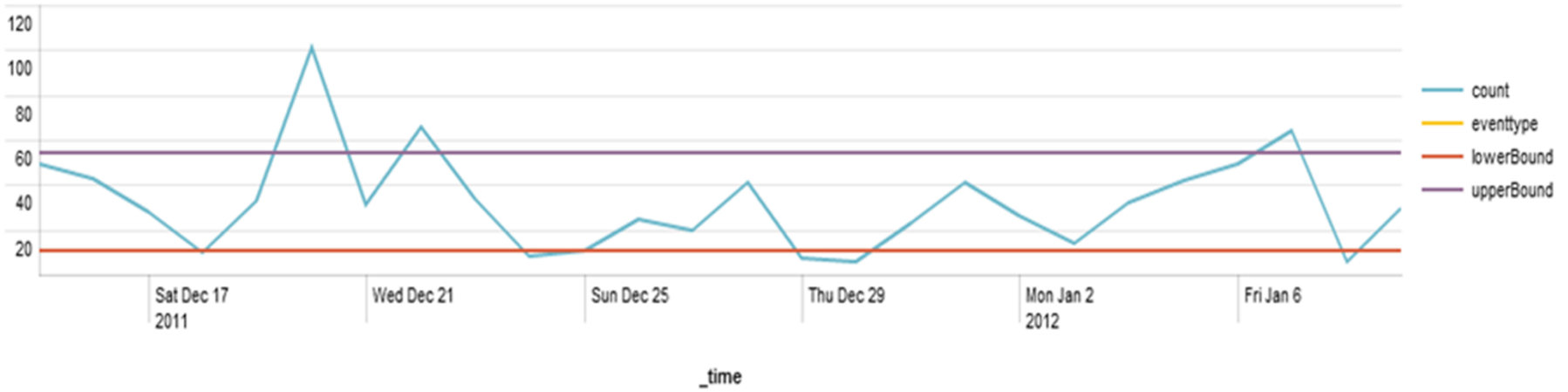
- Basic thresholds
  - *Does an event occur more than 0 times?*
- Relative thresholds
  - *... occur more than twice as often as yesterday?*
  - *... occur unusually based on another, related metric*
- Statistical modeling
  - *… more then X std. deviations from mean?*
  - *… more than X above the running average?*
    - *simple moving average*
    - *exponential averaging – give greater weight to recent data*
  - Do correlated events stay correlated?

Eventtype Trending | Actions

Eventtype: ecom-voicemail-reset-attempt

Analysis Type: 1x Standard Deviation Bounds

Last 30 days >



All Values

View:

All Values | Outlying Values | **High Values** | Low Values

	_time	count	eventtype	lowerBound	upperBound
1	12/20/11 12:00:00.000 AM	101	ecom-voicemail-reset-attempt	10.364549	54.250835
2	12/22/11 12:00:00.000 AM	66	ecom-voicemail-reset-attempt	10.364549	54.250835
3	1/7/12 12:00:00.000 AM	64	ecom-voicemail-reset-attempt	10.364549	54.250835

View full results

A Compound, Relative Metric

- Summary alert if
  - More than 30% of login attempts failed,
  - or logins came from more than one source IP

Subject: RITS - Indirects by distinct IPs

Name: RITS - Indirects by distinct IPs

Query Terms: sourcetype=rits rits_user=000* | eval success=if(action="Success", 1, 0) | stats distinct_count(src_ip) as ipCount, sum(success) as Successes, count as Attempts by rits_user, rits_lname, rits_fname | eval Failures=Attempts-Successes | eval failPercentage=(Failures/Attempts) | search ipcount>1 OR failPercentage>0.3 | sort -ipCount, -failPercentage | fields rits_user, rits_lname, rits_fname, ipCount, Successes, Failures

Link to results: https://splunk.ntelos.com:443/app/search/@go?sid=scheduler__nobody__search_UklUUyAtIEluZGlyZWN0cyBieSBkaXN0aW5jdCBJUHM_at_1288756800_597688622

