

SHUBHAM PRIYADARSHI

CYBER SECURITY ANALYST

📍 Noida • 📞 +917247577207 • ✉️ shubhampriyadarshi342@gmail.com

🌐 <https://www.linkedin.com/in/shubhampriyadarshi342/>

SUMMARY

Over 3.6 years of professional experience as a Cyber Security Analyst, driven by integrity, curiosity, and innovative thinking. Proven ability to analyze security trends and patterns across the cyber threat landscape and develop robust strategies to protect systems, networks, and sensitive data. Skilled in implementing security frameworks that ensure the resilience of businesses and client environments. A natural communicator with strong interpersonal and motivational skills, capable of building, mentoring, and leading successful teams to drive collaboration and achieve organizational security objectives effectively.

TECHNICAL SKILL

- MITRE Attack Framework
 - Threat Hunting
 - Ethical Hacking
 - Kusto Query Language
 - EDR
 - Log Analysis
 - CrowdStrike Falcon
 - Networking
 - Windows Internals
 - Splunk
 - Azure AD
 - Incident Response
 - Detection Rule
 - SOAR
-

WORK EXPERIENCE

Job Title: Cyber Security Analyst

June 2022-Current

Company: LTIMindtree

Project: DEX-H

- Proactively manage and respond to security threats and incidents by analyzing the system artifacts, including system files, running processes, and network connections, to detect and mitigate compromises such as malware, phishing, drive-by attacks, accidental data leaks, and internal data spillage.
- Leverage expertise in networking fundamentals, application protocols, system architecture, and basic software development to identify vulnerabilities and implement effective solutions.
- Coordinate with cross-functional teams to develop and execute remediation plans while escalating critical security concerns to customers.
- Continuously monitor emerging technologies and evolving threats, proactively adapting knowledge and processes to enhance the organization's capability to detect, investigate, and effectively resolve security incidents.

Job Title: Cyber Security Analyst

Feb 2022 - May 2022

Company: LTIMindtree

Project: DEX-E

- Monitored and analyzed endpoint alerts and telemetry from EDR platforms to detect and respond to advanced threats.
- Investigated suspicious activity such as privilege escalation, lateral movement, malware execution, and persistence techniques using EDR tools and log data.
- Performed root cause analysis and threat hunting based on indicators of compromise (IOCs) and MITRE ATT&CK techniques.
- Responded to security incidents, including containment, eradication, and recovery on compromised hosts.
- Developed and fine-tuned custom EDR detection rules to improve coverage and reduce false positives.
- Collaborated with threat intelligence, SOC, and IR teams to escalate and correlate multi-stage attacks.
- Created detailed incident reports and documentation for post-incident analysis and compliance requirements.

KEY ACHIEVEMENTS

- Reduced false positives by 30% through continuous tuning of detection rules.
- Led containment and remediation of a ransomware incident, preventing lateral spread across 300+ endpoints.
- Conducted monthly threat hunting exercises that uncovered previously undetected malicious persistence mechanisms.

ROLES AND RESPONSIBILITIES

- Filling the daily health, handling the incidents, and working with SLA.
- Working with the customer in the development of the project as a part of the pilot batch.
- Creation of metrics and dashboards and trackers and analyzing daily, weekly, and monthly reports on incidents.

CERTIFICATES

- GenAI
- SIEM
- CEH

EDUCATION

Bachelor of engineering from Sagar Institute of Research & Technology Excellence Bhopal (2015-2019).