Muscat, Oman

15-19 October 2017

www.silensec.com

Red Chungu™

Red Chungu™

TRAINING

by **Dr. Almerindo Graziano**
CEO Silensec

Muscat, Oman
VENUE

15-19 Oct 2017
DATES

Email:
ARCC@ita.gov.om
FOR REGISTRATION PLEASE CONTACT

المركز العربي الاقليمي للأمن السيبراني
ITU - ARAB REGIONAL CYBERSECURITY CENTER

REQUIREMENTS

A laptop is required to be able to work through all the practical hands-on workshops. Failure to meet the requirements below may result in the delegate not being able to carry out one or more of the practical workshops and thus not taking full benefit of the course. The minimum laptop requirements are:

- x86-compatible 1.5 Ghz CPU – minimum or higher
- 3GB RAM – minimum or higher
- 20 Gigabyte available hard drive space

About the Course

This course addresses the challenges faced by modern organizations with regards to Log Management in order to comply with business requirements, as well as the requirements imposed by the law, regulations and contractual obligations. A typical organization will have devices, computer systems and applications generating thousands of logs daily, each with specific requirements which must be met. In this course the student will work through a practical case study following a top-down approach to log management, starting from the requirements analysis down to the choice, deployment and configuration of log management tools and solutions.

Who Should Attend

This course is ideally suited for: security officers, IT managers, system administrators, intrusion detection analysts, security professionals wanting to gain practical knowledge and competences in the domain of Log Management.

Prerequisites

The course is "hands-on", technically focused and aimed at those individuals who have a good knowledge of common networking protocols, and practical familiarity with the Linux and Microsoft operating systems.

laptop requirements

A laptop is required to be able to work through all the practical hands-on workshops. Failure to meet the requirements below may result in the delegate not being able to carry out one or more of the practical course labs.
The minimum laptop requirements are:

- x86-compatible 1.5 Ghz CPU Minimum or higher
- 2GB RAM minimum or higher
- 30GB available hard drive space
- Wireless adapter

Course Outline

DAY 1 The course begins with a presentation of the overall log management process and introduction of the case study organization for which the log management process will be developed throughout the duration of the course. Day one completes with the identification of the log requirements, along with the choice of logs to be collected and the identification of the related security requirements.

DAY 2 Different log formats are presented to understand how logs are generated by different sources such as operating systems, applications and devices and the location of important log files. The course delves into the logging process for different flavours of the Windows and Unix/Linux operating systems while also explaining how to find specific information in log files.

DAY 3 It is time to review and practice with a range of tools that can be used to automatically collect, normalize and aggregate logs and move forward towards the implementation of the log management system for the case study organization.

DAY 4 A range of commercial and opensource log management solutions are reviewed and integration issues addressed. A log management system is deployed and configured for the case study organization.

DAY 5 The final day is dedicated to log review and analysis going through manual review techniques using scripts and working with log correlation rules to generate alerts for specific combination of events. The course concludes reviewing the log reporting process, using the chosen tools and log management system to generate log management reports.

Course breakdown

day 1

The log management process
- What is a log
- The importance of logging
- Key log management activities

Sources of requirements
- Business objectives
- PCI DSS, ISO27001 and other standards compliance
- Log management best practice

Establishing The Log Management Process
- Identifying the information to be logged
- Capturing the security requirements
- Establish Log Management Policy
- Role and Responsibilities

day 2

Logs
- Log formats and Syntax
- Anatomy of a good log

Windows Logging
- Logging in Windows Servers
- Logging in Windows Clients

Unix and Linux Logging
- The audit deamon
- Solaris, AIX, HP logs

Splunk
- Architectural Components
- Parsing and Indexing
- Installation and configuration
- Splunk Apps

AlienVault
- Architectural Components
- AlienVault Logger

day 3

Centralized Log Management
- Challenges of log management
- Log Management Architectural Components

Syslog
- Facilities and Security Levels
- Syslog Agents
- Syslog Implementations

Rsyslog
- Rsyslog configuration
- Clients configuration
- Writing filters

OSSEC
- Log Management with OSSEC
- Deploying and using OSSEC
- Writing OSSEC rules

day 4

Log Management Systems
- Features of a Log Management System
- Log Management Systems vs SIEM
- Log Management Solutions

day 5

Log Analysis
- Tool-based Analysis
- Manual Log Analysis
- Statistical Log Analysis

Periodic Log Reviews and Patterns
- Building a Log Baseline
- Daily, weekly, Monthly, Annual Reviews

Log Data Mining
- Finding Interesting Activities

Correlation
- Common Correlation Patterns
- Simple Event Correlator (SEC)

Log Reporting
- Key Reports to Generate
- Log Visualization

Log Security
- Attacks
- Covert Logging

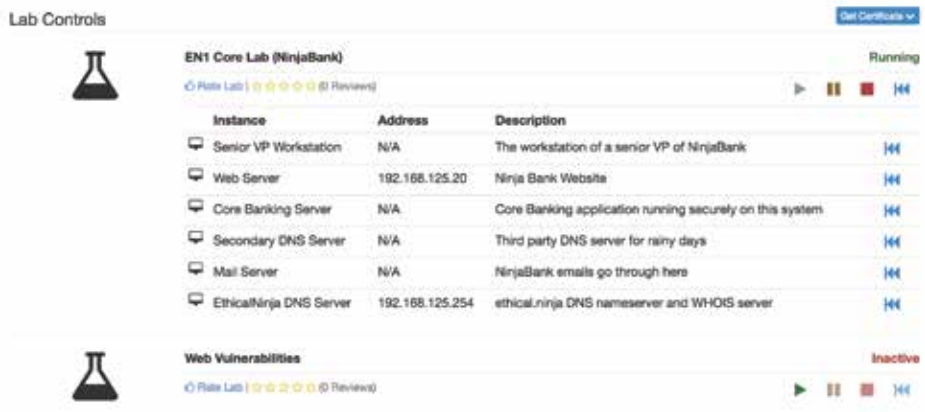
Devices and Applications Logs
- Networking devices
- Web servers and proxies
- Security Devices and Applications
- Systems and Applications

about the Author

Almerindo Graziano, PhD
Silensec CEO

Almerindo holds an MSc in Electronic Engineering and a PhD in mobile computer security, both from the University of Naples, Italy. For five years he was also the founder and course Leader for the MSc in Information Systems Security at Sheffield Hallam University, in collaboration with the British Standard Institution (BSI). He has personally authored a number of training courses from ethical hacking to intrusion detection, along with the first ever ISO27001 Lead Implementer certification course offered by BSI worldwide. His areas of expertise include standards compliance (e.g. ISO27001, ISO22301, PCI DSS), IT infrastructure protection, design of SIEM and Log Management systems and development of the development of cyber threat intelligence capabilities. He has consulted in formation security for private and government organizations across Europe, Africa and Middle East. He also works as a cyber security expert for the International Telecommunication Union (ITU) regularly delivering cyberdrills exercises and workshops for national CERTs and governments around the world

Silensec Online Learning Environment
SOLE



about Silensec

bsi. ISO/IEC 27001 Information Security Management

Silensec is an ISO27001 certified Information Security Management Consulting and Training company specialized in the development and delivery of advanced services across all areas of information security from the protection of infrastructure up to the classification and protection of data. Silensec offers over 30 training courses across all domains of cyber security and collaborates with the International Telecommunication Union (ITU) for the delivery of cyber security training and cyber drills to national CERTs worldwide.

silensec™ ISO27001 Certified