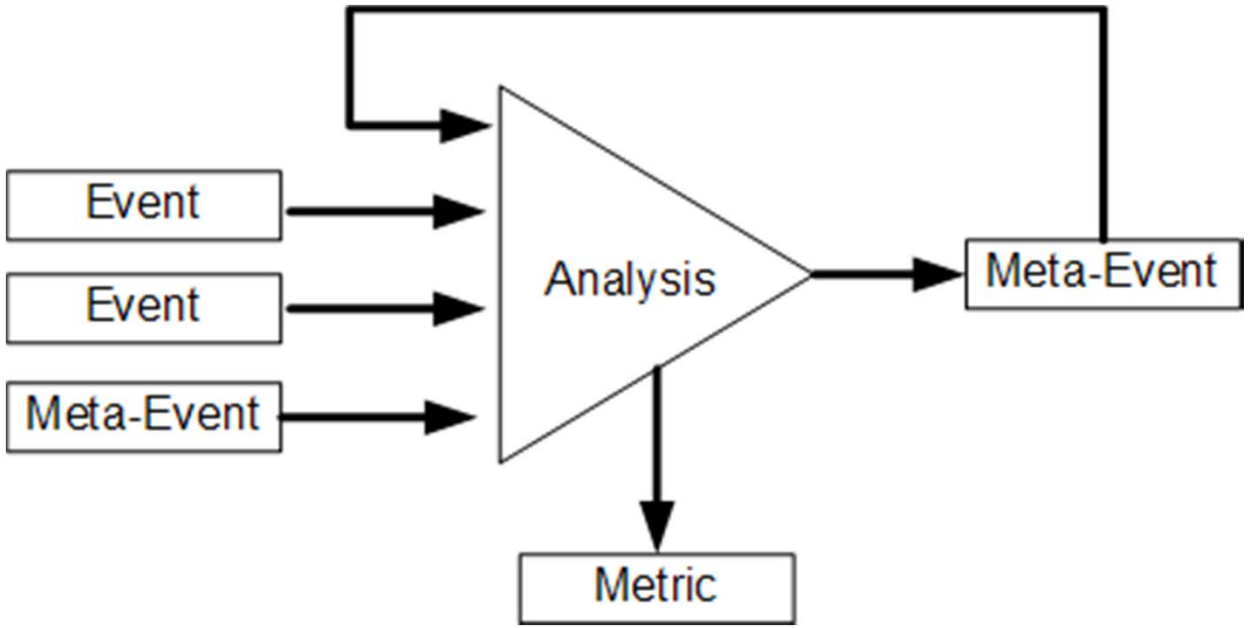
Alert trigger: Saved Search [RITS - Indirects by distinct IPs]: always(11)

rits_user	rits_lname	rits_fname	ipCount	Successes	Failures
	Excel Wireless - Jefferson Davis	Agent	3	9	4
	VISION MOBILE - WYTHEVILLE	Agent	2	6	5
			2	2	1
			1	1	2
			1	1	1
			1	2	2
			1	1	1
			1	2	1
			1	2	1
			1	2	1
			1	2	1

```
…
| eval failPercentage=(Failures/Attempts)
| search ipcount>1 OR failPercentage>0.3
| sort -ipCount, -failPercentage
…
```

Compound/Feedback Metrics

- Search/post-process to generate “meta-events”
- Traditional S[IE]M approach
- BUT – extend over multiple iterations



Correlation Metrics

- Build a correlation matrix
  - Compare each metric to every other metric
- Look for highly correlated metrics
- Monitor these for changes

Multi-Tiered Metrics

- Track multiple levels of the same type of activity
- Structure your metrics database accordingly

- Example:
  - Login Attempts
    - Login Attempts by User
      - Attempts by user and server
        - » Attempts by user / server / source IP

Data Augmentation

More Questions

- Malware
  - Are alerts legitimate?
  - Do alerts get proper follow-up?
- eCommerce
  - Customer logins from reseller IPs?
  - Multiple customers from same IP?
  - Account or voicemail reset attempts?
  - Unusual paths through the app (advanced modeling)

