DOMINIK RIMPEL

San Antonio, Texas | 915-345-8837 | linkedin.com/in/dominik-rimpel-dr20 | dominikrimp14@gmail.com

PROFESSIONAL SUMMARY

Cybersecurity and Computer Science graduate at UTSA with 3+ years of hands-on SOC experience, including shift lead responsibilities in a 24/7 embedded SOC environment securing national energy infrastructure across OT and IT environments. Experienced in security monitoring, threat detection, incident response, and investigation using Microsoft Sentinel (KQL), Splunk, and Microsoft Defender. Skilled in developing detections, tuning rules, enriching threat intelligence feeds, and documenting incidents in ServiceNow. Track record of mentoring junior analysts on SOC workflows and security best practices.

CERTIFICATIONS

CompTIA CySA+ (CS0-003) | CompTIA Security+ (SY-701) | Microsoft Certified: Security Operations Analyst Associate (SC-200)

WORK EXPERIENCE

SOC Analyst 1 - BlackSwan Cybersecurity, San Antonio, Texas *July 2025 – Present*

- Assume shift lead responsibilities in a 24/7 embedded SOC environment supporting national energy infrastructure across OT and IT environments, leading off-hours and weekend incident response and ensuring operational continuity
- Monitor and analyze security events by developing KQL queries in Microsoft Azure Sentinel and a machine learning based network detection and response (NDR) tool to detect anomalies, investigate threats, and escalate incidents per SOC playbooks.
- Perform Tier 2 responsibilities including deeper incident investigation, threat hunting, and escalation support while maintaining Tier 1 coverage within the embedded SOC.
- Leverage ETL processes with threat intelligence feed to enrich detections, improve correlation, reduce false positives, and support proactive threat hunting.
- Classify, prioritize, and escalate alerts based on threat severity, ensuring timely incident response in a high-availability, mission-critical setting.
- Maintain detailed incident response documentation and post-incident reporting in ServiceNow to support SOC operations and ensure audit trail integrity
- Assume incident command during off-hours and weekend shifts, coordinating analyst response, escalating critical incidents, and ensuring continuity of SOC operations.
- Tune detection rules and refine workflows across SIEM and NDR platforms based on behavioral anomaly analysis to reduce false positives and improve detection fidelity.

SOC Security Analyst – University of Texas at San Antonio, San Antonio, Texas *Jan 2023 – July 2025*

- Monitor and analyze system and network logs using Splunk, Microsoft Defender, Carbon Black and ExtraHop to identify anomalous activities and potential threats on Windows and Linux devices.
- Evaluate and correlate security alerts from Abnormal AI and DUO Admin to determine severity and take mitigation actions or escalate incidents
- Conduct vulnerability assessments and risk analysis to identify and remediate security gaps
- Develop and optimize Splunk queries and dashboards using SPL for real-time threat detection, improving visibility and reducing incident response time
- Assisted security engineers with Python scripting and automation of security monitoring tasks using Extrahop
- Supported incident response efforts involving chain of custody procedures, acting as a witness during secure device handoff to maintain evidence integrity.
- Mentored and trained 15+ interns each semester on security best practices and SOC processes

PROJECTS

Desktop Malware Analysis

- Reverse-engineered mock malware deployed through endpoint management tools; traced infection paths via system and network logs, identified insider threat, and updated SOC playbooks to strengthen incident response

RowdyHacksX: Evil Twin Attack

- Spearheaded a team of Cyber and CS students to deploy a Raspberry Pi-based Evil Twin Attack at RowdyHacksX, suppressing legitimate access points and redirecting devices to a malicious network
- Developed a PHP-powered captive portal to harvest test user credentials, demonstrating wireless network vulnerabilities and raising awareness of Wi-Fi security risks

EDUCATION

The University of Texas at San Antonio

Bachelor of Science in Computer Science *Graduated: May 2026*