Prempeh Agyemang

Alliston, Ontario, Canada | cbsprempeh@gmail.com | 416-277-8452

PROFESSIONAL SUMMARY

Cybersecurity and systems administration professional with hands-on experience building, securing, monitoring, automating, and troubleshooting enterprise-style IT environments. Skilled in Windows Server, Active Directory, TCP/IP networking, pfSense, Splunk SIEM, Sysmon, Snort IDS, Linux, VMware, and PowerShell. Experience includes security event monitoring, log analysis, threat detection, network segmentation, firewall administration, controlled security testing, and security workflow automation. Currently expanding hands-on capabilities in endpoint detection and response (EDR), endpoint telemetry, alert triage, and automated security operations.

EDUCATION

Diploma - Computer Networking | Georgian College

Relevant Coursework: Network Security, Cybersecurity, Cloud Computing, Advanced Networking, Data Management

CERTIFICATIONS & TRAINING

- Google Cybersecurity Professional Certificate
- Deep Web & Cybersecurity Certificate - EC-Council
- Coursera Network Projects Certificate
- CCNA: Enterprise Networking, Security and Automation - Cisco
- AWS Technology Cloud Essentials Badge
- TryHackMe SOC Level 1 Certificate
- IBM and ISC2 Cybersecurity Specialist
- Coursera Networking Project

TECHNICAL SKILLS

Systems Administration

- Windows Server 2016, 2019 & 2022; Active Directory Domain Services (AD DS)
- Domain Controllers, AD replication, Group Policy, DNS, DHCP, users, groups and OUs
- Identity & Access Management; file server administration; NTFS & share permissions
- Windows Event Logging, PowerShell administration and technical troubleshooting

Networking & Infrastructure

- TCP/IP, IPv4, subnetting, LAN/WAN networking, routing and network segmentation
- pfSense firewall administration, firewall rules, access control, NAT and DHCP
- VPN/IPsec fundamentals, IDS/IPS fundamentals, Wireshark packet analysis
- VMware virtual networking and network troubleshooting

Cybersecurity, SOC & EDR

- Splunk Enterprise SIEM, Universal Forwarder, SPL searches, dashboards and alerts
- Sysmon endpoint telemetry, Snort IDS, Windows Security Event analysis and centralized logging
- Threat detection and investigation, detection engineering, network traffic monitoring and vulnerability assessment
- EDR concepts and workflows: endpoint telemetry, behavioral detections, alert triage, investigation, containment and response
- Endpoint security investigation using process, network, authentication and persistence telemetry
- Controlled security testing with Kali Linux; firewall/IDS validation; security hardening and incident response fundamentals

Security Automation & Scripting

- PowerShell automation for Windows administration, endpoint checks, log collection and repetitive security tasks
- Python fundamentals for parsing, enrichment, data handling and security workflow automation
- Bash scripting for Linux administration and repeatable operational tasks
- Automation concepts: alert enrichment, IOC handling, response workflows, scheduled checks and repeatable remediation
- Git & GitHub for version control, documentation and project tracking

Cloud, Identity & Virtualization

- AWS cloud fundamentals; Microsoft Entra ID and hybrid identity fundamentals
- VMware Workstation; Linux administration; Kali Linux
- pfSense, Splunk, Sysmon, Snort and Wireshark

PROJECTS

Enterprise Active Directory & SOC Home Lab

Designed, built, secured, monitored, and troubleshot a segmented enterprise-style Active Directory and SOC environment using Windows Server 2022, VMware, Active Directory, Group Policy, DNS, pfSense, Splunk Enterprise, Sysmon, Snort IDS, and Kali Linux.

- Deployed multiple Windows Server systems with AD DS, DNS, Group Policy, domain controllers, users, groups and Organizational Units.
- Designed segmented Server, Client, Management, DMZ and External security-testing networks using VMware and pfSense.
- Configured pfSense routing, DHCP, NAT, firewall rules and network access controls.
- Implemented Splunk Enterprise SIEM for centralized Windows, Sysmon, pfSense and Snort log collection and security monitoring.
- Created SPL searches, dashboards, alerts and detection logic for authentication failures, account activity, PowerShell/CMD execution, reconnaissance and other security events.
- Deployed Sysmon for endpoint telemetry and Snort IDS for network threat detection.
- Used Kali Linux for authorized security testing and validated firewall, IDS, logging and SIEM visibility.
- Diagnosed and resolved networking, DNS, firewall, SIEM parsing, detection, VMware networking and system-resource issues.
- Documented the environment through a technical portfolio, network topology and GitHub repository.

Networking Projects

Completed hands-on networking projects involving routing, switching, IPv4 addressing, subnetting, network configuration, packet analysis, connectivity testing and troubleshooting.

PROFESSIONAL SKILLS

Technical Troubleshooting & Problem Solving | Analytical Thinking | Technical Documentation | Continuous Learning | Clear Communication | Time Management | Team Collaboration

LANGUAGES

English - Fluent