More Questions

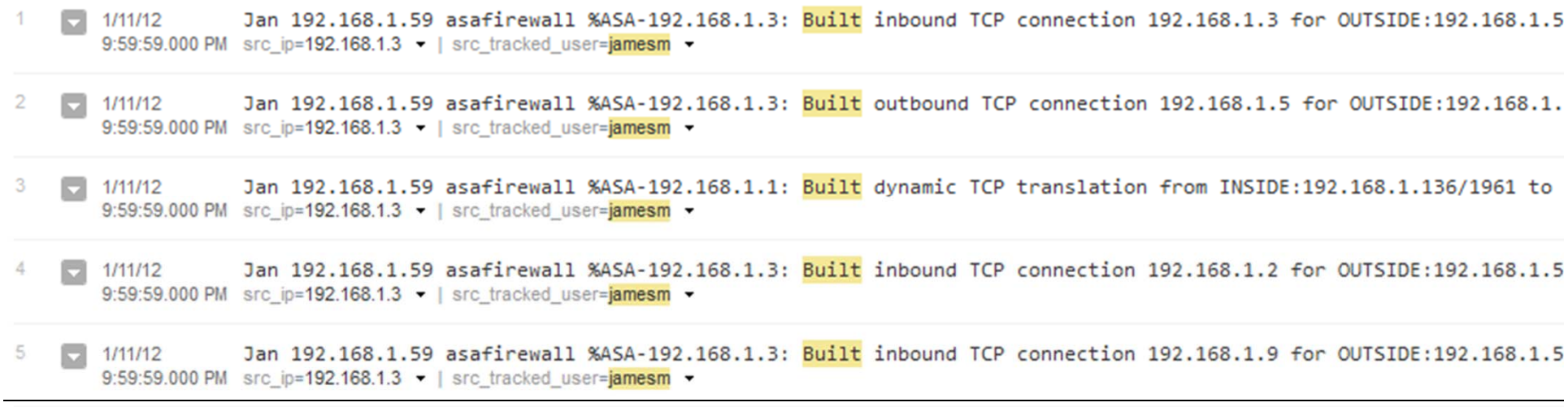
- Fraud prevention
  - Who is accessing customer data?
    - Authorized users?
    - Third-party fraud monitoring firms?
    - *“Who is watching the watchers”*

Augmenting Event Knowledge

- Correlate across data sources
  - Building meta-events
  - *e.g.,FireEye -> Antivirus -> IDS -> Firewall…*
- Bring related information in as soon as possible
  - *What user did that IP belong to?*
  - *File Integrity Monitor – new hash == malware?*
- Develop integrated workflows
  - More visibility for first responders

Example: User-to-IP bindings

- Audit trails often show IP address
  - Investigators usually want a user name
- Track information from other data sources
- Map the results in automatically



Correlating Across Devices

- Are malware alerts getting follow-up?
  - Antivirus log + Antivirus log + IDS + helpdesk
    - *If FireEye detects a potential infection, did A/V stop it?*
    - *Did IDS detect unusual traffic from the machine?*
    - *Was there a helpdesk ticket opened?*
- Change Management
  - Are system changes being approved?
  - Are people changing what they say they are?
  - CMDB + File Integrity Monitor + Change Control
- These are feedback metrics

Source IP

[redacted].44.134

Last 4 hours

Search

Results

Select a view:

Firewall Configuration | Recent Firewall Changes | Perimeter Firewall Hits | ISA Server Hits | RITS Login Attempts

If this tab shows "Not Present", then the Agent either did not exist in the firewall the last time Splunk checked. Check the next tab to see whether the agent has been added recently.

If this tab shows "Present", then the agent does not need to be added. Check the later tabs to see if the agent has tried to connect through the firewall, and whether RITS is seeing failed logins.

If this tab shows "Invalid", then the agent has given an incorrect IP address. Usually this occurs when an indirect rep has connected to the corporate LAN over VPN, or whe the agent provides an internal IP address such as 192.168.xx.xx. Have the agent visit whatismyip.com from a store computer to get the correct address.

Present

Configuration Last Refreshed: 09/01/2011 13:34:45.0

Source IP

[redacted].44.134

Last 4 hours

Search

Results

Select a view:

Firewall Configuration | **Recent Firewall Changes** | Perimeter Firewall Hits | ISA Server Hits | RITS Login Attempts

This tab lists recent configuration changes to the firewall that match the specified IP address. You can use this page to determine whether the IP address has been added since the last time Splunk's list of allowed IP addresses was updated.

No matching events found.

Source IP

[redacted].44.134

Last 4 hours

Search

Results

Select a view:

Firewall Configuration | Recent Firewall Changes | **Perimeter Firewall Hits** | ISA Server Hits | RITS Login Attempts

This tab lists recent firewall log entries matching the specified IP address. "Built" or "Permitted" entries indicate that agent successfully passed packets through the firewall.

