Matthew Downs

MATTHEWDOWNS225@GMAIL.COM | MATTHEW.DOWNS6@T-MOBILE.COM | (843) 499-7142 | Bellevue, WA
linkedin.com/in/matthew-downs2

Cybersecurity Engineer

I'm a cybersecurity engineer turning complex telemetry into actionable defense. With 5+ years in telecommunications, I've scaled enterprise log management pipelines at T-Mobile, connecting data across Cribl, NiFi, and Vector into Splunk, Sentinel, and XSOAR. My specialty is building people-focused ingestion workflows and automations that empower stakeholders to understand and mitigate cybersecurity risks—bridging the gap between technical visibility and organizational awareness.

CORE COMPETENCIES

Security Engineering
Telemetry pipeline design · Cribl · Vector · Apache NiFi · OCSF · Data normalization
SIEM integration · Splunk · Microsoft Sentinel · Anvilogic · Snowflake · XSOAR

Incident Response & Operations
ServiceNow (CMDB / IR modules) · Cortex XSOAR · Microsoft Defender · SentinelOne
Automation · Playbook development · Root-cause analysis · Compliance (PCI-DSS, CCPA, ISO 27001)

Cloud & Infrastructure
Azure · AWS · Linux · macOS · Network architecture · Log forwarding · Syslog / API integration

Scripting & Analytics
Python · PowerShell · Bash · SPL · KQL · SQL · Automation · Data correlation & enrichment

WORK EXPERIENCE

Cybersecurity Engineer, Program Lead – Threat Detection & Log Management (TDLM) *T-Mobile, Bellevue, WA | Oct 2025 – Present*
Focused on scalable telemetry ingestion and SIEM data governance across hybrid cloud infrastructure.
• Serve as program lead for the enterprise Threat Detection and Log Management (TDLM) initiative, ensuring consistent and compliant log ingestion across T-Mobile business units.
• Coordinate with application, infrastructure, and data owners to onboard critical log sources into the enterprise SIEM ecosystem.
• Design, maintain, and optimize data ingestion pipelines leveraging Cribl, Vector, and Apache NiFi for routing, transformation, and normalization of telemetry data.
• Integrate diverse log sources into downstream analytics platforms including Anvilogic, Cortex XSOAR, Microsoft Sentinel, Splunk, and Snowflake.
• Collaborate with detection engineering, threat hunting, and compliance teams to align ingestion standards with OCSF and internal governance frameworks.
• Lead documentation, onboarding workflows, and cross-team collaboration to enhance telemetry coverage and streamline data validation processes across the enterprise.

Analyst, Cybersecurity *T-Mobile, Bellevue, WA | May 2024 – Oct 2025*
• Led incident investigations and containment efforts using ServiceNow for ticket triage and CMDB correlation across assets and telemetry sources.
• Utilized Palo Alto Cortex XSOAR, Splunk, and Microsoft Defender to automate and enrich incident response workflows.

• Collaborated with internal threat-intel teams during multiple nation-state-aligned campaigns targeting telco infrastructure.
• Developed runbooks and escalation procedures improving mean time to respond (MTTR) and compliance with PCI-DSS, USGCI, CCPA, and ISO-27001 standards.
• Served as senior overnight analyst mentoring junior staff and ensuring consistent process adherence.

Associate Enterprise Info. Security Analyst *T-Mobile, Bellevue, WA | Dec 2023 – May 2024*
• Supported incident management through ServiceNow and XSOAR, managing large ticket volumes while ensuring SLA compliance.
• Performed CMDB-driven investigations correlating incidents with affected assets and applications.
• Partnered with threat-intel and detection engineering teams during high-severity investigations, providing data enrichment and context.
• Identified automation opportunities in ingestion and response workflows, improving operational efficiency.

EDUCATION

Trident Technical College, Charleston, SC | Associate Degree in Cyber-Security (2022 – Present)
Completed courses in HTML/CSS, Ethical Hacking, SECURITY+, NETWORK+, AWS, and Microsoft Server with a 4.0 GPA.

TECHNOLOGIES, CERTIFICATIONS & AWARDS

• Working toward SANS GIAC Certifications (expected 2025).
• Dean’s List (Fall 2022, Spring 2023, Fall 2023) with GPA 4.0.
• Experience with OpenVAS, Nessus, and LimaCharlie in home lab environments.
• Deployed and maintained multiple *nix and Windows virtual machines.