Nikola Badev

Cybersecurity Analyst | Security Operations | Physical & Cyber Systems Security
Wayne, New Jersey | (862) 832-7365 | nikola@badev.net

PROFESSIONAL SUMMARY

Security analyst with hands-on experience across cyber and physical security systems, incident response, network defense, and identity management. At AIG, I identified a credential cloning vulnerability in our global access card system, demonstrated the exploit to senior leadership, and drove a multi-site hardware remediation program affecting priority locations worldwide.

I run a home lab with a 24-bay PowerEdge R720, pfSense firewall with Suricata IDS/IPS, segmented VLANs, honeypots, and self-hosted services (it also doubles as a space heater for my 3D printer). I've been building and securing infrastructure since I was a kid—ran game servers through high school with 200+ concurrent paying users, handling backend operations and uptime.

CORE TECHNICAL SKILLS

Security Operations & Detection

- SIEM/SOAR platform management, alert triage, correlation, and workflow automation
- Incident response execution across the full lifecycle: detection, containment, eradication, recovery
- Threat hunting using endpoint, network, and log telemetry
- IDS/IPS deployment, tuning, and rule development (Suricata, Snort)
- Network traffic and PCAP analysis (Wireshark, Zeek)
- Vulnerability scanning and remediation tracking (Nessus)

DFIR & Threat Analysis

- Host-based and network-based forensic investigations (SIFT, FLARE VM)
- Memory acquisition and analysis (Volatility)
- Log analysis, event correlation, and timeline reconstruction (Splunk, Sysinternals)
- Malware behavior analysis in isolated environments
- Detection and investigation of DNS tunneling, proxy evasion, and C2 communications
- MITRE ATT&CK framework mapping for threat analysis and detection engineering
- NIST incident response and risk management frameworks

Windows, Identity & Endpoint Security

- Active Directory administration, security hardening, and attack surface reduction
- Group Policy design and enforcement for security controls
- Identity and access management: SSO, MFA, authentication flows, privilege management
- Endpoint protection deployment and management (Microsoft Defender, BitLocker, DLP)
- Windows Server administration (2016/2019): DNS, DHCP, GPO, permissions
- PowerShell scripting for security automation, auditing, and incident response

Networking & Infrastructure Security

- Network architecture design: LAN/WAN, segmentation, DMZ implementation
- Routing, switching, VLANs, trunking, and ACL configuration
- Firewall deployment and rule management (pfSense)
- VPN configuration and secure remote access (IPSec, WireGuard, OpenVPN)
- Network monitoring, diagnostics, and troubleshooting
- UniFi network management and VLAN segmentation

Cloud & Virtualization

- Experience working in hybrid environments with cloud and on-prem infrastructure
- AWS and Azure security controls, IAM policies, logging and monitoring
- Container security and orchestration (Docker, Kubernetes)
- Hypervisor deployment and management (Proxmox, ESXi, VMware, VirtualBox)

Physical Security & Offensive Testing

- Access control system security (125kHz, iClass, MIFARE, SEOS)
- RFID/NFC vulnerability assessment and credential cloning (Proxmark, Flipper Zero)
- Video management and intrusion detection system administration
- Network reconnaissance, enumeration, and credential capture
- Active follower of red team research, threat actor TTPs, and offensive security communities — tracks emerging techniques and tradecraft for defensive application

Scripting & Development

- Python: security automation, log parsing, custom tooling, data analysis
- SQL: data extraction and manipulation, query optimization, SQL injection testing and exploitation
- Lua: server-side scripting, plugin development, backend configuration for production game servers (200+ concurrent users)
- Java, Visual Basic, HTML: read, analyze, and modify code for vulnerability assessment and incident response
- Production experience: built custom plugins, managed backend systems, payment processing, and anti-cheat for live infrastructure

