Janarth Dheenadhayalan

janarth.dheenadhayalan@gmail.com | janarthd.com | LinkedIn

Summary

Software engineer with 5+ years of experience spanning security and infrastructure, with published research at IEEE S&P and USENIX Security (250+ total citations). Currently building detection and response systems at Microsoft; previously engineering high-performance networking infrastructure at AWS.

Technical Skills

Languages: Python, C#, C, C++, KQL | **Cloud:** Azure, AWS
Security: Detection Engineering, Threat Hunting, Incident Response, Threat Modeling, MITRE ATT&CK
Systems: Distributed Systems, Low-latency Networking, Packet Processing, Multithreading
AI: AI-Assisted Development, Agentic Coding Workflows, Context Engineering, LLM Integration

Experience

Microsoft — OneDrive/SharePoint Security Detection & Response Redmond, WA
Software Development Engineer II *July 2024 – Present*

- Re-engineered proactive blocking system from hardcoded rules to a dynamic architecture leveraging Entra identity token signals, evaluating hundreds of thousands of requests daily and catching real threats that resulted in direct customer notification
- Architected a degraded detection classification system that automatically flags detections missing critical data across thousands of rules, reducing on-call triage time and making it easy to onboard new detections
- Authored and shipped detection rules end-to-end mapped to MITRE ATT&CK techniques, designing a validation framework governing how detections are promoted from initial alerts through paging-level severity
- Led security investigations and major incident responses across OneDrive and SharePoint services; ran weekly threat model reviews and acted on findings
- Hunted for threats proactively via KQL and built dashboards to track detection health across the pipeline

Amazon Web Services — EC2 Networking Seattle, WA
Software Development Engineer II *February 2021 – June 2024*

- Designed fully automated device remediation workflow in Python covering 100K+ devices worldwide, reducing weekly sev2 alerts by over 70% (from 60–80 to approximately 20) and saving 10+ hours of manual work per week
- Owned the security review process for a 120-engineer organization, ran security architecture reviews across all teams, and pushed through compliance with U.S. (FedRAMP), U.K., and Chinese government regulations
- Implemented low-latency packet filtering system in C to drop bogon packets on internet egress traffic with only 5–10 clock cycle overhead
- Engineered noisy-neighbor mitigation in C++ to isolate workloads across customers on shared hardware
- Mentored intern through full project lifecycle; they received and accepted a return offer

Publications

250+ total citations

"Are Consumers Willing to Pay for Security and Privacy of IoT Devices?" — *USENIX Security*, 2023

"An Informative Security and Privacy 'Nutrition' Label for Internet of Things Devices" — *IEEE Security & Privacy*, 2022

"Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices?" — *IEEE S&P (Oakland)*, 2021

"Denial of Service Exploits on CUDA Devices Using Clock Function" — *UIUC Senior Thesis*, 2019

Education

Carnegie Mellon University Pittsburgh, PA
M.S. Electrical and Computer Engineering *December 2020*

University of Illinois at Urbana-Champaign Urbana, IL
B.S. Computer Engineering, Minor in Mathematics *May 2019*