Pham Ngoc Van

Cybersecurity Analyst

☎ (+84) 978 103 197 | ✉ phamngocvan.kma@gmail.com | linkedin.com/in/vanpn

Summary

I am a Cybersecurity Analyst with solid experience in Threat Hunting, Malware Analysis, and Vulnerability Assessment. I have worked across both cloud platforms (AWS, GCP, Azure) and containerized environments (Docker, K8s), as well as traditional on-premise infrastructure.

My background includes developing security automation tools, performing audits, and delivering actionable threat intelligence. I regularly support SOC teams in enhancing detection capabilities and incident response effectiveness.

I am also exploring AI and Machine Learning to advance threat detection through behavioral analysis and malware classification, aiming to strengthen proactive defense strategies.

Skills

OS	Linux, Windows, AIX
Databases	MySQL, SQLite, Elasticsearch
Cloud	AWS, GCP, Azure, Terraform
Container	Kubernetes (K8s), Tanzu, Docker
Languages	C/C++, Python, Golang, JavaScript, Bash, PowerShell
Frameworks	Flask, Vue.js, Node.js, Express.js, Django
Security Tools	Wireshark, Volatility, IDA Pro, Ghidra, Nmap, Cuckoo Sandbox, Tenable Nessus
Threat Hunting	Elastic Stack (ELK), YARA
Development	Git, GitLab, Ansible, Shell Scripting
Soft Skills	Analytical Thinking, Problem-Solving, Research, Collaboration, Time Management

Experience

Military Commercial Joint Stock Bank - MBBank **Jun 2021 – Present**

Cyber Security Analyst — Information Security Center

- Conducted proactive threat hunting to identify and mitigate potential cyber threats, including malware, network intrusions, and vulnerabilities.
- Led a cybersecurity team of 3 members, managing daily operations, assigning tasks, and mentoring team members in threat hunting, security auditing, vulnerability assessments, and security automation development.
- Performed security audits and vulnerability assessments across servers, applications, and network infrastructure, using tools such as Tenable Nessus and Core Impact to identify, validate, and prioritize security issues.
- Collaborated with Red Team and Pentest teams to validate security defenses and enhance overall security posture.
- Developed custom security automation tools to streamline audits and improve detection efficiency.
- Coordinated incident response efforts, supporting the SOC team with forensic analysis and actionable recommendations.
- Maintained and updated security checklists and documentation in alignment with CIS, NIST, and PCI DSS standards.
- Conducted research on emerging threats, tools, and tactics to stay ahead of evolving cyber risks.
- Proposed and implemented system hardening strategies to reduce attack surfaces and improve baseline security.

Bkav Corporation **Jun 2018 – May 2021**

Malware Analyst — Malware Research Center

- Worked at the Malware Research Center, specializing in reverse engineering and behavioral analysis of malware samples across various platforms (Windows, Linux, etc.).
- Analyzed and reverse-engineered malware to understand its behavior, persistence mechanisms, and objectives.
- Identified malware capabilities, classified threat families, and assessed potential impact on organizations.
- Researched new malware trends, evasion techniques, and threat actor TTPs to support threat intelligence efforts.
- Developed and implemented countermeasures to contain and prevent malware infections.
- Conducted malware detection, in-depth analysis, and remediation for enterprise clients and partners.
- Contributed to the development of Bkav Antivirus by implementing core security features such as Self-Defense, Shared Folder Protection, and Virus Processing Functions.
- Supported incident response efforts by delivering detailed malware analysis reports to internal security teams.
- Trained and mentored interns on static/dynamic malware analysis and security research methodologies.

Education

Vietnam Academy of Cryptography Techniques **2023**

Master of Science in Information Security

Vietnam Academy of Cryptography Techniques **2015 - 2020**

Engineer's Degree in Information Security
Minors: Application Security

Projects

MB HuntX – Threat Hunting Automation Solution

- Developed and deployed an advanced Threat Hunting solution with automated scanning and analysis to proactively detect and mitigate security threats.
- Integrated CIS Benchmark compliance checks and automated vulnerability scanning with actionable remediation guidance.
- Enabled multi-platform support (Windows, Linux, AIX, Container) via a portable scanner that supports both automated and isolated modes for flexible deployment in various environments.
- Leveraged Ansible to orchestrate scanner deployment and trigger automated mode across multiple target systems at scale.
- Integrated with the ELK Stack (Elasticsearch, Logstash, Kibana) for centralized log collection, visualization, and correlation of threat hunting results.
- Integrated with CyberArk PIM/PAS to securely manage privileged credentials during remote assessments and scanner execution.
- Implemented secure access controls using WebAuthn-based MFA and role-based access (RBAC) to enforce least privilege.
- Reduced manual workload by 40–50% through automation of scanning and compliance workflows.
- Delivered cost savings of approximately 2 billion VND/year by replacing outsourced security services with internal automated processes.

Automated Security Auditing Tool

- Developed a custom auditing tool to evaluate system configurations against industry benchmarks such as CIS and PCI DSS,...
- Automated compliance checks across servers and applications to identify deviations from security standards and best practices.
- Implemented scheduled configuration assessments to proactively detect misconfigurations and reduce risk exposure.
- Created reusable scripts and audit profiles to streamline assessment workflows and minimize manual intervention.

Honors & Awards

Honors

- Outstanding Employee of the IT Division, MBBank (2021) (Certificate)
- Outstanding Employee of the IT Division, MBBank (2024) - Recognized for contributions in cybersecurity innovation and automation (Certificate).

Awards

Efficiency Improvement Award – Initiative & Improvement Program (Phase II – 2024), MBBank (Certificate) *Jan 2025*

- MB HuntX significantly improved threat detection efficiency and automation in threat hunting workflows.
- Recognized for driving key cybersecurity process optimizations through the development and deployment of MB HuntX.
- Demonstrated innovation in enhancing security monitoring and incident response capabilities with the platform.

AWS Security Gameday *2022*

- Achieved 4th Place in the AWS Security Gameday 2022 competition, demonstrating proficiency in cloud security practices, incident handling, and rapid response to simulated cyber attacks.