KURZBESCHREIBUNG CSNTS-SCHULUNG

Certified Stormshield Network Troubleshooting & Support

Einführung

In diesem Kurs wird der Einsatz der Tools und Methoden erklärt, um die erforderlichen Kenntnisse für die Überprüfung und Behebung von Problemen über die Befehlsschnittstelle (CLI) in Stormshield Network UTN-Produkten zu erwerben.

Zielgruppe sind Mitarbeiter von Unternehmen, die die höchste Stormshield-Partnerschaftsebene erreichen möchten, sowie Bewerber, die Supporttechniker oder Fachschulungsleiter für unsere UTM-Produkte werden möchten.

Zielgruppe

IT-Verantwortliche, Netzwerk-Administratoren, IT-Techniker im Allgemeinen.

Pädagogik und Ziele der Schulung

Die Schulung findet im Klassenraum statt, wobei sich theoretische Kurse und praktische Übungen abwechseln.

Die Teilnehmenden erhalten Schulungsunterlagen, bestehend aus Lernstoff und praktischen Übungen (Labs). Zur Umsetzung der Elemente des Kurses verfügen die Teilnehmenden über ein umfassendes technisches Umfeld.

Zum regelmäßigen Nachschlagen stehen alle Aktualisierungen der Schulungsunterlagen 3 Jahre lang im PDF-Format auf unserer Plattform **https://institute.stormshield.eu** zur Verfügung. Außerdem finden die Teilnehmenden auf dieser Plattform ein virtuelles Umfeld über welches sie das Produkt bedienen und die praktischen Übungen nach Belieben ausführen können.

Nach der Schulung und Auffrischung der Grundkenntnisse können die Teilnehmer:

- Die Organisation des Dateisystems sowie die Daemons und Prozesse in einer Stormshield Network-Appliance verstehen
- Die Konfigurations- und Diagnoseanomalien basierend auf Appliance-Protokollen ermitteln
- Netzwerkkonfiguration und -Routing analysieren und diagnostizieren
- Aufzeichnungen des Netzwerkverkehrs erstellen und auswerten
- Netzwerkverkehr analysieren und diagnostizieren, der durch eine Sicherheitsrichtlinie gegangen ist
- Prozesse erkennen, die auf aktuelle Verbindungen angewendet wurden
- Zusammenfassungen von adaptierten, umfassenden und nutzbaren Informationen erstellen
- IPSec VPN-Richtlinien konfigurieren und diagnostizieren
- Hochverfügbarkeitskonfigurationen analysieren und diagnostizieren
- Konfigurationen mit Authentifizierung analysieren und diagnostizieren
- Konfigurationen mit Proxys (explizit und implizit) analysieren und diagnostizieren

Ort, Dauer und Anmeldung

Stormshield führt Zertifizierungsschulungen in Frankreich, Deutschland, Polen, Ungarn, Norwegen, Großbritannien, den Vereinigten Arabischen Emiraten, in der Region Asien-Pazifik und Afrika durch. Außerdem können unsere Kursleiter ab 4 Teilnehmern Schulungen vor Ort anbieten.

Der Kurs zu Fehlerbehebung und Support findet an vier aufeinanderfolgenden Tagen mit insgesamt 28 Stunden statt. Kursbeginn ist am ersten Schulungstag um 9:30 Uhr und an den weiteren Tagen um 9:00 Uhr (sofern vom Kursleiter oder von Stormshield nicht anders angegeben). Alle Anmeldungsgesuche müssen an Ihr Stormshield Schulungszentrum (STC) gesendet werden oder an den Stormshield-Schulungsservice (training@stormshield.eu). Die maximale Teilnehmerzahl ist auf 6 Personen pro Sitzung beschränkt.

Tarif

Der offizielle Preis beträgt 3.500 € ohne MwSt. für vier Schulungstage vor Ort sowie vier Online-Tests zwecks Zertifizierung.

Voraussetzungen und Material

Die Kursteilnehmer müssen über ein gültiges CSNE-Zertifikat verfügen.

Umfassende Kenntnisse für TCP/IP und UNIX-Shell sind erforderlich.

Für die Durchführung der im Kurs vorgeschlagenen Übungen benötigen die Teilnehmer einen tragbaren PC, nach Möglichkeit mit Windows-Betriebssystem (physisch oder virtuell per Netzwerkzugriff), und die entsprechenden Administratorrechte sowie die folgenden Softwareprogramme: Firefox, PuTTY (oder einen beliebigen anderen SSH-Client), WinSCP (oder einen gleichwertigen SCP-Client), Wireshark, VirtualBox oder gleichwertige VMware (VMware-Player oder VMware-Workstation).

Ausführliche Beschreibung

Tag 1

- Einführung
- Betriebssystem und entsprechende UNIX-Kommandos
    - Methoden des Zugriffs auf die Shell und Einstellungen
    - SSH: Funktionen
    - Dateisystem und Dateisystembefehle
    - Ordner und Ordnersystembefehle
    - System- und Benutzerumgebung
    - Dateien und Dateibefehle
- Protokolle
    - Lokale Protokolle: Speicherort, Eigenschaften, Syntax und Kategorien
    - Dazugehörige Befehle
    - Konfigurationsdateien
    - Logd-, logctl-, logging von Kernel-Nachrichten

