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

Cybersecurity-focused PhD candidate with 6+ years of experience in threat detection, alert correlation, and incident response. Proven ability to build robust frameworks and collaborate across teams.

Education

University of Illinois Chicago Chicago, IL
Doctor of Philosophy (Ph.D.) in Computer Science 08/2018 – 07/2025 (expected)
Advised by Dr. Venkat — Focus on cyber attack detection, alert correlation, and incident response frameworks
Master of Science (M.S.) in Computer Science, GPA: 3.7/4.0 08/2018 – 03/2024
Elective Courses: Secure Computer Systems, Security Foundations, Computer Algorithms, Operating Systems
West Bengal University of Technology Kolkata, India
Bachelor of Technology (B.Tech.) in Computer Sc. & Engineering, GPA: 8.2/10 08/2014 – 12/2017
Elective Courses: Algorithms, Compilers, OOPs, Computer Networks, Discrete Maths, Network Security

Technical Skills

Languages & OS: Python, C/C++, SQL, Bash, Custom Scripting Language, MO365, Linux, Mac, Windows, VMWare
Frameworks & Tools: Metasploit, Nmap, Wireshark, Cyber Threat Intelligence (CTI), Cyber-threat (Apt) Detection & Correlation, Splunk, Mitre ATT&CK, Ttps, Sigma, Red-team Engagements (Caldera), SAML, Kafka, Audit Logging, OWASP, CTFs, Active Directory, BloodHound, DFIR, EDR, API, ELK, YARA, LDAP, Knowledge of AWS (IAM, S3, EC2, CloudTrail, Athena), CSFs (NIST, ISO 27001, PCI, SOC 2, HIPAA), Reinforcement Learning, Web Protocols, Network/Application/AI Security, Forensic Analysis, Large Scale Data Analysis, Incident Response.
Misc: Git, Docker, VS Code, PyTorch.

Work Experience

Discovery Partners Institute, University of Illinois System. Chicago, IL
Graduate Research Assistant 10/2024 – Present
- Collaboration with cross-functional teams including faculty, staff scientists, and graduate students to develop security frameworks; mentored a master's student on thesis-driven research.
- Engineered a near real-time incident response framework that autonomously blocked up to 78% of cyber (Apt) attacks, reducing incident response times by up to 55%.
- Designed detection logic based on Mitre Att&ck Ttps, audit log anomaly patterns and endpoint telemetry to identify intrusions.
- Investigated and triaged security alerts from SIEM platforms for comprehensive framework evaluations.
- Correlated data across audit logs, endpoints, and network traffic to identify multi-stage cyber attacks.

Systems & Internet Security Lab, University of Illinois Chicago. Chicago, IL
Graduate Research Assistant 01/2019 – 09/2024
- Developed a cross-host attack correlation framework that used similarity detection to reduce investigation time by 30%, pinpoint key Apt patterns, expediting responses and reducing false positives.
- Created large datasets and designed experiments to simulate real-world cyber attack scenarios and evaluated different cybersecurity frameworks.

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** and R.Gjomemo. "Detection and Threat-Hunting Approaches for Advanced Persistent Threats". *Encyclopedia of Cryptography, Security and Privacy* 2024.
- **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