Kevin Troy Thompson, CISSP

Kevin.Thompson@me.com | LinkedIn.com/in/KevinTroyThompson | www.ktt.pw

As a dedicated Security Content Engineer with a robust background in cybersecurity, I am currently spearheading security content development at ConnectWise, where I've progressed from a L1 Security Analyst to a Team Lead of Security Content, specializing in SIEM rule creation and optimization. My passion for cybersecurity extends into the realm of AI, where I explore how machine learning can revolutionize threat detection and response. With an MS in Cybersecurity Management and certifications like CISSP and NSE7, I am committed to enhancing security frameworks through innovative solutions and continuous learning. My goal is to bridge the gap between traditional cybersecurity measures and AI-driven strategies to create more resilient security systems.

EDUCATION and CERTIFICATIONS

University of Utah, David Eccles School of Business — Salt Lake City, UT
Master of Science, Cybersecurity Management — August 2023

University of Utah, David Eccles School of Business — Salt Lake City, UT
Bachelor of Science, Information Systems — May 2020

ISC2 Certifications

Certified Information Systems Security Professional (CISSP) — Issued Aug 2023

CompTIA Certifications

Security+, Linux+, and CySA+ — Issued 2019 - 2020

Fortinet Certifications

Fortinet NSE 7 Network Security Architect — Issued May 2022

EXPERIENCE

ConnectWise — Tampa, FL (Remote)

Team Lead, Security Content — April 2023 – Present

- Lead a team of security content engineers, driving innovation in CW SIEM and FortiSIEM rule creation and optimization
- Spearhead the implementation of CW SIEM's "Enhanced Alerting" feature, developing its initial ruleset
- Advise the development team on critical features and functionality to enhance SIEM capabilities
- Implement automation to assist the SOC with triaging and alert escalation
- Collaborate with cross-functional teams to align security content with evolving threat landscapes and client needs
- Mentor junior team members, fostering a culture of positivity, excellence, continuous learning, and professional development

Security Engineer — April 2022 – April 2023

- Developed and deployed advanced SIEM rules to proactively detect and mitigate emerging security threats across customer environments
- Performed in-depth analysis of security logs to identify opportunities for alerting and reporting, strengthening overall threat detection capabilities
- Provided expert-level support for FortiSIEM and ConnectWise SIEM platforms, including device configuration, user management, and customized report generation to meet specific customer requirements
- Leveraged SIEM tools to help customers successfully pass compliance audits, providing real-time monitoring and reporting for NIST 800-53, NIST 800-171, HIPAA, and other security standards, resulting in improved security posture and regulatory compliance
- Expertly troubleshot collector issues and data feed problems, ensuring seamless ingestion of security events for comprehensive monitoring
- Developed and delivered training to new cybersecurity engineers on FortiSIEM and ConnectWise SIEM usage and security best practices, enhancing team capabilities

Security Analyst Level 3 — July 2021 – April 2022

Security Analyst Level 1 — July 2021 – July 2020

- Conducted comprehensive daily security log analysis for 650+ clients, identifying and investigating potential indicators of compromise to ensure robust threat detection
- Collaborated with engineering teams to develop and fine-tune SIEM rules, significantly reducing false positives and enhancing threat detection accuracy
- Designed and delivered comprehensive training programs for new cybersecurity analysts, focusing on analytical processes and FortiSIEM proficiency, accelerating team onboarding and operational readiness

For more work experience information, please see my LinkedIn - LinkedIn.com/in/KevinTroyThompson