SIEM Logging

Presenters:
Matt Bradley, EchoSat
Agenda

• Housekeeping
• Presenters
• About Conexxus
• Presentation
• Q & A
Housekeeping

This webinar is being recorded and will be made available in approximately 30 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck
- Survey Link – Presentation provided at end

Participants
- Ask questions via webinar interface
- Please, no vendor specific questions

Email: info@conexxus.org
Conexxus Host
Allie Russell
Conexxus
arussell@conexxus.org

Moderator
Kara Gunderson
Chair, Data Security Committee
POS Manager, CITGO Petroleum
kgunder@citgo.com

Speakers
Matt Bradley
Solutions Engineer, EchoSat
mbradley@echosat.com
About Conexxus

• We are an independent, non-profit, member driven technology organization
• We set standards…
  – Data exchange
  – Security
  – Mobile commerce
• We provide vision
  – Identify emerging tech/trends
• We advocate for our industry
  – Technology is policy
## Conexxus Webinar Schedule

<table>
<thead>
<tr>
<th>Month</th>
<th>Subject</th>
<th>Speaker(s)</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2017</td>
<td>SIEM Presentation</td>
<td>Matt Bradley</td>
<td>EchoSat</td>
</tr>
<tr>
<td>April 2017</td>
<td>Internet of Things &amp; Impact of Bring Your Own Device to the Workplace</td>
<td>Bradford Lowey, Jeff Gibson</td>
<td>Wayne Fueling, EchoSat</td>
</tr>
<tr>
<td>May 2017</td>
<td>Customer Engagement Technologies to Enhance Sales and Profitability</td>
<td>Ed Collupy, Gray Taylor, Lesley Saitta</td>
<td>W. Capra, Conexxus, Impact 21</td>
</tr>
</tbody>
</table>

If you have a suggestion for a webinar, please contact Conexxus at info@conexxus.org.
2017 Conexxus Annual Conference
Loews Annapolis Hotel
Annapolis, Maryland
April 23 – 27, 2017
Centralized Logging and Alerting (SIEM)
What is SIEM?

A combination of SIM (Security Information Management) and SEM (Security Event Management)

Critical component of situational awareness

Provides

• Real-time visibility into network events
• Access to historical records for forensic purposes
• Reporting tools for compliance requirements

Software based, hardware based, or offered as managed service
Who needs a SIEM?

Any organization with information to protect

Any organization required to meet compliance standards

PCI, SOX, HIPAA
What does a SIEM do?

- Aggregation of event data
- Event correlation
- Alerting
- Reporting
What does a SIEM NOT do?

• **Provide 100% protection**
  • Help you protect yourself
• **Make you compliant**
  • Help you reach compliance
Business Benefits of SIEM?

Operational Efficiency
- Real-time Monitoring
- Application status, down-time, trending

Cost Savings
- Unification of multiple critical apps
- Licensing

Compliance
- Meet regulatory requirements

Centralization
- Reduced complexity
- One place to look

ROI
- Impossible to manually analyze log data
- IT can focus on strategy
What to look for in a SIEM?

Log Collection
- Agent versus Agentless
- Centralization
- Interoperability (APIs)

Log Retention
- Tamper-proof (encryption?)
- Simple retrieval and easy analysis
- Duration (know your requirements)

Performance
- EPS (Events per Second) rate
- Bandwidth
- Processing power
What to look for in a SIEM?

Event Correlation (real-time)
- Predefined rulesets and alerts
- Customizable rulesets and alerts
- Ensure correlation is easy and intuitive

User Activity Monitoring
- Audit Trail

Compliance Reporting
- Out-of-the-Box regulatory compliance (PCI, HIPAA, SOX)
- Customizable reports
What to look for in a SIEM?

File Integrity Monitoring
- Business critical files and folders
- Record adds/changes/deletions/views etc.
- Ensure correlation is easy and intuitive

Forensics Tools
- Log search functionality

Dashboards
- Configurable, drillable
- Help admins make timely, informed decisions
- Exportable
Security Alerting Example

• Threats classified (High, Medium, Low)
• Threats blocked automatically
• Events logged
• Notification sent
Providers

Dozens of options

- Understand your needs
Preparation – What’s important

IT / Security
Security Events
Flows
Server Logs
Database Activity

Compliance
Identity Context
Data Access
Usage
WHO - WHAT - WHEN - WHERE
Selection Criteria

Meet Business Needs?

Scalability

Policy and Reporting

Capabilities

Ease of Management

Customization

Integration
Selection Process

- Define your needs
  - Committee based?
  - Identify systems, workflows
- Formulate Requirements
- Evaluate
  - RFI
  - Select Finalists (execute POC)
- Cost comparison
- Acquisition, Implementation, Maintenance
- Select and Deploy
Implementation

NSA Mode vs. Clearly Defined Requirements
Define what is important (use case)
- Classify Exceptions
- Event Spikes
- Time Stamps

Sources (POS, Back Office, Tank Monitor, Router, Switch, Firewall, PC, etc.)
- Syslog
- Local Host Logs (Application, Security, System)
- Active Directory (Adds, Changes, Logins)
- Remote Access (VPNs)
- Databases
- Servers (File Integrity)

Data Storage
- Relational database - Historically
- Currently Indexed File Storage (flat file)
Operations

Maintain your SIEM
• Threats evolve
• Corporate policies change
• Regulatory changes

Human element a factor
• PCI 3.1 Section 10.6.1
  Review logs daily
  Automated or manual
  Ownership / Responsibility
• Website: www.conexxus.org
• Email: info@conexxus.org
• LinkedIn Group: Conexxus Online
• Follow us on Twitter: @ConexxusOnline

April 2017 @ 12:00PM Eastern:
Internet of Things & Impact of Bring Your Own Device to the Workplace