Hermann Deutch

contact

(240) 643-9114

hdeutcho@gmail.com

Dallas-Fort Worth Metroplex, TX 76120

Summary

Security-focused network and edge device engineer with proven expertise securing large-scale Customer Premise Equipment (CPE), including router gateways and distributed network endpoints. Experienced in enforcing device hardening standards, managing vulnerability lifecycles, and implementing secure configurations across fleet-scale environments. Strong background in ISP and enterprise networking combined with automation (Python, Ansible) to drive compliance, reduce attack surface, and support incident response. Adept at packet-level analysis, endpoint forensics, and securing Linux-based systems in fast-paced, high-impact environments.

work history

2023 current

Sr Information Analyst / OT Solutions Architect

McKesson | Irving

- Led security architecture for distributed edge devices and OT-connected endpoints, enforcing defense-in-depth strategies
- Hardened Linux-based CPE and gateway devices using CIS-aligned baselines, reducing attack surface by 40%+
- Built automated compliance validation using Python and Ansible across simulated device fleets
- Developed vulnerability management pipeline for firmware and service-level CVEs, improving remediation efficiency
- Partnered with engineering teams to enforce secure configurations across distributed environments
- Supported incident response by analyzing device logs and network traffic to identify root causes
- Established governance frameworks for data quality assurance, ensuring compliance with industry standards and regulations.
- Applied least privilege and RBAC principles to restrict device access, reducing the risk of unauthorized configuration changes and lateral movement
- Created dashboards to monitor and track key performance indicators.

2021 - 2023

Sr Endpoint Security Engineer

Verizon Wireless | Irving

- Designed and secured large-scale ISP network infrastructure supporting distributed customer endpoints

- CPE & Endpoint Security: Device Hardening
- Fleet-Scale Endpoint Protection
- Network Security: Palo Alto (App-ID, NAT, Policies)
- Zero Trust Segmentation
- Systems Security: Linux Hardening
- Vulnerability Management: CVE Analysis
- Risk Prioritization & Remediation Lifecycle
- Compliance Automation (Python, Ansible & YAML)
- Incident Response: Packet Analysis

- Improved network performance and reliability across multiple regions
- Collaborated with cross-functional teams to ensure secure deployment of network services
- Hardened Linux-based gateway and endpoint systems by securing SSH access (key-based auth, disabling root login), minimizing exposed services, and applying secure kernel parameters
- Designed and implemented device hardening standards aligned with CIS benchmarks, ensuring consistent security posture across distributed endpoint fleets
- Troubleshot complex network issues, ensuring minimal downtime and optimal service delivery.
- Secured firmware and device lifecycle processes, including validation of configurations, patching strategies, and mitigation of firmware-level vulnerabilities
- Developed documentation for network architecture, policies, and procedures to ensure compliance and consistency.

2019 - 2021

Sr Network & Security Engineer

McKesson | Irving

- Defined and enforced security standards for OT-connected devices and edge systems
- Implemented Zero Trust segmentation and NAC solutions (Cisco ISE)
- Developed hardening guidelines for network-connected endpoints
- Evaluated and deployed next-generation security technologies
- Led end-to-end vulnerability lifecycle management, from detection to remediation validation, improving security posture and reducing mean time to remediation (MTTR)
- Supported incident response and threat analysis by correlating vulnerability data with real-world exploitation risks, enabling targeted remediation of high-risk endpoints
- Sustained business compliance and service availability while improving delivery metrics by reducing attack surface from 58 % to 92% on CP&E

(Wireshark, tcpdump)

- Threat Detection
- RCA

education

jan 2025 **Master of Science: Cybersecurity**
Western Governors University | Salt Lake City, UT

jan 2014 **Master of Science: Telecommunications**
Supcom

certifications

Cisco Certified Network Associate (CCNA)

Cisco Certified CyberOps Associate.

Palo Alto Networks Certified Network Security Administrator (PCNSA) – Palo Alto Networks.

Juniper Networks Certified Internet

2017 - 2019 **Senior Network Security Engineer**
SemGroup Corp | Tulsa

- Established firmware security protocols for routers and gateways
- Deployed and managed firewall solutions (Palo Alto, Cisco)
- Implemented micro-segmentation strategies for secure network environments
- Conducted vulnerability assessments and penetration testing to identify security weaknesses.
- Developed and enforced security policies to enhance compliance with industry standards.

oct 2015 - dec 2017 **IP/E Lead Support Engineer**
Zayo Group | Tulsa

- Performed CPE and edge device security operations, including monitoring, troubleshooting, and ensuring availability of router gateways and fiber-based endpoints
- Supported fiber-based access networks (SONET/DWDM) and validated performance using Ethernet test equipment (JDSU, T-Berd) across distributed customer environments
- Collaborated with install/activation teams to deploy secure hybrid cloud and customer-edge connectivity solutions, ensuring proper configuration of edge devices and gateways
- Engineered and troubleshot ISP-grade protocols including MP-BGP, ISIS, MPLS L3VPN, and MST, ensuring secure and resilient routing across customer edge networks
- Performed deep network and device-level troubleshooting, isolating faults across routing, switching, and CPE layers in high-availability environments
- Administered and secured DNS/BIND services on Unix/Linux systems, ensuring reliable name resolution and hardened configurations
- Designed and implemented public and private telecommunications network solutions, integrating secure edge connectivity for enterprise customers
- Led and coordinated network deployment and installation projects, including provisioning of

Specialist (JNCIS) - Juniper Networks.

Cisco Certified Network Professional (CCNP) - Cisco Systems.

Certified Information Systems Security Professional (CISSP) -International Information System Security Certification Consortium (ISC)². - in Progress

routers, switches, and CPE devices across customer environments
- Supported end-to-end lifecycle of network and CPE equipment, including deployment, monitoring, incident resolution, and performance optimization
- Managed and secured a large-scale multinational Ethernet/IP network, supporting diverse infrastructure including Cisco, Juniper, Nokia-Siemens, and Accedian CPE / edge performance monitoring devices

jan 2011 - feb 2012

Network & System Engineer

Quanteq Technology Services | Cameroon

- Managed and secured Windows Server and VMware environments, supporting backend systems used for device management, monitoring, and configuration enforcement.
- Implemented secure configuration standards on networking hardware (Cisco and multi-vendor), ensuring compliance with enterprise security baselines and reducing vulnerabilities.
- Maintained and updated network and CPE topology documentation, enhancing visibility and supporting incident response and troubleshooting efforts.
- Collaborated with cross-functional teams (design, operations, Layer 1, PMs) to deploy secure infrastructure and CPE solutions across distributed environments.

projects

CPE Security Hardening Framework: Designed a scalable framework for securing router gateways and edge devices including hardening, vulnerability management, automation,and threat detection.

languages

French

Native or Bilingual

German

Limited Working