All valid connection attempts will be on dest_port 443. Denied connection attempts on port 80 indicate that the agent is using an incorrect URL.

« prev 1 2 3 4 5 6 7 8 9 10 next »

	_time	action	protocol	src_ip	src_port	dest_ip	dest_port	dest_service	access_group
1	1/17/12 9:20:05.000 PM	Deny	icmp	[redacted]4.134		[redacted]			OUTSIDE-IN
2	1/17/12 9:19:56.000 PM	Deny	icmp	[redacted]134		[redacted]			OUTSIDE-IN
3	1/17/12 9:19:51.000 PM	Deny	icmp	[redacted]44.134		[redacted]			OUTSIDE-IN
4	1/17/12 9:19:46.000 PM	Deny	icmp	[redacted].44.134		[redacted]			OUTSIDE-IN
5	1/17/12 9:19:46.000 PM	Deny	icmp	[redacted].44.134		[redacted]			OUTSIDE-IN
6	1/17/12 9:19:46.000 PM	Deny	icmp	[redacted]44.134		[redacted]			OUTSIDE-IN
7	1/17/12 9:17:32.000 PM	Built	tcp	[redacted]4.134	45652	[redacted]	443	https	
8	1/17/12 9:17:32.000 PM	Built	tcp	[redacted]44.134	45651	[redacted]	443	https	
9	1/17/12 9:17:32.000 PM	Built	tcp	[redacted]44.134	45650	[redacted]	443	https	
10	1/17/12 9:17:31.000 PM	Built	tcp	[redacted]44.134	45649	[redacted]	443	https	

Source IP

[redacted].44.134

Last 4 hours

Search

Results

Select a view:

Firewall Configuration | Recent Firewall Changes | Perimeter Firewall Hits | ISA Server Hits | **RITS Login Attempts**

This tab lists login attempts against the RITS Web server from the specified IP address. If any entries are seen here, then network connectivity and firewall configurations are correct.

Failures that appear here may indicate a disabled agent account, or incorrect login credentials.

	_time	action	src_ip	dest_host	rits_user	rits_fname	rits_lname
1	1/17/12 8:57:28.000 PM	Success	[redacted].44.134	WL[redacted]	[redacted]	Agent	[redacted]

Closing Remarks

General Approach

- Focus on the overall monitoring problem
  - Move beyond simple blacklisting and reporting
- Start building a metrics database
- Integrate/Correlate all of your data sources
- Explore visualization options

Contact Info / Q&A

Paul Southerington

Senior Security Engineer

nTelos Wireless

souther@gmail.com

Dormant Malware Attacks – What's Next?

Paul Southerington
nTelos Wireless

Session ID: SP02-108
Session Classification: Advanced

RSA CONFERENCE 2012

Spare Slides

Basic Visualization

splunk> Splunk for OSSEC

App | Manager | Alerts | Jobs | Logout

Search | Dashboards & Views | Searches & Reports | Agent Management | Help | About

