Guy Bruneau, GSE

LOG, LOG, LOG EVERYTHING REMOTELY

About Me

- Senior Security Consultant @ipss inc.
- Incident Handler @Internet Storm Center
  - gbruneau@isc.sans.edu
- SIEM user since 2001, IDS before that
- Mid to large enterprises
-  @GuyBruneau

Agenda

- Why collect logs and/or packets?
- How much can I trust my equipment?
- Collection, detection and reporting
- Some logging devices
  - Open Source (free)
  - Commercial

Network Forensics – What & Why?

- Defined as analysis of network traffic or network events
- Accuracy requires collecting everything, well almost
- Without accurate logs, incident response is difficult
- Almost impossible to assess real impact
- Packet collection enhances incident resolution

How Good Is My Equipment?

- NSS Labs testing shows 98.5% effectiveness
  - IPS, NGFW, endpoint protection system
  - 1.5% bypass perimeter and host layer defenses
  - Stealthy attacks give control to malicious actors
- Suggest: Control the attacker by redirecting the attack against a target you can watch and control
- Reality: Catch what you can detect and block
- Are you prepared to operate at 60% capacity?
  - Withstand a breach, with reduced services
  - Example: Home Depot, JP Morgan Chase

Collect & Centralize Logs - Challenges

- Voluminous amount of logs to process
  - 100 events per second is >8 billion events/day
- Managing system logs into meaningful intelligence
  - Can you find that needle in the haystack?
- High speed networks are challenging packet collection and metadata accuracy
- Accurate packet collection is dependant on speed and storage capacity
- How complete and accurate is the data?

Regulations - Failure

- Failure to comply can have painful results
  - Fines/penalties
  - Additional audits
  - Loss of brand value
  - Delay/hard stop on business processes
- Exposures may result
  - Customer and investigation costs
  - Loss of customers
  - Lawsuits

End Goals

- Centralize logging
- Consider event rate
- Normalize the data (system independent)
- Reporting and analysis functions
- Notification and alerting
- Minimum administration

Ref: https://www.nsslabs.com/system/files/public-report/files/Cyber%20Resilience_0.pdf

Password Guessing – SQL Attack

- Would you want to know someone is after your SQL database?

Logon Type:	10
Account For Which Logon Failed:	
Security ID:	NULL SID
Account Name:	root
Account Domain:	DBSERVER
Failure Information:	
Failure Reason:	Unknown user name or bad password.
Status:	0xc000006d
Sub Status:	0xc0000064

Logon Type:	10
Account For Which Logon Failed:	
Security ID:	NULL SID
Account Name:	kelly
Account Domain:	DBSERVER
Failure Information:	
Failure Reason:	Unknown user name or bad password.
Status:	0xc000006d
Sub Status:	0xc0000064

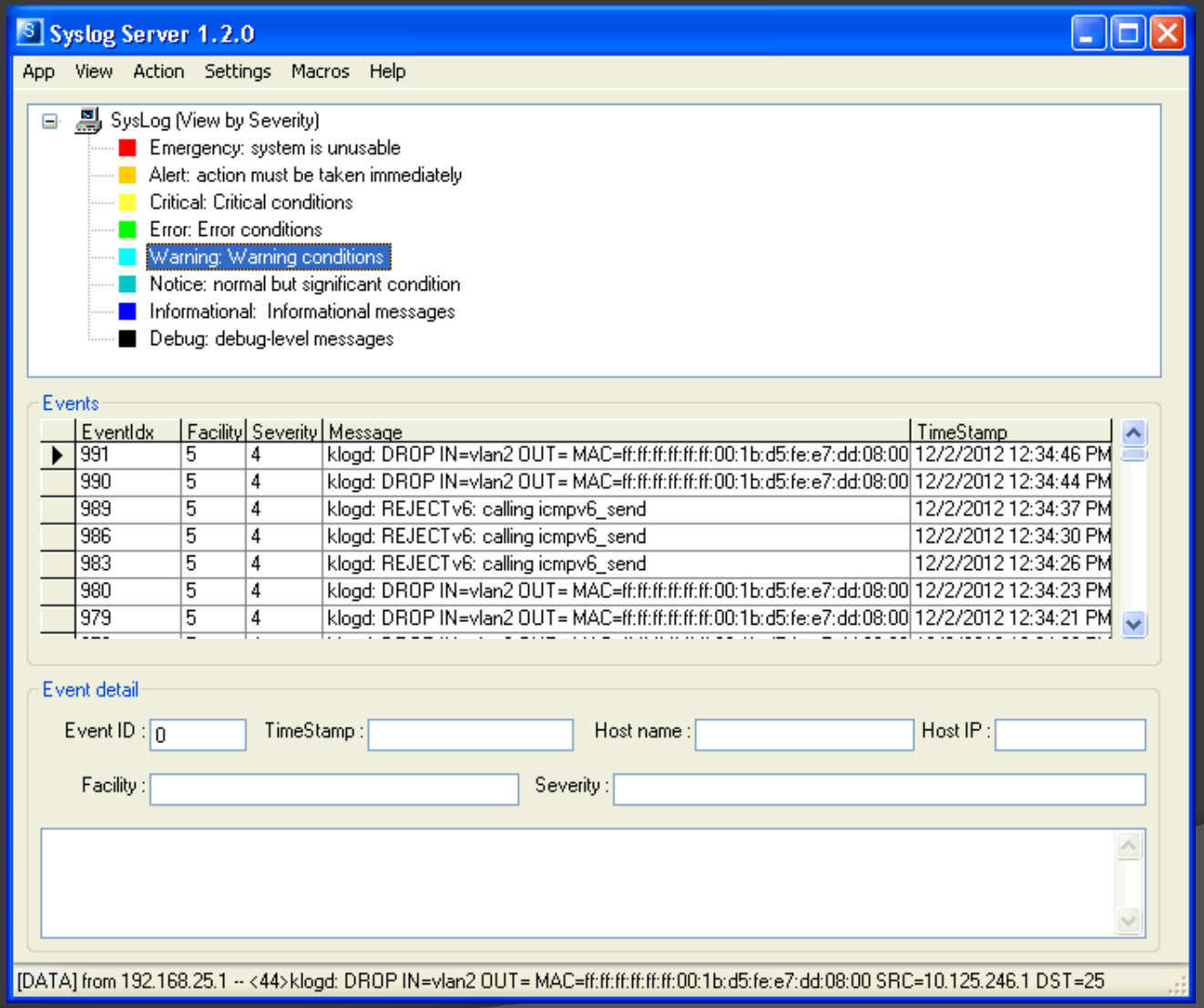
Logon Type:	10
Account For Which Logon Failed:	
Security ID:	NULL SID
Account Name:	sql
Account Domain:	DBSERVER
Failure Information:	
Failure Reason:	Unknown user name or bad password.
Status:	0xc000006d
Sub Status:	0xc0000064

