
PRIYA THAPA

New York

priyathapa2506@gmail.com | LinkedIn: linkedin.com/in/priyathapa07 | GitHub: github.com/priyathapa07 | Blog: darktrace.com/people/priya-thapa

PROFESSIONAL SUMMARY

Cybersecurity Analyst with 4.5+ years of hands-on experience in threat investigation, Security Operations Center (SOC) environments, and data-driven threat intelligence. Proven track record in developing and tuning detection logic, building behavioral models, and conducting deep analytical research on emerging cyber threats. Adept at cross-functional collaboration to enhance detection coverage, reduce insider risk, and strengthen overall security posture. Driven to apply advanced analytics and automation to strengthen threat detection, streamline SOC workflows, and elevate enterprise-wide cyber resilience.

SKILLS

- Security and Monitoring Tools: Darktrace, Wireshark, Nessus, Nmap, Snort, Shodan, Splunk, Elastic Stack, OpenSearch
 - Databases: SQL Server, Firebase
 - Operating Systems and Platforms: Linux (Kali, Ubuntu), windows server, Metasploit
 - Cybersecurity Frameworks: MITRE ATT&CK, NIST Cybersecurity Framework (CSF), NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection)
 - Languages: Java, HTML, CSS, Python, R
 - IDE Tools: IntelliJ Idea, Spring Tool Suite
 - Version Control: GitLab, GitHub, SVN
 - Frameworks and Architectures: Spring, RESTful Services, MVC
-

WORK HISTORY

Darktrace – New York, NY

Senior Cyber Analyst, August 2025 – Present

- Lead efforts as a core member of the Model Development Team, designing, refining, and tuning advanced detection and response models focused on insider threats and emerging cyber risks; resolved 40+ model performance and tuning issues, driving measurable improvements in detection accuracy and coverage.
- Collaborate cross-functionally to improve existing detection logic and develop new models in response to evolving attack techniques; independently created 5+ new detection models through hands-on experimentation and threat research, leveraging global threat intelligence and telemetry data to identify novel threat patterns and integrate findings into Darktrace's detection framework.
- Contribute to the Threat Intelligence team by conducting research, threat hunting and sharing insights across the organization; authored 1 technical blog, delivered 2 team-wide presentations, and currently finalizing the AMS Threat Trend Report to highlight emerging patterns observed in client environments.
- Oversee complex threat investigations within the SOC, leading investigations into high-priority case along with incident response and management team and producing detailed SPOT reports that inform strategic response; develop standardized workflows and author training resources to elevate team performance and ensure procedural consistency.
- Mentor new analysts through structured onboarding, weekly office hours, and hands-on labs; deliver team-wide presentations on emerging cyber threats, detection techniques, and practical demos to foster continuous learning and operational excellence.

Cyber Analyst, Oct 2022 – July 2025

- Leveraged Darktrace's suite of tools to proactively monitor network activity and generate 5–7 daily Threat Intelligence Reports addressing potential threats and observed alerts.
- Conducted both real-time and retrospective threat analysis within a Security Operations Center (SOC) and authored detailed 3-5 SPOT reports that informed executive-level threat response, based on deep-dive investigations of suspicious behavior.
- Applied advanced analytics and data visualization techniques using EKL, Python, SQL, and advanced Excel to clean, analyze, and interpret datasets ranging from hundreds to millions of records; uncovered threat patterns and produced 2+ strategic threat trend reports over 2 years and published around 2 threat blogs.
- Collaborated with the model development team to create and optimize 10+ Darktrace's detection and respond models, leveraging deep threat research and experimentation with emerging vulnerabilities to enhance SOC detection capabilities.

Cyber Technology Specialist, May 2021- Oct 2022

- Acted as the principal technical liaison between clients, strategic partners, and internal stakeholders, translating complex threat intelligence into actionable insights and aligning detection strategies with business objectives.
- Delivered 50+ tailored threat intelligence briefings and analytical reports to diverse audiences, ranging from SOC analysts to C-level executives, enabling informed decision-making and proactive risk mitigation.
- Managed the operational integrity of 100+ client deployments, ensuring seamless integration, optimal performance, and continuous alignment with evolving threat landscapes and organizational needs.

Key Achievement:

- Achieved top 5 ranking in Darktrace RESPOND competition 2021 Cyber Engineer and Technician (CET) category by optimizing Darktrace Antigena Network for clients' environment.

Allari Inc– New York, NY

Cybersecurity Researcher and Content Writer, Nov 2020 – May 2021

- Leveraged cybersecurity and cyberspace operations expertise to conduct research and author over 20 articles.
- Conveyed highly complex cybersecurity topics that meet the objectives and goals of the intended audience.

Consolidated Edison, Inc – New York, NY

Security and Compliance Analyst, Jun 2019 – Jun 2020

- Configured the backend of the company's software, Change Gear, to facilitate smooth database management of over 100,000 companies' cybersecurity assets.
- Stayed up to date on NERC CIP Standards policies that the company upholds to protect critical cyber assets.
- Conducted vulnerability assessments on 20-30 cyber assets, including HMI, PLCs, and operational technology, in a test lab using tools such as Metasploit, Ubuntu Armitage, Nmap, and Nessus.
- Developed automation solutions using PowerShell, Bash, and other programming languages to manage 100,000 files and folders.

EDUCATION

Master's in information technology: University of the Cumberlands | *GPA: 4.0*

Bachelor of Science in Computer Science Information System and Security: John Jay College of Criminal Justice, CUNY | *GPA: 3.75 | Magna Cum Laude honors | Dean's List Honoree*

ACCOMPLISHMENTS

- **Certifications:** Cisco Networking and Cybersecurity Essentials, Darktrace Analyst, IBM Cloud for the Enterprise demonstrating strong foundational and applied expertise across network security, threat detection, and cloud technologies.
- **Leadership:** Executive Board Member of ISACA at John Jay College, actively shaping cybersecurity education and governance initiatives for the student chapter.
- **Community Engagement:** Volunteer with Microsoft Philanthropies' TEALS program and mentor for the CyberGirls Fellowship, supporting cybersecurity education and career development for underrepresented groups.
- **Recognition:** Achieved 3rd place in the [2020 ISACA Student Cybersecurity Case Competition](#) (New York Metropolitan Chapter), showcasing analytical and strategic problem-solving in real-world threat scenarios.
- **Professional Contributions:** CSFI (Cyber Security Forum Initiative) Volunteer, contributing to research and collaborative defense efforts within the global cybersecurity community.