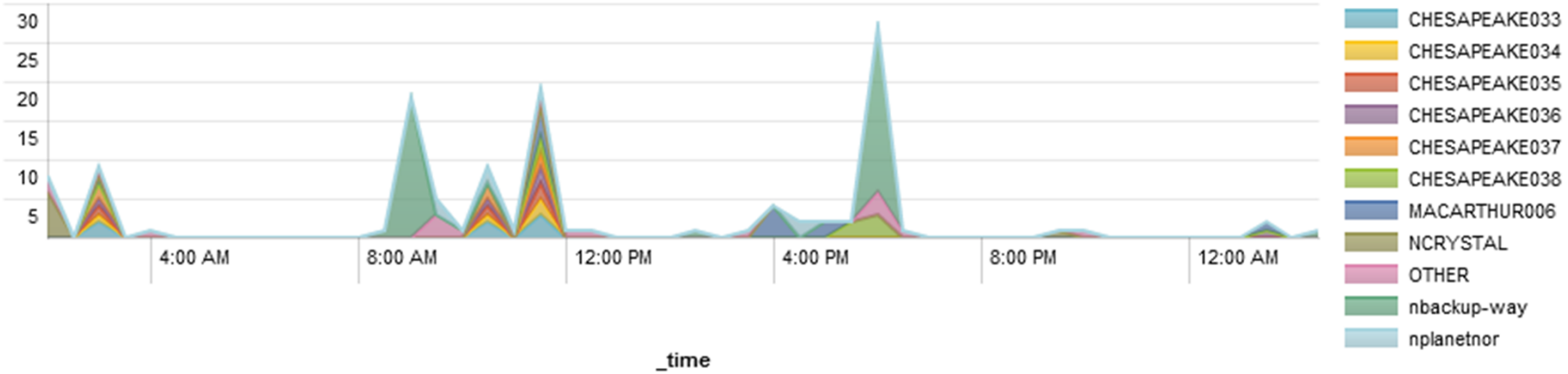
OSSEC File Integrity | Actions

Changes Over Time (By Host)

4m ago

View:

Changes Over Time (By Host)



All Changes

4m ago

All Changes | Filesystem Changes | Windows Registry Changes

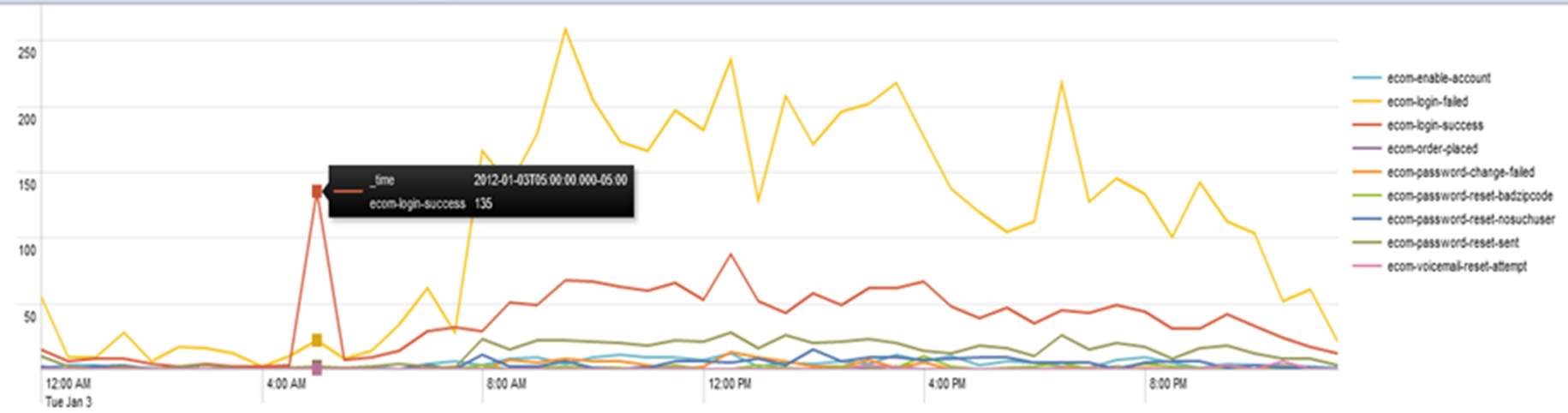
« prev 1 2 3 4 next »

	_time	reporting_host	file_dirname
1	2/15/12 1:46:17.000 AM	MACARTHUR006	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class\{4D36E96C-E325-11CE-BFC1-08002BE10318}\0000\GlobalSettings\R
2	2/14/12 6:34:14.000 PM	377144-splfwd1	HKEY_LOCAL_MACHINE\Software\Classes\Installer\UpgradeCodes\
3	2/14/12 6:28:49.000 PM	HARBOURVIEWMGR	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\SessionData\
4	2/14/12 6:22:41.000 PM	nicky	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\

eCommerce Security Overview - Search ...

ntelos.com https:/[redacted]

Google



Voicemail Passcode Reset Attempts

	_time	src_ip	user	mdn	attempts	src_ip_city	src_ip_region_name	src_ip_country_code
1	1/3/12 10:42:29.000 PM	184.52.230.32	[redacted]	304[redacted]	6			US
2	1/3/12 9:31:37.000 PM	24.154.150.145	[redacted]yahoo.com	740-[redacted]	3	South Point	OH	US
3	1/3/12 3:33:30.000 PM	76.7.50.140			1	Ridgeway	VA	US
4	1/3/12 3:08:07.000 PM	76.3.243.122	[redacted]hotmail.com	434-[redacted]	3	Palmyra	VA	US
5	1/3/12 11:40:06.000 AM	64.4.98.145	[redacted]@yahoo.com	540[redacted]	1	Covington	VA	US

