Checkliste für Sensor und Konsole nach der Bereitstellung

Veröffentlicht: 2024-09-26

Nachdem Sie einen ExtraHop bereitgestellt haben Sensor oder Konsole, melden Sie sich in den Administrationseinstellungen des ExtraHop-Systems an über `https://<extrahop-hostname-or-IP-address>/admin` und konfigurieren Sie die folgenden Einstellungen. Beziehen Sie sich auf den Abschnitt der ExtraHop Admin-UI-Leitfaden in jeder der unten aufgeführten Aktionen angegeben, sofern nicht anders angegeben.

Passwort

Sorgen Sie nach dem Testzeitraum für die Systemsicherheit. Ändern Sie das Standardkennwort. Weitere Informationen finden Sie in der Häufig gestellte Fragen zu Standardbenutzerkonten.

NTP

Zeit ist im ExtraHop-System von entscheidender Bedeutung, insbesondere bei der Ereigniskorrelation mit zeitbasierten Metriken und Protokollen. Stellen Sie sicher, dass die NTP-Einstellungen für Ihre Infrastruktur korrekt sind, testen Sie die Einstellungen und synchronisieren Sie NTP. Weitere Informationen finden Sie unter Konfigurieren Sie die Systemzeit.

Zeitzone

Die richtige Zeitzone ist entscheidend, um geplante Berichte zur richtigen Zeit auszuführen. Stellen Sie sicher, dass das ExtraHop-System die richtige Zeitzone hat. Weitere Informationen finden Sie unter Konfigurieren Sie die Systemzeit.

Fernauthentifizierung

Richten Sie die Fernauthentifizierung ein. Die ExtraHop-Appliance integriert sich in LDAP, RADIUS, SAML, und TACACS+.

Firmware-Aktualisierung

Die ExtraHop-Firmware wird häufig mit Verbesserungen und behobenen Fehlern aktualisiert. Stellen Sie sicher, dass Sie über die aktuelle Firmware verfügen. Weitere Informationen finden Sie unter Aktualisieren Sie die Firmware auf Ihrem ExtraHop-System.

Audit-Protokollierung

Das ExtraHop-System kann Ereignisse an einen Remote-Syslog-Collector senden. Weitere Informationen finden Sie in der Audit-Log-Daten an einen Remote-Syslog-Server senden.

SMTP

Das ExtraHop-System kann Benachrichtigungen und Systemzustandsbenachrichtigungen per E-Mail versenden. Richten Sie Benachrichtigungen ein und testen Sie sie. Weitere Informationen finden Sie unter E-Mail-Einstellungen für Benachrichtigungen konfigurieren.

System-Benachrichtigungen

Das ExtraHop-System kann E-Mails senden, wenn es Probleme feststellt. Erstellen Sie eine E-Mail-Gruppe , um Benachrichtigungen zu erhalten. Weitere Informationen finden Sie unter Konfigurieren Sie eine E-Mail-Benachrichtigungsgruppe.

iDRAC

Jede physische ExtraHop-Appliance hat eine iDRAC Port, ähnlich wie iLO oder KVM over Ethernet. Verbinden und konfigurieren Sie den iDRAC-Port. Weitere Informationen finden Sie unter Konfigurieren Sie die iDRAC Remote Access Console.

TLS-Zertifikat

Jedes ExtraHop-System wird mit einem selbstsignierten Zertifikat geliefert. Wenn Sie eine PKI-Bereitstellung haben, generieren Sie Ihr eigenes Zertifikat und laden Sie es auf jedes ExtraHop-System hoch. Weitere Informationen finden Sie in der TLS-Zertifikat Abschnitt.

DNS-A-Eintrag

Es ist einfacher, über den Hostnamen auf ein ExtraHop-System zuzugreifen als über die IP-Adresse. Erstellen Sie eine A Datensatz in Ihrem DNS-Root (“`exa.yourdomain.local`„) für jedes ExtraHop-System in Ihrer Bereitstellung. Schlagen Sie in Ihrem DNS-Administrationshandbuch nach.

Festplattenverschlüsselung

Aktivieren Sie die Sicherheit auf Speicherlaufwerken, um die Verschlüsselung auf virtuellen Laufwerken bereitzustellen (nur EDA 9300, EDA 10300 und Intrusion Detection System 9380). Weitere Informationen finden Sie unter Konfigurieren Sie selbstverschlüsselnde Festplatten (SEDs).

Geräte verbinden

Verbinde die Konsole und Sensoren für alle Paket- und Plattenspeicher. Weitere Informationen finden Sie unter Verbinden Sie den EXA 5200 mit dem ExtraHop-System und Sensoren und Konsole mit dem Packetstore verbinden.

Cloud-Dienste

Stellen Sie eine Verbindung zu den ExtraHop Cloud Services her, um Erkennungen und Fernzugriff zu aktivieren. Weitere Informationen finden Sie unter Stellen Sie eine Verbindung zu ExtraHop Cloud Services her.

Bedrohungsinformationen

Konfigurieren Sie die Einstellungen für Bedrohungsinformationen, um Anzeichen für eine Gefährdung in Ihrem Netzwerk zu identifizieren. Weitere Informationen finden Sie unter Bedrohungsinformationen

Netzwerkstandorte

Klassifizieren Sie IP-Adressen, die nicht RFC1918 entsprechen, als Teil Ihres internen Netzwerk. Weitere Informationen finden Sie unter Geben Sie eine Netzwerklokalität an.

Tuning-Parameter

Verbessern Sie die Qualität und Genauigkeit regelbasierter Erkennungen, indem Sie Optimierungsparameter hinzufügen. Weitere Informationen finden Sie unter Geben Sie Optimierungsparameter für Erkennungen und Metriken an

Erweiterte Analyse

Richten Sie die erweiterte Analyse je nach Bedarf auf bestimmte Gerätegruppen oder Aktivitätsgruppen aus, je nachdem, wie wichtig sie für Ihr Netzwerk sind. Weitere Informationen finden Sie unter Prioritäten der Analyse.

TLS-Verkehr entschlüsseln

Entschlüsseln Sie weitergeleiteten TLS-Verkehr, indem Sie den privaten Schlüssel und das Serverzertifikat hochladen, die diesem Verkehr zugeordnet sind. Weitere Informationen finden Sie unter Entschlüsseln Sie den TLS-Verkehr mit Zertifikaten und privaten Schlüsseln.

Perfect Forward Secrecy (PFS) konfigurieren

Entschlüsseln Sie den TLS-Verkehr von Ihren Linux- und Windows-Servern. Weitere Informationen finden Sie unter Installieren Sie den ExtraHop Session Key Forwarder auf einem Linux-Server und Installieren Sie den ExtraHOP Session Key Forwarder auf einem Windows-Server.

Anpassungen und Datenspeicher-Backup

Erstellen Sie ein System-Backup, bevor Sie die Firmware aktualisieren oder bevor Sie eine größere Änderung an Ihrer Umgebung vornehmen. Weitere Informationen finden Sie unter Einen Sensor oder eine Konsole sichern.