Caleb Smith

Cyber Security Engineer | Threat Hunting

Cyber Security Engineer focused on Microsoft Sentinel, Microsoft Defender, and threat hunting. I develop KQL investigations, detection content, and automation for multi-client SOC environments, drawing on extensive cloud and infrastructure experience.

Certifications obtained

 SC-100 Cybersecurity Architect Expert	 SC-200 Security Operations Analyst Associate	 SC-900 Security, Compliance and Identity Fundamentals	 AZ-104 Azure Administrator Associate
 AZ-140 Azure Virtual Desktop Specialty	 AZ-800 | AZ-801 Windows Server Hybrid Administrator Associate	 AZ-900 Azure Fundamentals	 AI-900 Azure AI Fundamentals

Completion is listed in the supplied CV; current renewal dates are not included.

Core skills

Microsoft Sentinel | Microsoft Defender | Threat Hunting | KQL Investigations | Detection Engineering | SOC Automation | Azure Lighthouse | Azure DevOps and Bicep | PowerShell and Python | Azure and Microsoft 365 | Intune and Identity | Infrastructure Security

Education and further learning

Cybrary.IT Online

CompTIA Linux+ course certificate | 10 CEU/CPE; CompTIA A+; Corporate Cyber Security Management; Microsoft 365 Web Content Management / SharePoint; Virtualization Management

Shaw Academy Online

Introduction to Web Design

Alison Advanced Learning Systems Online

Fundamentals of Network Security; I.T Management - Software and Databases; Leadership Skills in Business

Windermere High School

English first language, Afrikaans second language, Physics, Maths, Biology and Geography. Standard Grade subjects.

Professional experience

Advania Group

DEC 2016 - PRESENT | Formerly Content and Cloud

Cyber Security Engineer | September 2024 - Present

- Engineer Sentinel analytics rules, hunts, watchlists, and workbooks across client environments.
- Develop KQL investigations for suspicious identity, email, sign-in, and endpoint activity.
- Use Microsoft Defender and Sentinel telemetry to support threat hunting and incident investigation.
- Manage multi-client security content through Azure Lighthouse.
- Build Azure DevOps, Bicep, and PowerShell workflows for content validation and deployment.
- Develop SOC tooling with audit logging, role-based access, pre-checks, and approval workflows.
- Create incident exports and reporting workflows for monthly security reviews.

Technical Lead | April 2024 - September 2024

Senior Technical Specialist | April 2022 - April 2024

Senior Support Services Engineer | December 2016 - April 2022

Earlier technical roles covered infrastructure, Microsoft 365, Intune, identity, endpoint security, and client support.

Bowline Fulfillment (Pty) Ltd

APR 2007 - MAY 2016 | I.T Network Administrator

- Administered network infrastructure, servers, accounts, email, and connectivity.
- Provided desktop, network, and software support to 30 end users.
- Maintained DNS, DHCP, NAT, WINS, file services, backups, and data recovery.
- Reviewed firewall configurations quarterly and investigated suspicious emails.
- Managed technical inventories, Microsoft software audits, and licensing.
- Maintained CCTV monitoring, surveillance backups, and camera systems.

Hargrave Library Services

FEB 2003 - APR 2007 | Data Capturing

Customer liaison, quotations, tenders, sales, and administration. Desktop support, networking, troubleshooting, and SAP ERP systems.

S & L Electronics

APR 1999 - JUL 2002 | Administration / Data Capturing

Administration, data capturing, stock control, customer service, and sales.

References available on request.