NUARI
NORWICH UNIVERSITY APPLIED RESEARCH INSTITUTES

Cybersecurity Analyst

Full-time | Remote | Security Operations

About NUARI

Norwich University Applied Research Institutes (NUARI) is a 501(c)(3) nonprofit applied research organization based in Northfield, Vermont. We work with government, industry, and academic partners to advance cybersecurity, critical infrastructure protection, and national security resilience. Our team operates at the intersection of research, technology, and real-world security operations, delivering work that has direct impact on public and private sector readiness.

NUARI is expanding its Security Operations Center (SOC) capability and is hiring analysts who want to be part of something meaningful. This is a rare opportunity to join a mission-driven team at the ground floor of a growing SOC, working alongside practitioners who have supported state, local, and government clients on some of the most consequential cybersecurity challenges in the public sector.

Role Overview

The Cybersecurity Analyst is a full-time remote position focused on monitoring, analyzing, and responding to security events across diverse customer environments. This role sits within NUARI's growing managed SOC function and works across a customer base that includes state, local, and government organizations, regulated industries, and critical infrastructure operators.

You will investigate alerts, triage incidents, and support containment and remediation of threats. You will also contribute to the continued improvement of NUARI's SOC processes, tooling, and customer documentation.

Responsibilities

- Monitor security events and alerts across customer environments using SIEM and related tooling
- Perform incident triage: classify, prioritize, escalate, and document security events according to defined runbooks
- Conduct log review, correlation analysis, and initial malware and vulnerability triage
- Assess application and network security configurations and identify anomalies or misconfigurations
- Collaborate with technical and non-technical stakeholders to communicate risk and findings clearly
- Produce accurate, well-organized incident documentation and customer-facing reports
- Support the development and refinement of SOC runbooks, procedures, and detection logic
- Contribute to customer onboarding activities including asset inventory review and log source validation
- Participate in shift coverage as NUARI's SOC scales toward 24/7 operations

Qualifications

Required:

- Must be a U.S. Citizen
- 3+ years' experience in a professional work environment
- Demonstrated experience in cybersecurity operations: threat analysis, incident response, or security monitoring
- Familiarity with network security concepts including traffic analysis, anomaly detection, and defensive controls
- Experience with the Elastic SIEM stack (Elasticsearch, Kibana, Elastic Security); familiarity with other platforms such as Microsoft Sentinel or Splunk is a plus

- Strong written communication skills; ability to document incidents and findings clearly for both technical and non-technical audiences
- Ability to work independently in a remote environment, manage concurrent tasks, and communicate proactively with a distributed team
- Bachelor's degree in Cybersecurity, Computer Science, Information Technology, or a related field, OR equivalent practical experience
- Eligible to obtain and maintain a U.S. Department of War personal security clearance

Preferred:

- Relevant certifications: Security+, CySA+, GSEC, CEH, or equivalent
- Experience with Microsoft 365 security tooling (Defender, Purview, Entra ID)
- Familiarity with compliance frameworks: NIST CSF, CMMC, NIST 800-171, or CIS Controls
- Application security experience including common vulnerability classes and secure configuration review
- Malware analysis fundamentals: identifying indicators of compromise and supporting remediation
- Experience in a managed security service or multi-customer SOC environment

What We Offer

- Mission-driven work with direct national security relevance
- Fully remote position with flexibility
- Exposure to state, local, government, and critical infrastructure customer environments
- Opportunity to grow within a rapidly expanding SOC function
- Collaborative environment with experienced cybersecurity professionals
- Competitive compensation commensurate with experience, anticipated salary range of $65K - $85K

How to Apply

Submit your resume and cover letter describing your SOC or incident response experience to info@nuari.org with the subject line: Cybersecurity Analyst Application. Applications are reviewed on a rolling basis.

Norwich University Applied Research Institutes is an Equal Opportunity/Affirmative Action Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex or national origin. Applications from women and people of diverse racial, ethnic, and cultural backgrounds are encouraged. Please visit https://nuari.org for more information.