View full results

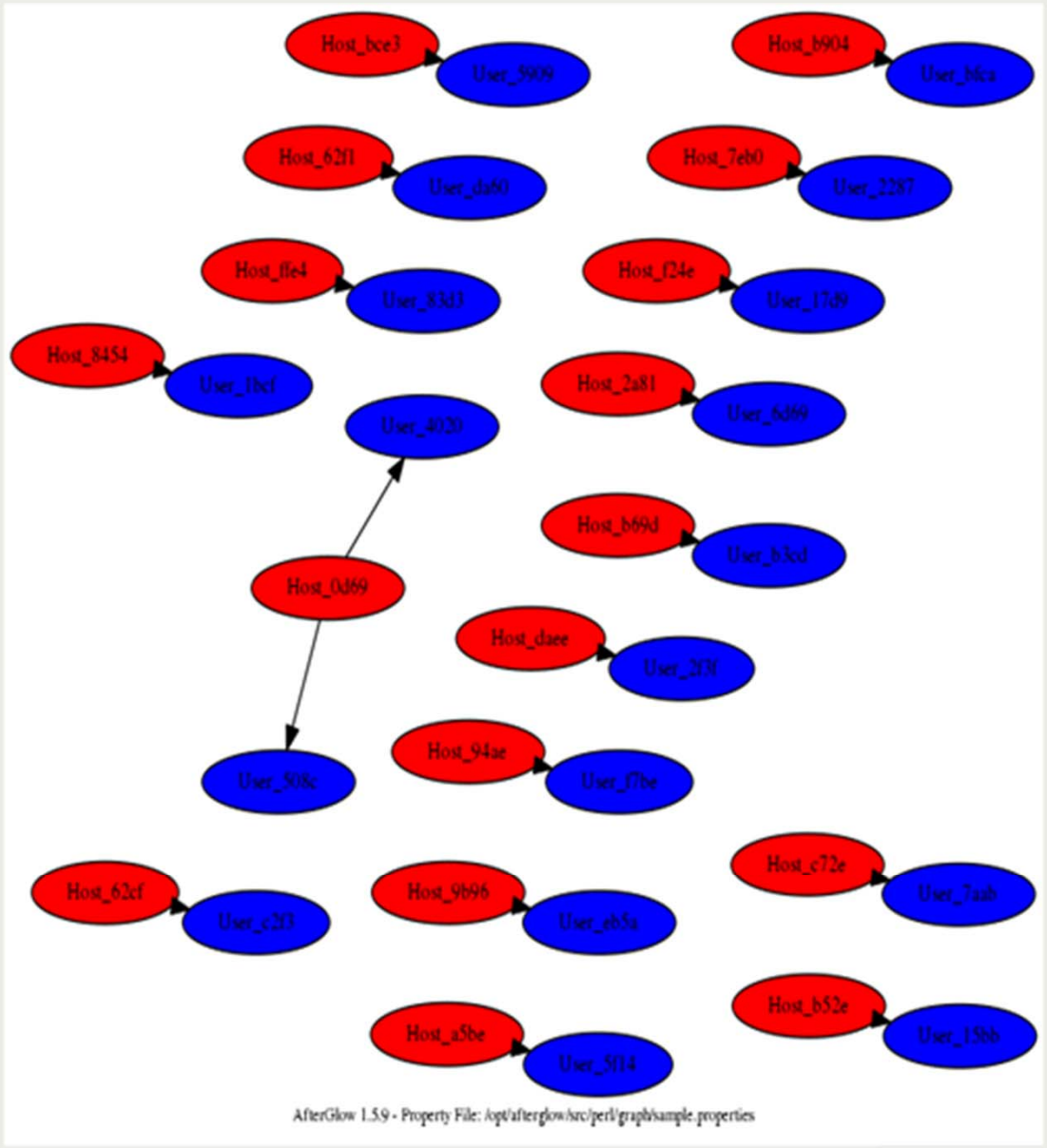
WAF Alerts

