Sutanu Kumar Ghosh

312-792-9189 | sghosh34@uic.edu | linkedin.com/sutanu-ghosh | sutanughosh.com

Cybersecurity researcher specializing in threat detection and automated incident response. A final-year PhD Candidate in Computer Science with a proven track record of developing novel frameworks that significantly reduce threat exposure and response times in network environments.

Technical Skills

Languages & OS: Python, C/C++, SQL, Bash, Git, Custom Scripting Language, Microsoft 365, Linux, macOS, Windows
Security Tools: Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), Wireshark, Nmap, Metasploit, Caldera, BloodHound, YARA, Sigma, PowerShell, EnCase, Volatility, EDR, Firewalls, Audit Logging
Frameworks & Standards: Mitre ATT&CK & TTP, NIST (CSF, AI RMF), ISO (27001, 42001), OWASP Top 10, Compliance (SOC 2, PCI-DSS, HIPAA), Microsoft Purview, AI Governance, AI Risk Management
Cloud & Virtualization: AWS (IAM, S3, EC2, CloudTrail, Athena), Entra ID, Docker, VMware, Kafka
AI/ML & Data Analysis: PyTorch, Reinforcement Learning, Large-Scale Data Analysis, Threat Modeling, Anomaly Detection, Natural Language Processing (NLP)
Security Concepts: Incident Response (IR), Digital Forensics (DFIR), Threat Hunting & Cyber Threat Intelligence (CTI), SIEM Engineering, Alert Correlation, Red Teaming, Vulnerability Assessment, Web Protocols, Network Security, SAML, LDAP.

Work Experience

Discovery Partners Institute, University of Illinois System. Chicago, IL
Researcher 10/2024 – Present

- Engineered a novel, AI-driven incident response framework using reinforcement learning that autonomously blocked 78% of multi-stage APT attacks in a simulated enterprise environment, cutting Mean Time to Respond (MTTR) by 55% and drastically reducing security risk exposure.
- Designed and implemented advanced detection logic based on Mitre ATT&CK TTPs and audit log anomaly patterns, improving threat detection accuracy and providing high-fidelity alerts for SIEM integration.
- Correlated and analyzed telemetry from disparate sources, including audit logs, EDR, and network traffic to reconstruct complex, multi-stage attack chains and identify key adversary infrastructure.
- Led research collaboration across a cross-functional team of faculty and graduate students; mentored a Master's student, guiding their thesis research on automated threat mitigation.

Systems & Internet Security Lab, University of Illinois Chicago. Chicago, IL
Graduate Research Assistant 01/2019 – 09/2024

- Developed OSTINATO, a cross-host attack correlation framework that leveraged attack activity similarity detection to automatically group related alerts, reducing security analyst investigation time by 30% and minimizing alert fatigue.
- Pioneered the CITAR framework, a Cyber Threat Intelligence (CTI)-driven system that reconstructed sophisticated attack graphs from low-level system events, enabling proactive threat hunting and attribution.
- Architected and generated large-scale, realistic datasets simulating enterprise networks under attack, enabling robust validation and performance benchmarking of various cybersecurity defense frameworks.
- Investigated and triaged thousands of security alerts from SIEM platforms (Splunk, ELK) to evaluate framework performance, resulting in a 40% reduction in false positive rates through refined detection logic.

Education

University of Illinois Chicago Chicago, IL
Doctor of Philosophy (Ph.D.) in Computer Science 08/2018 – 09/2025 (expected)
Advised by Dr. Venkat — Focus on cyber attack detection, alert correlation, and incident response frameworks
Master of Science (M.S.) in Computer Science, awarded en route, GPA: 3.7/4.0 03/2024
Relevant Courses: Secure Computer Systems, Security Foundations, Computer Algorithms, Operating Systems

West Bengal University of Technology Kolkata, India
Bachelor of Technology (B.Tech.) in Computer Science & Engineering, GPA: 8.2/10 08/2014 – 12/2017

Selected Publications

- **Sutanu Kumar Ghosh**, R.Gjomemo, and V.N.Venkatakrishnan. "Citar: Cyberthreat Intelligence-driven Attack Reconstruction". *Proceedings of The 15th ACM Conference on Data and Application Security and Privacy (CODASPY '25).* 2025.

- **Sutanu Kumar Ghosh**, K.Satvat, R.Gjomemo, and V.N.Venkatakrishnan. "Ostinato: Cross-host Attack Correlation through Attack Activity Similarity Detection". *Proceedings of the 18th International Conference on Information Systems Security (ICISS '22)* 2022.

Awards

Best Paper Award @ *18th International Conference on Information Systems Security (ICISS) 2022* 12/2022
NSF Student Travel Award @ ACM CODASPY 2025 04/2025
Award for Graduate Research @ University of Illinois Chicago. 06/2025