- Konfigurationsdateien
    - Verzeichnisse, Struktur und allgemeine Syntax
    - Backups (*.na), deckbackup, tar
    - Werkskonfiguration
- Netzwerk und Routing
    - Einstellungen der Netzwerkschnittstellen
    - Brücken und damit verbundene Befehle
    - Routing-Funktionen und ihre Prioritäten
    - Standardrouten und statische Routen
    - Gatemon und andere Objekte
    - Dynamisches Routing
    - Damit verbundene Befehle, Routenanzeige
    - Verbose-Modus
- Erfassung und Analyse des Datenverkehrs
    - Einführung und Hinweise
    - Allgemeine Syntax und Argumente
    - Übliche Filter
    - Beispiele mit Erklärungen und Vorbereitung für gute Datenerfassung
    - Datenverkehrsanalyse mit tcpdump (TCP, UDP/icmp-Datenverkehr)

Tag 2

- Daemons und Prozesse
    - Liste und Rolle
    - Überwachungs-Daemon
    - Dynamische Objekte
- Objekte
    - Objektsyntax
    - Dynamische Objekte
- ASQ-Stadien in der Analyse
    - Schrittweise Analyse der Netzwerkebenen
    - Dazugehörige Befehle
    - Globale Parameter
    - Profile und Spezialeinstellungen
    - Asynchrone ASQ: verschiedene Anwendungsfälle und Watermarking
    - ASQ Verbose-Modus
- ASQ: Sicherheitsrichtlinien
    - Konfigurationsdateien und -ordner, Regelsyntax
    - Filter: zugewiesene Befehle
    - Filter: Beispiele für geladene Regeln (Aktion, Inspektionsebene, Plugins, PBR, QoS, Schnittstellen, Proxy)
    - Filter: Übersetzung von Gruppen und Listen

- NAT: Wiederholung (dynamische NAT, Port-basierte statische NAT, statische/bimap-NAT, keine NAT)
- NAT: dazugehörige Befehle
- NAT: Syntax und geladene Regeln

- ASQ: Stateful und Zustandstabellen
  - Tabelle der geschützten Adressen
  - Host-Tabelle
  - Verbindungstabelle: Beispiele für Verbindungszustände (NAT, vconn, FTP Plugin, async, lite…)
- FTP: synthetische Fallstudie
  - Mechanismen des passiven und aktiven Modus
  - Erforderliche Filterregeln

Tag 3

- Eventd: Ereignismanager
- IPSec-VPN
  - IKE/IPSec Stormshield Network-Implementierung
  - Konfigurationsdateien
  - Sicherheitsrichtlinie (SPD, SA)
  - IKE-Verhandlungen
  - Verhandlungen: Main- und Aggressive-Modus
  - ISAKMP und IPsec SA
  - IKE-Vorschläge
  - Besonderheiten: NAT-T, DPD, Keepalive, SharedSA, Non-NAT-Richtlinie, SPD-Cache
  - Dazugehörige Befehle
  - Analyse eines IPSec-SA
  - Protokolle
  - Benachrichtigungen „SA löschen“
  - Erfassung und Analyse des ISAKMP-Datenverkehrs
  - Besonderheiten von dynamischen Peers
  - Verbose-Modus und häufige Fehler

Tag 4

- PKI und Zertifikate
  - Wiederholung und allgemeine Richtlinie
  - CA-Verzeichnis
  - Konfigurationstipps
  - Zertifikatsüberprüfung
- Hochverfügbarkeit
  - Allgemeine Punkte
  - Konfigurationsdateien

- Dynamische Objekte
- Aktivierungsphasen, Management von Netzwerkschnittstellen
- Prozesse und damit verbundener Datenverkehr
- Replikation/Synchronisierung
- Ereignisse und Hochverfügbarkeitsprotokolle

- Authentifizierung und Nutzer
  - Benutzerdatenbanken
  - Interne LDAP-Basisstruktur
  - Konfigurationsdateien für Nutzerbasis
  - Zugeordnete Attribute
  - Importieren/Exportieren der internen LDAP-Datenbank in LDIF
  - Verbose-Modus der internen LDAP-Datenbank
  - Authentifizierungsmethoden: LDAP/AD, Kerberos, Radius, SSL, SPENEGO, SSO
  - Mehrbenutzermodus
  - Konfigurationsdateien im Authentifizierungsmodul
  - Dazugehörige Befehle
  - Verbose-Modus im Authentifizierungsmodul und SSO-Agent
  - Konfiguration des Captive-Portal in HTTP
- Proxys
  - Allgemeine Punkte
  - Expliziter HTTP-Proxy
  - Implizierter/transparenter HTTP-Proxy
  - Implizierter/transparenter SMTP-, POP3- und FTP-Proxy
  - Implizierter SSL-Proxy

Zertifizierungsprüfung

Die Zertifizierung besteht aus einer Online-Prüfung (3 Stunden 30 Minuten, 60 Fragen).

Die Prüfung besteht aus Multiple Choice-Fragen und offenen Fragen über Funktionen, Einstellungen und erweiterte Methoden zur Fehlerbehebung, die eingesetzt werden müssen, um auf Zwischenfallsberichte des Kunden umfassend reagieren zu können.

Die Mindestpunktzahl für die Zertifizierung beträgt 70 %.

Die Prüfung wird nach dem Ende der Schulung automatisch für die Dauer von sechs Monaten auf der Plattform **https://institute.stormshield.eu** freigeschaltet. Sollte innerhalb dieses Zeitraums die Ablegung der Prüfung nicht möglich sein, wird automatisch und sofort ein zweiter Versuch freigeschaltet, der innerhalb einer zusätzlichen Woche zu absolvieren ist.