Systems Administration & Platforms

- Windows: 7/8/10/11, Server 2016/2019 — deployment, hardening, Group Policy, Active Directory, production troubleshooting
- Linux: Kali, Ubuntu, Debian, RHEL/CentOS, TailsOS — primary environment for security operations, server infrastructure, daily use
- macOS, iOS, Android, FreeBSD, GrapheneOS — administration, security configuration, mobile security
- Hypervisors: Proxmox, ESXi, VMware, VirtualBox — deployment and management of virtualized infrastructure
- Hardware hacking and modding: iOS jailbreaking, Android rooting, Xbox JTAG — understanding systems at the firmware and bootloader level since teen years

PROFESSIONAL EXPERIENCE

American International Group, Inc (AIG) – Jersey City, NJ

Physical Security Systems Analyst II | Jan 2024 – Present

- Identified a critical credential cloning vulnerability in AIG's global access card system. Demonstrated that iClass Standard and Elite keys could be copied and replayed to gain unauthorized building access. Presented findings to senior management, directly driving approval for a tiered global security technology refresh.
- Led technical planning for remediation alongside HID and senior leadership. Expanded scope beyond card readers to include intrusion detection, access control, and video management system upgrades at priority sites worldwide.
- Designed and implemented a centralized Incident Management System that transformed alert handling. Identified critical monitoring gaps, which led to establishing a dedicated Active Monitoring team now triaging events from badge anomalies to emergency door releases.
- Partner with security integrators and internal IT teams to commission, upgrade, and troubleshoot physical security systems for new sites and major office upgrades globally.
- Maintain SQL-based tracking systems for credential lifecycle management and onboarding workflows.

Allied Universal Security Services (Client: AIG) – Jersey City, NJ

Security Systems Analyst | Jun 2023 – Jan 2024

- Configured, programmed, and deployed intrusion detection, access control, and video management systems for global AIG sites.
- Served as an escalation point for hardware and software issues, coordinating cross-functional resolution with vendors and internal IT.
- Conducted system health assessments and CCTV forensic reviews supporting incident investigations.

Securitas Security Services USA (Client: Novartis) – East Hanover, NJ

Security Operations Center Analyst | Nov 2022 – Jun 2023

- Monitored alarms, CCTV, and intrusion detection platforms in a 24/7 SOC environment for a pharmaceutical facility.
- Executed incident response procedures, coordinating with law enforcement and emergency services as required.
- Managed centralized alarm monitoring, radio dispatch, incident documentation, and remote panel programming.

Kollins Communications – Ramsey, NJ

Digital Signage Support Technician III | Mar 2022 – Nov 2022

- Troubleshot, maintained, and deployed digital signage and distributed AV infrastructure.
- Performed preventative maintenance and managed customer support via Zendesk.

HOME LAB & PROJECTS

Home Security Infrastructure

- 24-bay Dell PowerEdge R720 in a server rack. Runs Proxmox hosting multiple VMs and Docker containers.
- pfSense firewall with Suricata IDS/IPS for traffic inspection and threat detection. Snort deployed for additional logging and alerting.
- Network segmented via UniFi into dedicated VLANs for security operations, IoT, and server infrastructure.
- Self-hosted services: Mailcow mail server (SPF/DKIM/DMARC), honeypots, and portfolio site (badev.net) deployed via GitHub/Cloudflare.
- Cisco equipment for hands-on routing and switching practice beyond managed UniFi gear.

DFIR & Threat Analysis

- Forensic investigations using SIFT Workstation and FLARE VM.
- PCAP analysis with Zeek: malware behavior, DNS tunneling, and C2 communication detection.
- Memory forensics with Volatility; timeline reconstruction using Splunk and log parsing tools.

Network Security & Offensive Testing

- Network traffic interception and credential exposure analysis using Wireshark.
- Host discovery, port scanning, and service enumeration with nmap and native OS tools.
- Practiced exploitation techniques: ARP spoofing, traffic redirection, session hijacking (controlled environments).

EDUCATION & CERTIFICATIONS

Security+ – In Progress

Google Cybersecurity Certificate – 2024

Synergis Technical Certification (SC-STC-001-5.xx) – 2023 - 2026

Omnicast Technical Certification (SC-OTC-001-5.xx) – 2023 - 2026

Cybersecurity Professional Certificate – New Jersey Institute of Technology, 2023

Purdue University – Purdue Polytechnic Institute, Cybersecurity Studies – 2017–2019