ST220 ONTAP Security and Ransomware Protection Administration

Kurzbeschreibung:

Im NetApp Workshop **ST220 ONTAP Security and Ransomware Protection Administration** lernen Sie, wie Sie die in die NetApp® ONTAP® 9-Datenmanagementsoftware integrierten Sicherheits- und Compliance-Funktionen verwalten. Sie erfahren, wie Sie eine sichere IT-Umgebung nach Zero Trust Prinzipien wie "Least Privilege Access" und "Encrypt Everything" aufbauen. Außerdem administrieren, konfigurieren und managen Sie die integrierten Datensicherheits- und Compliance-Funktionen von ONTAP 9, zu denen die Datenaufbewahrung mit SnapLock Software und die Datenintegrität mit autonomem Ransomware-Schutz gehören.

Zielgruppe:

Das NetApp Training **ST220 ONTAP Security and Ransomware Protection Administration** ist ideal geeignet für:

- Systemadministratoren
- Cloud Architekten
- Operatoren
- Datenschutzspezialisten
- Unternehmensarchitekten

Voraussetzungen:

Um dem Lerntempo und den Kursinhalten des Workshops **ST220 ONTAP Security and Ransomware Protection Administration** gut folgen zu können, empfehlen wir vorab den Besuch der NetApp Trainings:

- ST200c ONTAP 9.x Admin Basics
- ST221c ONTAP 9.x Data Protection & High Availability
- ST217c ONTAP 9.x - NAS Advanced inkl. Troubleshooting

Sonstiges:

Dauer: 3 Tage

Preis: 2970 Euro plus Mwst.

Ziele:

Der NetApp Kurse **ST220 ONTAP Security and Ransomware Protection Administration** befähigt Sie zu:

- Sichern eines ONTAP-basierten Speichersystems nach den Prinzipien von Zero Trust
- Anwendung der Least Privilege Access Control auf ONTAP-Administratoren und -Benutzer
- Sicherung von Daten während der Übertragung
- Schutz von Daten während der Speicherung
- Durchsetzung der Einhaltung von Datenschutz- und Datenaufbewahrungsrichtlinien
- Sicherer Zugriff auf Daten durch NAS-Protokolle

- Schutz der Daten vor Beschädigung durch Ransomware oder Malware

Inhalte/Agenda:

- ♦ **Sicherheits Konzepte**
  - ♦ ◊ Vorstellung der Sicherheitsbedrohungen
    ◊ Security Standards und Regularien
    ◊ Zero Trust Ansatz
    ◊ Security Assessment mittels des OnCommand Unified Managers

  - ♦ **Absicherung der ONTAP Management-Administration**
  - ♦ ◊ ONTAP Authentication Optionen
    ◊ Role based access control (RBAC)
    ◊ Multifactor authentication (MFA)
    ◊ Multi-Admin Verification (MAV) (Vier Augen Prinzip)

  - ♦ **ONTAP Network Security**
  - ♦ ◊ Sichere Trennung von Netzwerken: IPSpaces, Broadcast Domains
    ◊ Erhöhen der Sicherheit bei SAN, iSCSI und NVMe

  - ♦ **ONTAP Storage Security**
  - ♦ ◊ Datenverschlüsselung auf Volume- und Aggregate-Ebene
    ◊ Key-Management der Datenverschlüsselung

  - ♦ **ONTAP Data Lifecycle Management inkl. Data Retention**
  - ♦ ◊ SnapLock Funktionen
    ◊ Advanced SnapLock Funktionen u.a. ausgewählte, falsch abgelegte Daten sicher vorab zu löschen
    ◊ Dokumentation der Daten-Löschung über Logging

  - ♦ **Erhöhung der ONTAP NAS Sicherheit**
  - ♦ ◊ Deaktivierung unsicherer Netzwerkprotokollversionen und Aktivierung 100% Verschlüsselung im Netzwerk
    ◊ Unix NFS User Authentication und Authorization auf Export- und Filesystem Ebene
    ◊ Windows SMB User Authentication und Authorization auf Share- und Filesystem Ebene
    ◊ Aktivierung des "Storage-Level Access Guard" für NTFS-Security-Datenbereiche
    ◊ User Access Auditing and Logging

  - ♦ **Schutz der NAS Daten Integrität**
  - ♦ ◊ Möglichkeiten der Erstellung von Recovery Points (Snapshots)
    ◊ Schutz der Daten vor Viren durch Antiviren-Scanner
    ◊ Schutz vor Speicherung ungewollter Daten durch File Access Policies (FPolicy)
    ◊ Minimierung des Datenverlustes durch Ransomware
    ◊ Daten Recovery nach einer Ransomware Attacke
    ◊ Cloud Insights Cloud Secure Service

  - ♦ ◊