Free Loggers

- Basic syslog server
- Sagan → Sguil Database
- Windows Syslog Server
- NXLOG Community Edition
  - Supports Unix, Android, Windows, etc
  - Read logs from various databases

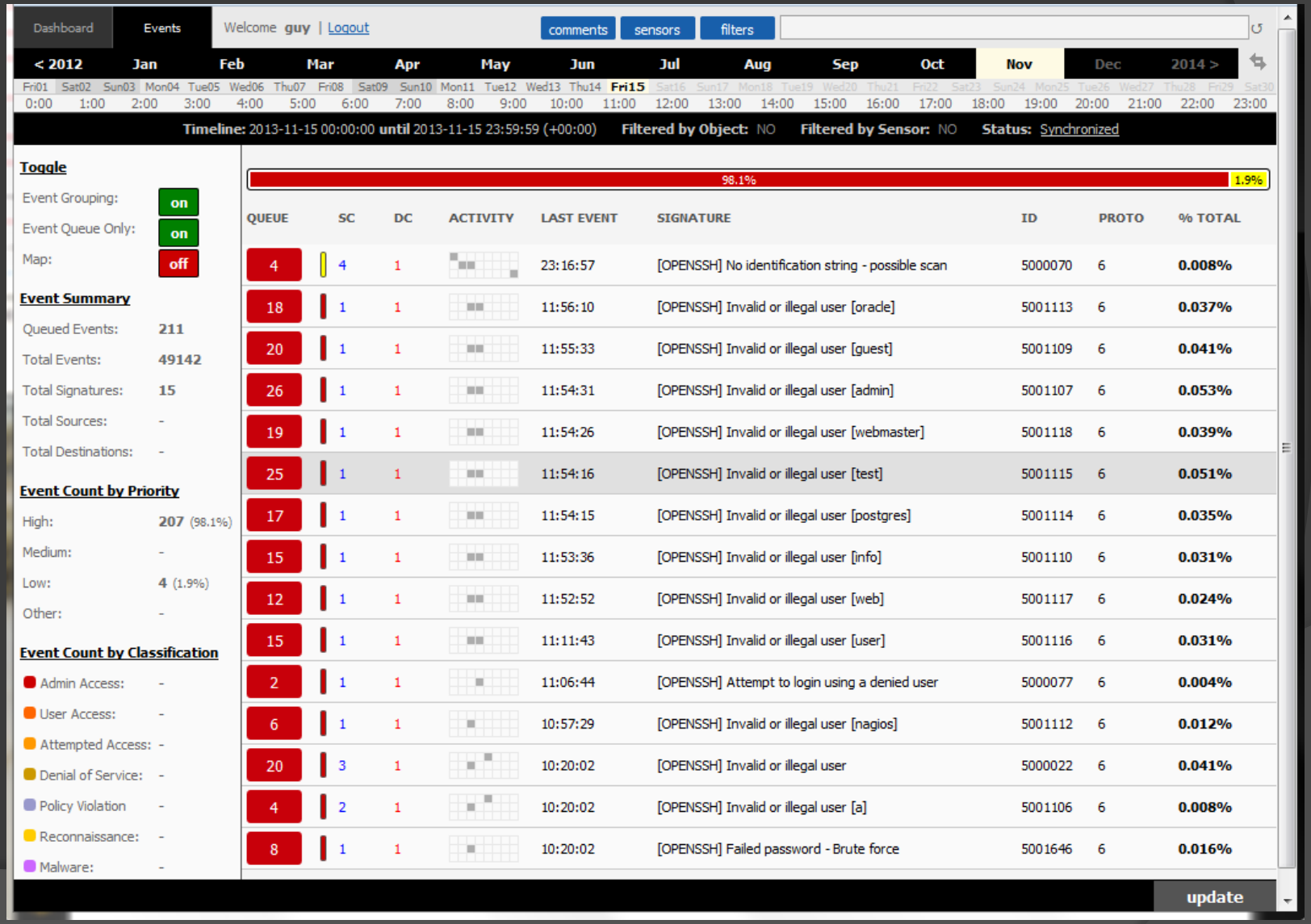
http://nxlog-ce.sourceforge.net
http://log4ensics.com/features