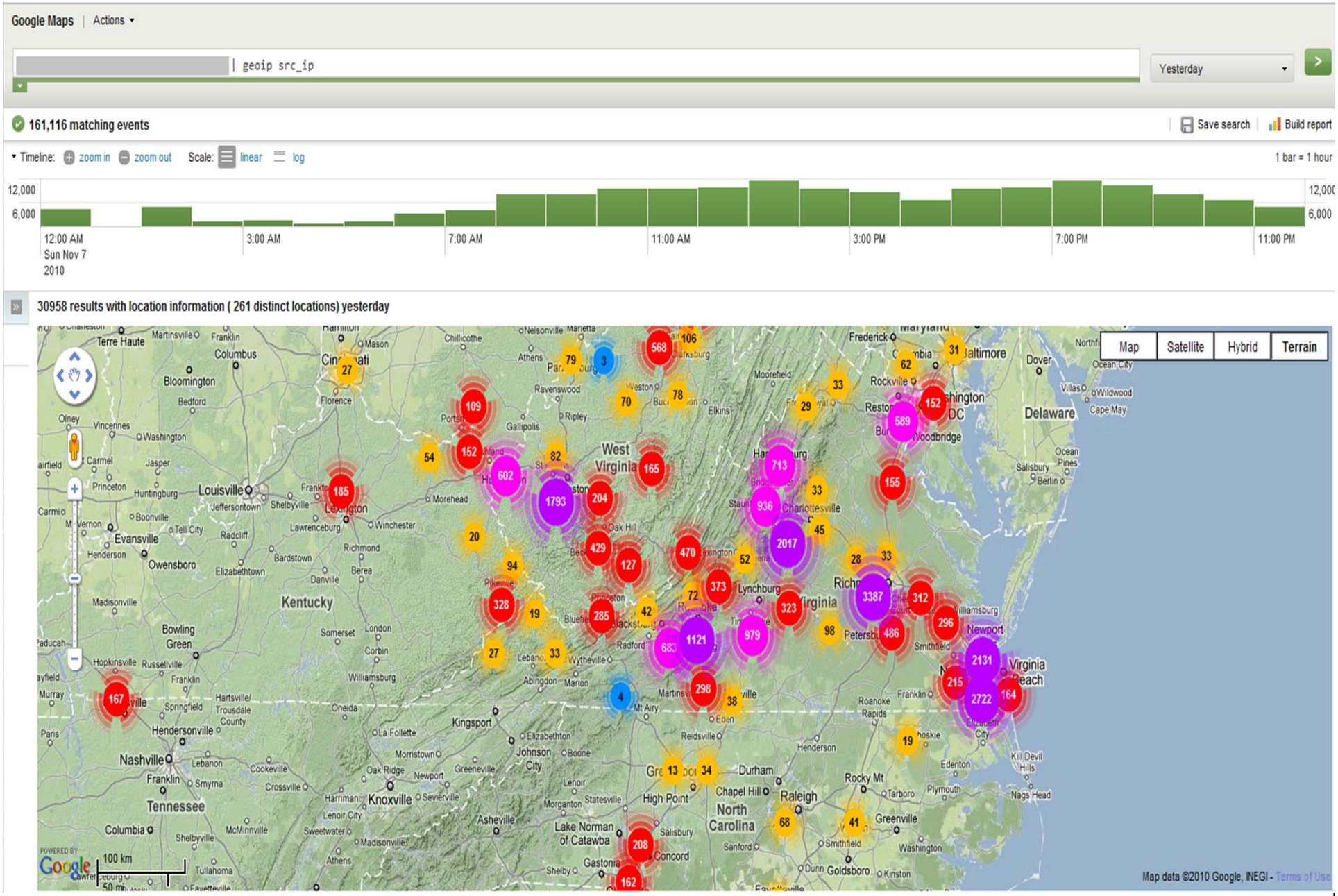
« prev 1 2 3 4 5 6 7 8 9 10 next »

