WPN4-ELK NetEye Log Analytics & SIEM Trainining

Agenda

Module title	Module Purposes	Duration	Day
NetEye Elastic module overview 🆕	Overview of all NetEye Elastic OEM main functionalities based on Online demo	⏰1h	DAY 1
Introduction	• Presentations • LogManagement Architecture overview • Review of the Elastic module web interface	⏰1h	DAY 1
Log Presentation	• Kibana presentation ○ Lab: Dashboard navigation, search, visualize, monitoring ○ Lab: Creating dashboards and all necessary elements	⏰2h	DAY 1
Log Collection	• Log Collection through Elastic *Beats Agents and Elastic Agents ○ Introduction ○ Elastic Common Schema concepts ○ Lab: Configuration of Elastic Agents to collect data from different sources ○ Central Configuration of Agents through Fleet Management	⏰3h	DAY 2
Log administering	• Index Management • Lifecycle Management • Elastic backups and snapshots • Elastic Stack Monitoring • Enrichment	⏰2h	DAY 3

Log signing	• Blockchain for real-time log signing • Lab: Use of the NetEye real time log signing function	⏰1h	**DAY 3**
Elastic Stack integration in NetEye	• Role Management and troubleshooting • Multitenancy • Enrichment of Director Data • Deepening on GDPR issues related to the collection of system logs	⏰1h	**DAY 4**
Security Module	• Detection • Analysis with timeline • Log Correlation through EQL • Lab: Create new dedicated detection rule • IoC Rules • Deepening on the strategy for the collection of logs from Windows perimeter with the Windows Forwarder Event • Endpoint protection	⏰2h	**DAY 4**
Machine Learning Introduction	• Machine Learning in the Elastic Stack • Lab: Simple ML Job creation	⏰0.45 h	**DAY 4**
Exam Information	• Recap and Exam Information • Q&A	⏰0.20 h	**DAY 4**