Basic Syslog Server



http://sourceforge.net/projects/syslog-server/

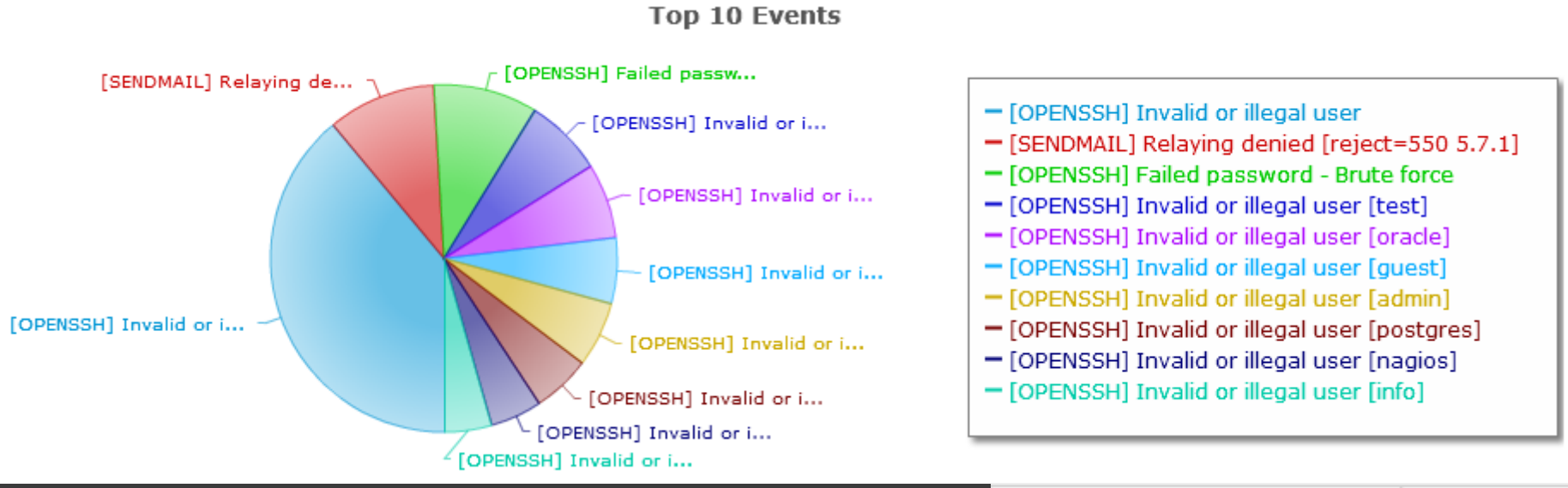
Sagan → Sguil Database



Commercial Products

- Evaluations available
  - HP ArcSight
  - Splunk
- IBM QRadar
- RSA Security Analytics → Log Decoder
- Snare → Sends Windows logs in syslog format

ArcSight Logger – Unix Logs



deviceEventClassId	_count
[OPENSSH] Invalid or illegal user	324
[SENDMAIL] Relaying denied [reject=550 5.7.1]	84
[OPENSSH] Failed password - Brute force	81
[OPENSSH] Invalid or illegal user [test]	61
[OPENSSH] Invalid or illegal user [oracle]	58
[OPENSSH] Invalid or illegal user [guest]	51
[OPENSSH] Invalid or illegal user [admin]	51

Summary

- Inaccurate (or absent) logs = difficult incident response
- Meeting regulations more than just a check box (PCI, PEPIDA)
- Can you survive a breach?
  - Operate at 60%, contain and investigate

Ref: http://eromang.zataz.com/2011/08/16/arcsight-logger-l750mb-now-for-free/