WPN4-ELK NetEye Log Analytics & SIEM Training

Agenda

Module title	Module Purposes	Duration	Day
NetEye Elastic module overview NEW	• Overview of all NetEye Elastic OEM main functionalities	1h	**DAY 1**
Introduction	• Presensations • Log Management First Contact	1h	**DAY 1**
Log Manager Web Interface	• Kibana: Discover Overview ○ Lab: Play with Kibana features (discover) • Kibana: Visualize Overview	2h	**DAY 1**
Log Manager Web Interface	• Kibana: Dashboard Overview, Canvas ○ Lab: Play with Kibana features (visualize and dashboard)	1h	**DAY 2**
Log Collection	• Elastic Common Schema (ECS) • Log Collection through Agents (Beats) • Log Collection through Agents (Elastic-Agent) and Fleet Management ○ Lab: Configure Fleet Management and Elastic-Agent on NetEye • Log Collection on appliance (Syslog)	3h	**DAY 2**
Log Administering	• Index Management • Lifecycle Management • Elastic backups and snapshots • Elastic Stack Monitoring • Enrichment	2h	**DAY 3**
Log Enrichment	• Enrichment with Icinga Director Data	0.30h	**DAY 3**

	○ Lab: Play with Host enrich		
Log Signing	• Blockchain for real-time signing • Lab: Use of the NetEye real time log singing function	0.30h	**DAY 3**
Elastic Stack integration in NetEye	• Role Management • NetEye Troubleshooting • Lab: Role Authentication • Multitenancy • Lab: Multitenancy • Alerting in Kibana and integration with Tornado • Lab: Configure Tornado Webhook •	2h	**DAY 4**
Elastic Security App	• Detection, Host and Network • Timelines • Endpoint protection ○ Lab: Enable Elastic Endpoint on Windows	1h	**DAY 4**
Various	• Deepening on GDPR issues related to the collection of system logs • Collect all windows events through Windows Event Forwarding (WEF)	0.45h	**DAY 4**
Exam Information	• Recap and Exam Information • Q&A	0.20h	**DAY 4**