Caleb Winters

Murfreesboro, TN · caleb.winters@example.com · (615) 555-0145 · linkedin.com/in/example-caleb-winters

My Key Qualifications

- Currently a Junior Cyber Security Analyst at LifePoint Health, monitoring and triaging alerts in **Microsoft Sentinel and Splunk** for hospital and clinic systems.
- **35 tickets per week** handled under SOC runbooks, escalating confirmed incidents with documented evidence in ServiceNow.
- Phishing review for user-reported email in **Microsoft Defender for Office 365**: 180 messages analyzed over 6 months, first-response time cut **from 42 minutes to 28**.
- **CompTIA Security+** certified (2025) with a BS in Information Technology from Middle Tennessee State University.
- Built a Sentinel SOC lab in Azure for a university capstone: **6 KQL analytic rules** that detected 24 simulated attack events including brute-force and suspicious sign-ins.
- Team vulnerability review for a student health clinic using Qualys surfaced **17 high-severity findings**, 12 closed before handoff via a remediation tracker.

Experience

Junior Cyber Security Analyst — **LifePoint Health**, regional hospital and healthcare services operator

Nov 2025 – Present · 1 yr

- Monitor and triage security alerts across Microsoft Sentinel and Splunk covering endpoint, identity, and network events, handling an average of 35 tickets per week while meeting internal escalation timelines for confirmed incidents.
- Escalate higher-severity cases with documented evidence in ServiceNow, following SOC runbooks and validating alert context before handoff.
- Supported the team's phishing response workflow by analyzing user-reported email in Microsoft Defender for Office 365, reviewing 180 reported messages over 6 months and cutting average first-response time from 42 minutes to 28 minutes.
- Confirmed exposures with system owners and tracked remediation tickets through ServiceNow alongside infrastructure teams.

Education

- **Middle Tennessee State University** — Bachelor of Science in Information Technology · 2021 – 2025 · Relevant coursework: Network Security, Windows Systems Administration, Computer Networks, Digital Forensics, Information Security Risk Management

Sample resume made with Specific Resume · specificresume.com

Projects

- **Sentinel SOC Capstone**
  Built a small SOC lab in Microsoft Azure for a university capstone, ingesting Windows and firewall logs into Microsoft Sentinel and creating detections for suspicious sign-in and brute-force activity. The 6 analytic rules caught 24 simulated attack events during final testing.
  Tech: Microsoft Sentinel, Azure, Kusto Query Language (KQL), Windows Event Logs
- **Campus Clinic Vulnerability Review**
  Team project for a student health clinic reviewing workstation exposure, documenting common weaknesses, and recommending remediation priorities for IT staff. Identified 17 high-severity findings and built a remediation tracker the client used to close 12 before project handoff.
  Tech: Qualys, Microsoft Excel, Windows, TCP/IP

Skills

- **SIEM & Security Monitoring:** Microsoft Sentinel, Splunk, Kusto Query Language (KQL), Incident Triage
- **Vulnerability & Endpoint Security:** Tenable, Qualys, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Vulnerability Management
- **Identity & Email Security:** Active Directory, Phishing Analysis
- **Ticketing & Platforms:** ServiceNow, Windows

Certifications

- **CompTIA Security+** – CompTIA (2025)