Forcepoint DLP Administrator

Length 3 Days

Description

During the three days, you will learn how to test an existing deployment, how to administer policies and reports, handle incidents and endpoints, upgrade and manage the Forcepoint DLP system. You will develop skills in creating data policies, building custom classifiers and using predefined policies, incident management, reporting, and system maintenance.

Participants

End-User/Customers: System administrators, network security administrators, IT staff,
Channel Partners: Sales Engineers, consultants, implementation specialists

Objectives

Understand simple Forcepoint DLP product deployments
- Create and use custom classifiers
- Use predefined classifiers, rules and policies
- Control various channels of potential data leaks – in TCP networking, discovery and by endpoint
- Manipulate incidents and reports
- Configure incident workflows using TRITON GUI or email
- Perform the backup and restore

Programme

Topic 1: Forcepoint DLP Architecture

1) AP-DATA Product and Basic Deployment
a) Forcepoint product overview
b) What is DLP
a) What is new in the 8.x versions
b) Simple Forcepoint DLP deployments, network topology before and after
c) Management consoles
d) Forcepoint DLP key configurations
e) Registering CG and Forcepoint Email Security
f) ICAP-mode Protector
g) Data security in cloud deployments

2) Forcepoint DLP Components, Transaction Processing
a) Involved machines, OS, virtualization, processes
b) Load Balancing and Policiy Engine Interface (PEI)
c) Processing data transactions, Policy Engine (PE)
d) Testing DLP channels
e) CLI tools to extract plaintext and test policies

f) Custom logic in rule conditions
g) Testing limits of file size, large ZIPs and timeouts.

Topic 2: DLP Policies

1) Custom and Predefined Classifiers
a) Keyphrases and dictionaries
b) Regular expressions
c) File classifiers
d) Script overview. “Supporting terms” near sensitive data; context analysis
e) Credit cards: PCI audit rules, CCN classifiers, Luhn check, prefixes (BINs)
f) Policy exceptions for custom LDAP groups, domains, etc.
g) Cumulative rules (Drip DLP)

2) Fingerprinting and ML
a) File fingerprinting; possibly with ignored sections
b) Database fingerprinting
c) Scheduling, exporting and synchronizing fingerprints
d) Machine Learning

Topic 3: Endpoints; Discovery

1) Data Endpoint
a) Data Endpoint Initial setup
b) EP statuses and disabling them
c) EP profiles, updates and incident reporting
d) Endpoint support for browsers
e) Endpoint support for email clients
f) Hooking application OS calls
g) Unhooking/excluding applications
h) Encryption with User-Defined Key and Profile Key
i) EP and printer drivers, screenshots, optical media, LAN control

2) Discovery Policies
a) Custom and predefined discovery policies
b) Scheduling file scans, incremental scanning
c) Scheduling scans of SharePoint Online, Outlook PST, etc.
d) Responding to discovery incidents
e) Configuring file discovery on EP
f) Incremental scans
g) FPNE – fingerprint classifiers on EP

Topic 4: Incidents and Maintenance

1) Incidents and Reporting
a) Incident manipulation: release, escalation, severity change, assignment, deletion
b) Action plans and notifications
c) Force-release feature
d) Email-based workflow
e) Create a Delegated Admin (DA) with limited permissions

f) Incident reports – exporting from TRITON GUI or with a script
g) Traffic and audit logs

2) Diagnostics, Backups, Upgrades
a) Inspecting PEI and PE logs; issues with timeouts and load balancing
b) Mega-breaches and performance
c) Gathering diagnostics for issue escalation
d) Archiving incident DB partitions and forensics
e) Full backup and restore of a AP-DATA Forcepoint DLP configuration
f) Semi-automatic failover
g) Forcepoint DLP Manager and system module upgrades, backward compatibility
h) Endpoint upgrades, backward and forward compatibility