100% Remote: Palo Alto Networks Security Engineer – NGFW Prisma Access / Cloud Firewall (m/w/d)

Für unseren Kunden suchen wir einen Palo Alto Networks Security Engineer (m/w/d) in Vollzeit und Remote.
Das Projekt setzt eine einheitliche Netzwerk- und Sicherheitsarchitektur auf Basis von Palo Alto Networks um. Sie unterstützen die interne bei Konzeption, Implementierung, Migration, Test und Dokumentation. Schwerpunkt: praktische Erfahrung, strukturierte Zuarbeit und En internen Spezialisten in Arbeitsspitzen.

Rahmenparameter:
Start: asap
Laufzeit: bis Ende 2026 + Option zur Verlängerung
Auslastung: Vollzeit
Einsatzort: Remote

Aufgaben: Bestehende Designs, Konfigurationen, Regelwerke, Abhängigkeiten und Migrationsplanungen analysieren und kommentiere
Lösungsoptionen und Best Practices aus vergleichbaren Palo-Alto-Implementierungen einbringen
Bei HLD/LLD, Konfigurationsvorgaben, Migrationskonzepten, Runbooks, Testfällen und Betriebsdokumentation zuarbeiten
Konfigurationen und Änderungsvorschläge vorbereiten; produktive Änderungen nur nach Freigabe mit den verantwortlichen Teams
Workshops, Reviews, Tests, Pilotierungen, Cutover-Vorbereitungen und Hypercare unterstützen
Fehlerbilder analysieren, Ursachen/Lösungswege dokumentieren, Hersteller-/Partner-Tickets vorbereiten
Offene Punkte, Risiken und Abhängigkeiten nachhalten und an Projektverantwortliche melden
Wissenstransfer durch Pairing, Dokumentation und Übergaben an interne Mitarbeitende

Fachliche Aufgaben: Zielarchitektur/Übergangsdesign für Perimeter-, DMZ- und Datacenter-Firewalls prüfen/ergänzen;
HA/Clustering, Interfaces, Routing/BGP, NAT, VPN/IPsec, Zonen und Segmentierung unterstützen
Baseline-Konfigurationen für Management, Templates, Device Groups, Naming, Objekte, Security Profiles, Threat Prevention, URL-/DN und Log Forwarding vorbereiten/reviewen
Firewall-Regeln/Objekte analysieren, bereinigen, normalisieren, auf Zonen, App-ID, User-ID und Security Profiles abbilden; Migrationsto bewerten
Cutover-, Rollback-, Pre-Check-, Failover- und Abnahmeschritte ausarbeiten; Tests/Migrationen begleiten, Findings dokumentieren
Prisma-Access-Konfiguration für Tenant, Locations, Mobile Users, Remote Networks, Service Connections, Routing/BGP, Identity, User-ID Egress-IPs, Logging/Monitoring unterstützen
Ablösung von Zscaler und Cisco Secure Client zuarbeiten; Default-Route-, Proxy/PAC-, Zertifikats-, Client-, Server-, OT-, Kubernetes- ur Applikationsabhängigkeiten analysieren
Policies/Objekte auf Benutzer, Gruppen, Standorte und Anwendungen abbilden; URL Filtering, DNS Security, File Blocking, Application C Legacy-Ausnahmen testen/optimieren
Pilot/Rollout unterstützen; Client-Onboarding, Tunnel-/Routingprüfung, Fehleranalyse, Known-Issue-Liste, Rollback und Hypercare Palo
Series bzw. Cloud-NGFW-Designs für Azure/AWS unterstützen; Hub-and-Spoke-, Landing-Zone-, VNet/VPC-, Transit- und Routing-Arch berücksichtigen
Einbindung der Firewalls in Cloud-Routing, HA, Skalierung, Zonen-/Segmentmodell, NAT, DNS, VPN/Service Connections sowie Management-/Logging-Strukturen vorbereiten
Cloud-Regelwerke, Security Profiles und Datenflüsse analysieren; Anforderungen für Egress, Ingress, East-West- und Hybrid-Cloud-Kor aufbereiten

Implementierung, Tests, Failover, Performanceprüfung, Cutover und Fehleranalyse mit Azure-, AWS-, Netzwerk- und Security-Teams unt

Skills: Praktische Erfahrung mit Palo-Alto-Firewalls (Perimeter, DMZ, Datacenter) inkl. HA/Clustering, Zonen- und Segmentierungskonze
Security Profiles
Know-how in Routing-Protokollen, insbesondere BGP, sowie NAT- und VPN/IPsec-Design für komplexe, mehrstufige Netzwerktopologier
Erfahrung in Analyse, Bereinigung und Migration bestehender Firewall-Regelwerke auf App-ID, User-ID und Zonenkonzepte, inkl. Bewer
geeigneter Migrationstools
Praxiswissen in Aufbau/Betrieb von Prisma Access (Mobile Users, Remote Networks, Service Connections, Identity/User-ID, feste Egress
Rahmen von SASE-Transformationen
Erfahrung in Ablösung etablierter Lösungen inkl. Proxy/PAC-, Zertifikats- und Client-Abhängigkeitsanalyse
Kenntnisse im Design von Palo-Alto-VM-Series- bzw. Cloud-NGFW-Lösungen innerhalb von Hub-and-Spoke-, Landing-Zone- und VNe
Architekturen
Fähigkeit, Cutover-, Rollback-, Pre-Check- und Failover-Pläne strukturiert auszuarbeiten und Migrationen mit klaren Abnahmekriterien z
Sicherer Umgang mit High-Level-/Low-Level-Designs, Betriebsdokumentation und nachvollziehbaren Testfällen
Erfahrung in strukturierter Fehleranalyse, Ursachenklärung und Vorbereitung von Hersteller-/Partner-Tickets
Fähigkeit zur Zusammenarbeit mit Azure-, AWS-, Netzwerk- und Security-Teams sowie zum Wissenstransfer via Pairing und Dokumentat
Gute Deutsch- und Englischkenntnisse in Wort und Schrift