MATHEWS K DANIEL

CLOUD SECURITY ARCHITECT

CONTACT

hi@mathewskdaniel.com
www.mathewskdaniel.com
@mathewskdaniel
@mathewskdaniel

SKILLS

- **Cloud Security Architecture**
- **Microsoft Sentinel Architecture**
- **Defender for Cloud CSPM & CNAPP**
- **Defender for Endpoint**
- **Defender for Office 365**
- **Azure Key Vault & Event Hubs**
- **Azure Firewall IDPS, WAF, DDoS**
- **Entra ID Security**
- **Azure PIM**
- **Terraform, Azure Logic Apps**
- **PowerShell, Python, Kusto Query Language (KQL) & JSON**
- **Cisco Secure NGIPS**
- **Trellix/McAfee NSP**
- **Palo Alto NGFW**
- **Cisco Secure Network Analytics (StealthWatch)**
- **Cisco ISE (ACS)/TACACS+**

CERTIFICATIONS

- **SC-100** - Microsoft Certified: Cybersecurity Architect Expert
- **SC-200** - Microsoft Certified: Security Operations Analyst Associate
- **AZ-500** - Microsoft Certified: Azure Security Engineer Associate
- **AZ-900** - Azure Fundamentals
- **CLF-C02** AWS Cloud Practitioner
- ITIL Foundation

TRAININGS/POC

- Microsoft Purview/Azure AIP
- Microsoft Copilot for Security Ninja
- Google SecOps (Chronicle)
- Trellix UCE/MVISION
- Wiz, Tenable CSPM
- Microsoft Defender for Cloud Apps(CASB)

EDUCATION

Bachelor of Engineering 2009-2013
Electrical & Electronics | UCE, Ariyalur
CGPA: 8.1/10

PROFILE

Security Architect with over 10 years of overall experience in Cloud Security, On-prem Security, SIEM/SOAR/CSPM/CNAPP, IDS/IPS, and NGFW technologies. A passionate security advocate seeking a dynamic role to enhance cloud security, privacy, and compliance.

WORK EXPERIENCE

Atos(Eviden) IT Solutions Pvt. Ltd.

Cloud Security Architect/Senior Consultant *2020 - PRESENT*

- Led multiple Greenfield and Brownfield Microsoft Sentinel deployment Projects, enhancing security visibility and posture by over 85%.
- Led SIEM migration to Microsoft Sentinel, reducing costs by 30% and improving detection and response efficiency by over 40%.
- Authored technical documentation and SOPs to standardize Sentinel platform management and security operations.
- Implemented CSPM & CNAPP with Microsoft Defender for Cloud, ensuring compliance (PCI DSS, ISO 27001, NIST, HIPAA) & Secure Score above 90%
- Designed and implemented Azure Key Vault for disk encryption, certificate, and secret management; architected Azure Event Hubs for centralized log collection to SIEMs; and deployed Azure WAF and DDoS Protection to secure public-facing applications.
- Secured Office 365 with EOP policies, SPF/DKIM/DMARC setup, and transport rules; reduced email/O365 based threats by 45 %
- Driven Defender for Endpoint (MDE) and Defender for Servers deployments, configuring AV, ASR & ATP polices improving endpoint security coverage by 40%.
- Configured and maintained Entra ID (Azure AD) Conditional Access Policies & Entra Privileged Identity Management (PIM).

Perimeter Security Engineer/Consultant *2017 - 2020*

- End-to-end management of Perimeter Security infrastructure, including deployment, configuration, OS upgrades, patching, security policy administration, rule base audits, third party integrations, migration and decommissioning of following.
  - Trellix/McAfee NSP
  - Cisco ISE (ACS)/TACACS+
  - Cisco Secure NGIPS & ASA
  - Palo Alto NGFW
  - Cisco Network Analytics(StealthWatch)
  - Vmware ESXi & Workstation

FIS (Fidelity Information Services Inc.)

Information Security Engineer Sr. 2015 - 2017

- Led L2 SOC operations, handling threat detection, investigation, threat hunting and response using SIEM, EDR, and threat intel tools like RSA Security Analytics, LogRhythm, Cisco FMC, McAfee ePO, and FireEye

ADDITIONAL INFORMATION

- Technophile, Privacy and FOSS Advocate.
- Passionate Homelab and Selfhosting enthusiast.
- Curious AI tinkerer, exploring GenAI tools, APIs, and self-hosting LLMs.
- Creative automation builder, developing Telegram bots for productivity and entertainment.
- Tech blogger, sharing insights at https://blog.mathewskdaniel.com
- Multilingual communicator, proficient in English, Malayalam, Tamil & Hindi.