	_time	src_ip	src_tracked_user	action	severity	vuln_name	vuln_detail
1	1/3/12 10:46:41.000 PM	70.32.207.204		Block	High	URL is Above Root Directory	URL is Above Root Directory www.frawgwireless.com/../images/3-points.jpg
2	1/3/12 10:21:38.000 PM	94.23.237.34		Block	High	Signature Violation	EXPDB-17602:WordPress-TimThumb-Plugin-RCE
3	1/3/12 10:21:38.000 PM	94.23.237.34		Block	High	Signature Violation	EXPDB-17602:WordPress-TimThumb-Plugin-RCE
4	1/3/12 10:19:29.000 PM	76.10.214.75		Block	High	Signature Violation	EXPDB-17602:WordPress-TimThumb-Plugin-RCE

882 matching events

Create alert Add to dashboard





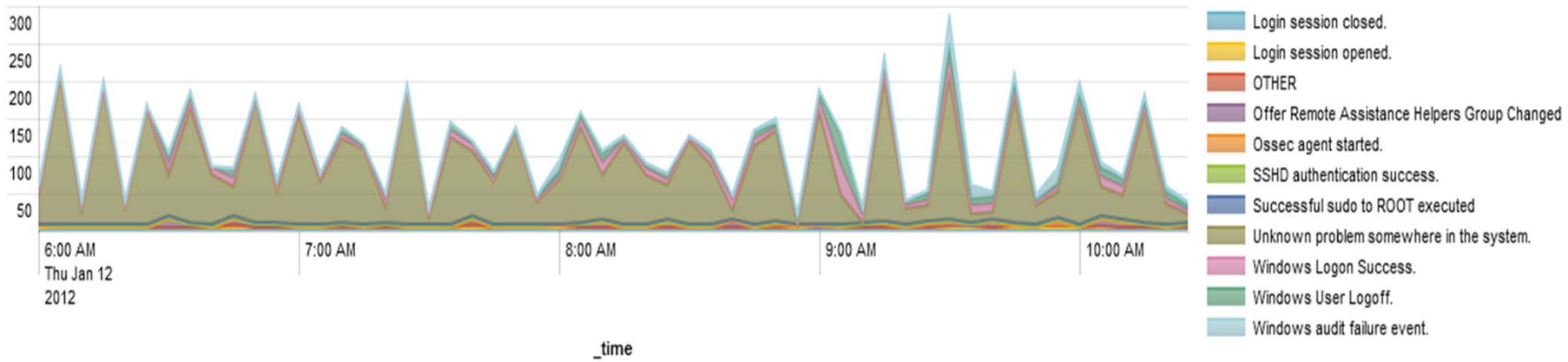
OSSEC Dashboard | Actions

OSSEC Server

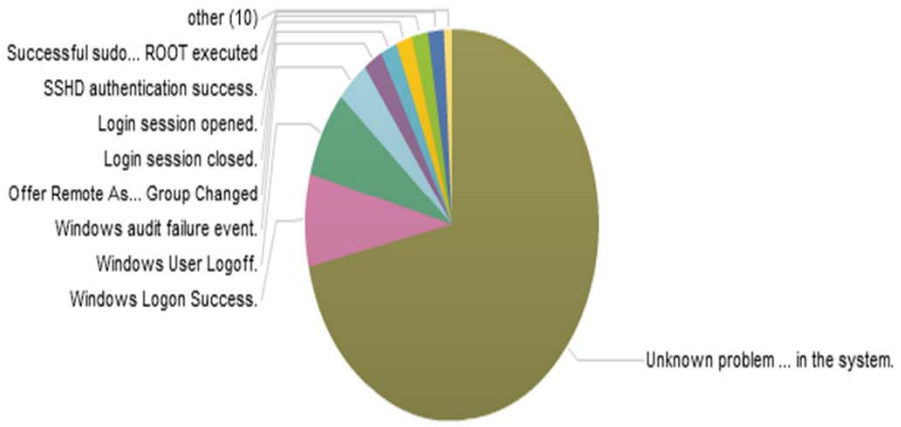
All OSSEC Servers

Last 4 hours

OSSEC - Top Signatures Over Time



OSSEC - Top Signatures



View more results

	signature	count
1	Unknown problem somewhere in the system.	4327
2	Windows Logon Success.	466
3	Windows User Logoff.	434
4	Windows audit failure event.	213
5	Offer Remote Assistance Helpers Group Changed	128
6	Login session closed.	108
7	Login session opened.	108
8	SSHD authentication success.	108
9	Successful sudo to ROOT executed	108
10	Ossec agent started.	14