Logging and Monitoring

Moderator Name:

Mark Smith, SVP infrastructure and Risk Management

Panelists Names:

Amani Fawzy, Chief Technology Officer, Fawry

Gavin Robinson, Corporate Information Security Manager, Keane UP

Logging and Monitoring

- Logging
- File Integrity Monitoring
- 24X7 monitoring
- Managing volumes of data

Reg/Standard	Coverage area
ISO 27001	A.7, A.12
PCI	10
EI3PA	10, 11
HIPAA	164.308a1iiD
FISMA	SI-4

Signature	Total #
ossec: Windows Logon Success.	1419 (44%)
juniper-netscreen-fw: Permit	395 (12%)
Fortigate: Allowed traffic	235 (7%)
ossec: Windows audit failure event.	199 (6%)
cisco-asa: Deny protocol src [interface_name:SRC_IP/SRC_PORT] [dst interface_name:DST_IP/DST_PORT] [type {string}, code {code}] by access_group acl_ID [0x8ed66b60, 0xf8852875]	157 (5%)
cisco-asa: Teardown TCP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [reason] [(user)]	145 (4%)
cisco-asa: Built {inbound|outbound} UDP connection number for interface_name:real_address/real_port (mapped_address/mapped_port) to interface_name:real_address/real_port (mapped_address/mapped_port) [(user)]	132 (4%)
cisco-asa: Teardown UDP connection number for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [(user)]	123 (4%)
cisco-asa: Built {inbound|outbound} TCP connection_id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port) [(user)]	123 (4%)
ossec: Windows is shutting down.	114 (4%)
ossec: Successful sudo to ROOT executed	49 (2%)
ossec: Windows User Logoff.	41 (1%)
ossec: Multiple Windows audit failure events.	28 (1%)
cisco-asa: Deny IP due to Land Attack from SRC_IP to SRC_IP	20 (1%)
ossec: Windows DC Logon Failure.	15 (0%)
ossec: SSHD authentication success.	10 (0%)
ossec: Login session opened.	10 (0%)

ControlCase
Compliance as a Service

Components of a Logging/FIM/Monitoring solution

ControlCase
Compliance as a Service

Assets and Log Generation

- Assets
  - Comprehensive asset list during deployment
  - Continuous monitoring for new assets and assets dropping off
  - Correlation with other sources such as scanning and asset management repositories
  - Alerts in case of new assets and assets dropping off

- Log Generation
  - Servers – syslog, Windows logs
  - Network devices – syslog, SNMP, SDEE
  - Security devices – syslog, SNMP, SDEE
  - Mainframes – SFTP, flat files
  - Databases – Localized logging, database logging software in case local logging is resource intensive
  - Applications – Database lookup, SFTP, custom plugins

ControlCase
Compliance as a Service

FIM Alerts

- Agents such as ossec
- Software such as ControlCase HIDS, Tripwire etc.
- Integration with log alerts
- Monitoring vs. expected changes

Security Information and Event Management

- Consolidated alerts from
  - Syslog
  - Custom sources
  - FIM alerts
  - SFTP
- Correlation of data based on
  - Source/Destination IP addresses
  - Source of alerts
  - Vulnerabilities
  - Past history
  - User performing action

ControlCase
Compliance as a Service

Centralized Dashboard

ControlCase
Compliance as a Service

Panel Discussion

- Discussion Primer Questions
  - What are components of a good logging and monitoring program?
  - What are challenges in implementing a logging and monitoring program?

ControlCase
Compliance as a Service