Updated: November 2024

Richa Priyanka

itsrichap@gmail.com pagesweturned.com priyankaricha

Research Interests

Network Security, Internet Measurement, Information Integrity & Privacy, Threat Intelligence

Education

University of Michigan **Present**

Doctor of Philosophy (Ph.D.) in Computer Science

Relevant Coursework: *Advanced Computer Networks, Human-AI*

Georgia Institute of Technology **December 2023**

Master of Science (M.S.) in Cybersecurity (Information Security)

Relevant Coursework: *Secure Computer Systems, Network Security, Applied Cryptography, Data Analytics & Security, Enterprise Cybersecurity Management, Binary Exploit Lab, Security Incidence Response*

Kalinga Institute of Industrial Technology **May 2016**

Bachelor of Technology (Honours) in Electronics and Telecommunications

Professional Experience

Palo Alto Networks **March 2020 – August 2025**

Solutions Architect, Cortex

- Led Cortex XSOAR proof of concepts (POCs) for strategic clients in India, SAARC, and North America bringing in over 10 million in business just in 2022.
- Created threat actor and campaign trackers by correlating information from threat intelligence sources with the active incidents in an organization to enhance visibility into active critical threats in an organization.
- Formulated an algorithm that uses parameters like an indicator's age, associated incidents, and reporters' admiralty distribution to calculate a threat score of the Indicator of Compromise (IOCs). This solution helps analysts from the target Fortune 500 company prioritize critical threats from 250k+ indicators per day.
- Integrated all firewalls, endpoint security, SIEM and communication tools and created automated workflows for security analysts to investigate and respond to security incidents, supporting the BlackHat NOC.
- Created data parsers, mappers, and correlation rules for stitching event logs from more than 20 security sensors in Cortex XSIAM. Created workflows to semi-automatically hunt for signatures from active threat campaigns.
- Designed solutions to lower the overall time taken to investigate and respond to security incidents for large strategic customers from several hours to under 5 minutes.
  - Developed integrations with third-party tools using Python or Javascript to interact with all products needed in the incident response cycle from a unified console.
  - Authored playbooks to define and automate end-to-end investigation and response processes for scenarios like phishing, malware, and account compromise, automating up to 90% of the incidents hitting the SOC queue.
  - Embedded benchmarks and measurements in the processes to measure the effectiveness of incident response and created self-healing and escalation workflows to handle system and process disruptions.

Cyware Labs **August 2019 – Feb. 2020**

Solution Scientist

- Worked closely with product engineering teams to design threat intelligence analysis and sharing features in CTIX and CSAP to facilitate proactive threat analysis.
- Designed bi-directional threat intelligence sharing workflow for a major financial information sharing center (ISAC) with more than 250 members using CTIX and CSAP.
  - The threat intelligence exchange solution accepted threat incident reports from analysts from 250+ member organizations using a member portal.

    - The solution aggregated and enriched indicators of compromise collected from the report, and forwarded processed information to ISAC analysts.
    - The analyzed indicators of compromise, along with an automatically curated report are shared with the member community via STIX/TAXII and through the member portal.

Deloitte **July 2016 – July 2019**

Associate Solution Advisor

- Redesigned the security operations of a major financial bank by migrating them to Phantom (SOAR), integrating their SIEM, WAF, EDR, email security, and threat intelligence.
- Established the innovation team to drive efficient cyber risk advisory services.
    - Created a Robotic Process Automation (RPA) tool to completely automate the role management process on Oracle Cloud.
    - Created a lightweight tool to automatically onboard new applications on Sailpoint following precise security configurations based on the application category.
    - Developed a patch management system for vulnerable assets to identify device owners, provide visibility into risky assets, and automate patching.

Honors & Awards

- Best Solutions Architect for Cortex - Palo Alto Networks
- Innovation Award for creating automation solutions to increase ROI for the managed services team - Deloitte
- Client service award by a Fortune 500 client for exceptional performance during incident response - Deloitte

Projects

Safe Service Workers **August 2023**

Skills: C++, Javascript, Python, ML, Web Security

- Analyzed thousands of websites that support Web Push Notifications (WPNs) for my MS Thesis project; remotely advised by Dr. Mustaque Ahamad
- Analyzed 3K websites to develop a tool to detect if the website misuses service workers to trigger malicious notifications with 96% recall and 98% accuracy.

Blockchain federated identity **February 2018**

Skills: Ethereum, Python, React, Identity & Access Management

- Implemented a private, decentralized Identity Verification solution to create a federated service for users to create or update their identity with federal agencies like DMV.
- The solution employed a Proof-of-Authority based consensus algorithm to validate changes in a user's identity attributes. The underlying cryptographic chain was used to ensure that the data stored is tamper-resistant.

Risk-based threat and vulnerability management **April 2022**

Skills: Python, Javascript, Neo4j, Threat intelligence, Vulnerability management

- Developed a proof-of-concept solution to quantify risk across vulnerable assets, by correlating with threat intelligence and information about active security violations on the assets.
- The solution provided a unified interface to investigate critical vulnerable assets and provided visibility into the riskiest vectors for large organizations with segregated business units.

Social media scraping detection and analysis **August 2023**

Skills: SOAR, Python, Github, Web-scraping

- Created a proof-of-concept to discover social-media data scraping projects on Github by analyzing 200k+ public repositories.
- Created for a large social media company, the project identifies repositories that are accessing disallowed or risky endpoints for scanning.
- Designed a threat actor tracking system by correlating intel from the deep and dark web forums to identify actors who perform unauthorized scraping and subsequently sell that data on the dark net.

Teaching & Workshop Experience

Workshops

- Delivered Threat Intel Management sessions in a premier summit for Security Operation, Symphony, and other conferences.
- Represented Palo Alto Networks at conferences - Symphony and Ignite.
- Represented Cyware Labs at the Annual Information Security Summit 2019.

Mentorship

- Delivered comprehensive training to system engineers and product partners on creating an orchestrated SOC with integrated threat intelligence.
- Mentored interns and new hires through in-depth knowledge transfer focused on RPA & Blockchain.
- Led hands-on training sessions for managed services practitioners for RPA tools - UiPath, Automation Anywhere & BluePrism.

Teach for India

- Actively volunteered to tutor underprivileged middle school students in shelter homes, helping Teach for India achieve its goal to ensure all children in need of care and protection are able to realize long-term outcomes equitable with the middle-class.