GUTEMA DUBE

Roseville, MN • (612) 601-5051 • gutemafdube@gmail.com • gutemadube.com

Cybersecurity Professional | Identity Security & Engineering | Threat Hunting | Cloud Security & GRC

PROFESSIONAL SUMMARY

Cybersecurity professional with 10 years of IT experience, with a dedicated focus on cybersecurity since 2025. Currently serving as Cybersecurity Analyst and Security Engineering and Program Lead at Osseo Area Schools, delivering security engineering, threat hunting, governance program development, and identity security across a production environment. Skilled in vulnerability management, KQL-based threat hunting, incident response, detection engineering, identity and access management, and cloud security across AWS, Azure, and Google environments. Brings both technical depth and a strong collaborative approach, working across IT teams, security partners, and leadership to deliver measurable security outcomes.

CORE COMPETENCIES

Security Engineering & Operations: Microsoft Defender XDR, Red Canary MDR, Splunk, Microsoft unified security platform, KQL/Kusto threat hunting, detection engineering, vulnerability management (Nessus), incident response, continuous monitoring, Defender for Cloud Apps, App Governance, DLP, CASB, OWASP, MITRE ATT&CK

Identity & Access Management: Microsoft Entra ID, Google IAM, Active Directory, Office 365 Admin, MFA/SSO, conditional access, Zero Trust architecture, Group Policy, PIM, RBAC, privileged access management

Cloud & Infrastructure Security: AWS (SAA & CCP certified), Azure (Developer Associate, AZ-104/305 trained), hybrid cloud environments, network security, cryptography & encryption, IaC (ARM), CI/CD security, REST APIs

Scripting & Automation: PowerShell, Python, Bash, REST APIs, JSON, GitLab version control

GRC & Compliance: NIST CSF, NIST 800-53, ISO 27001, HIPAA, HITECH, FERPA, CIPA, risk register development, vendor risk management, audit documentation, tabletop exercise design, CompTIA Project+, ITIL 4 Foundation

IT Operations & Tooling: Intune, Jamf, Jira, Zendesk, Incident IQ, network troubleshooting, endpoint management

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst | Security Engineering & Program Lead | *Mar 2025 – Present*

Osseo Area Schools | Minneapolis, MN

- **Threat Hunting & Vulnerability Management:** Builds and executes custom KQL threat hunting queries informed by MITRE ATT&CK tactics and techniques to detect, analyze, and prioritize threats and vulnerabilities district-wide. Led a Log4Shell (CVE-2021-44228, CVSS 10.0) investigation that mapped every exposed device by device status, user context, physical location, and folder path, and drove full remediation to verified closure in collaboration with system administrators.
- **Detection Engineering & Monitoring:** Administers Microsoft Defender XDR district-wide; monitors endpoint, identity, cloud, and SaaS environments; tuned detections in collaboration with Red Canary MDR reducing alert noise by ~30%; manages Intune vulnerability workflows.
- **Identity & Access Management:** Administers Entra ID conditional access, Office 365 admin roles, Google IAM, and DLP; hardened MFA policies for all admin roles regardless of location or network; configured break-glass account exclusion logic; manages user security reviews and access lifecycle.
- **Cloud App Security & MDR Integration:** Enabled and configured Microsoft Defender for Cloud Apps and App Governance delivering full OAuth visibility and DLP across the environment. Conceived and drove Red Canary MDR integration with Entra ID Identity Protection in collaboration with the Red Canary security team and internal sysadmins, enabling automated IR playbook automation including token session revocation and additional response actions categorized by incident type and severity.
- **Governance, Risk & Compliance:** Designed NIST CSF governance framework, vendor risk tracking program, and risk register in collaboration with IT leadership; communicates security posture to leadership; authors compliance documentation aligned with HIPAA, FERPA, and HITECH.
- **Security Awareness & IR:** Collaborated with IT and leadership to elevate cybersecurity awareness across the organization through training and phishing simulations via Microsoft Attack Simulator. Actively

manages incidents from triage through containment and recovery; designed IR playbooks and tabletop exercises.

Lead IT Specialist | Independent Consultant | *Mar 2025 – Sep 2025*
Independent Consulting | Minneapolis, MN

- Conducted cybersecurity assessments, risk assessments, and IT audits; identified and remediated privilege gaps including excessive external consultant access; proposed and implemented Least Privilege, PIM, and RBAC strategies. Delivered prioritized remediation recommendations and compliance-aligned documentation.

Departmental IT Support Lead | *Nov 2022 – Apr 2024*
University of Minnesota | Minneapolis, MN

- Led endpoint rollout projects and infrastructure upgrades; aligned security configurations with HIPAA/FERPA compliance requirements in a regulated research environment; contributed to hardware and software validation testing.

IT Technician → Technology Coordinator | *Jan 2021 – Nov 2022*
Saint Paul Public Schools | Saint Paul, MN

- Advanced from technician to coordinator; managed endpoint security, patching, deployments, AD account lifecycle, and user security reviews across multiple sites within HIPAA/FERPA safeguards.

IT Field Technician | *Sep 2017 – Dec 2020*
Minneapolis Public Schools | Minneapolis, MN

- Provided field service across 10+ locations; coordinated technology deployments, security patching, and AD account management; documented recurring issues for systemic resolution.

SELECTED PROJECTS

Log4Shell (CVE-2021-44228) — Full Threat Investigation & Remediation | KQL / Microsoft Defender XDR
Custom KQL queries built to silently hunt Log4Shell exposure across a live production environment; mapped every exposed device by device status, user context, physical location, and folder path, and drove full remediation to verified closure in collaboration with system administrators.

Security Governance, Risk & Vendor Management Programs | NIST CSF / Built in Collaboration with IT Leadership
Designed and implemented a complete NIST CSF governance framework, risk register, and custom vendor risk tracking program with risk-based scoring — all built in collaboration with IT leadership without third-party GRC tooling. Supporting HIPAA, FERPA, and NIST CSF compliance requirements.

Identity Engineering — Conditional Access Hardening & MDR Integration | Microsoft Entra ID / Red Canary
Hardened Entra ID Conditional Access policies to enforce MFA for all admin roles from any location, with precise break-glass exclusion logic. Separately conceived and drove Red Canary MDR integration with Entra ID Identity Protection, enabling automated IR playbook triggers for identity-based threats — in collaboration with the Red Canary security team and internal sysadmins.

Full project portfolio available at gutemadube.com/projects

EDUCATION & CERTIFICATIONS

B.S., Cloud Computing — Western Governors University | July 2026
M.S., Cybersecurity (in progress)
University of Minnesota — 6-month Cybersecurity Boot Camp & 6-month Cloud Computing Bootcamp | 2023–2025
AI Fundamentals Nanodegree • AI Programming with Python — Udacity, 2025
Active Certifications: AWS Certified Solutions Architect – Associate • AWS Certified Cloud Practitioner • Microsoft Azure Developer Associate • CompTIA Cloud+ • CompTIA Project+ • ITIL® 4 Foundation • ISC2 Certified in Cybersecurity (CC)
In Progress: CCSP • CISSP