# MICHAEL KEENAN

(813) 997-2832 | mkeenan@michaelkeenan.com
https://www.linkedin.com/in/michaeldkeenan | https://www.youtube.com/@mnaneek


## SENIOR NETWORK SECURITY ENGINEER

Senior Network Security Engineer with 10+ years of experience designing, implementing, and securing enterprise network and cloud infrastructure across healthcare, defense, and critical infrastructure environments. Expertise in network security engineering, firewall architecture, SIEM operations, and Zero Trust frameworks, with hands-on experience across Palo Alto, Fortinet, Cisco, Azure, and AWS platforms. Proven track record of reducing security incidents, improving system uptime, and leading large-scale security deployments in highly regulated environments aligned with NIST, ISO 27001, and HIPAA standards. Recognized for leading cross-functional teams, delivering secure infrastructure solutions, and strengthening organizational security posture.

## CORE SKILLS

- Network Security Engineering
- Firewall Architecture (Palo Alto, Fortinet, Cisco ASA)
- SIEM & Threat Detection (Splunk, QRadar, ArcSight)
- Cloud Security (Azure, AWS)
- Zero Trust Architecture
- Identity & Access Management (IAM, PAM)
- Network Segmentation & Access Control
- Compliance (NIST, ISO 27001, HIPAA)
- Secure Network Architecture Design
- Encryption & Key Management (PKI)
- Secure DevOps / DevSecOps Integration
- Third-Party Risk & Vendor Security Assessments

## PROFESSIONAL EXPERIENCE

**Lancesoft (L3Harris)** | Remote **May 2025 – Present**

**Information Security Systems Engineer (Cleared – Public Trust Clearance)**

Hired in support of Australian Defense Force and airport cybersecurity infrastructure upgrade project. Work on an international team of IT professionals to ensure project deliverables are properly documented and implemented according to Critical Design Documents (CDD) and System Design Documents (SDD). Specific technologies include Cisco Threat Grid, Imprivata Privileged Access Management System (PAM), and Splunk SIEM.

- Conduct security compliance and systems validation for large-scale defense and airport infrastructure projects, ensuring alignment with Critical Design Documents (CDD) and System Design Documents (SDD).
- Implement and manage network security controls using Fortinet FortiGate firewalls across 14 sites, reducing unauthorized access through IPS, application control, and geo-blocking policies.
- Support SIEM and threat analysis operations using Splunk and Cisco Threat Grid to monitor, detect, and investigate potential security incidents.
- Collaborate with cross-functional global teams to deliver cybersecurity infrastructure projects, ensuring adherence to security standards and project milestones.
- Leverage AI-driven compliance tools to automate documentation validation and improve the accuracy of security implementation processes.

**New Age Technology (Kindred Healthcare / LifePoint Health)** | Remote **Oct 2021 – May 2025**

**Network Security Engineer/Network Engineer**

Originally hired as a contractor for Kindred Healthcare to provide Network Security Engineering services in compliance with HIPAA and ISO 27001 Guidelines. Kindred was later acquired by LifePoint Health which made it necessary to incorporate each network for shared information access. Responsibilities include the securing of identity access control and information transport services in the form of VPN and secure IP routing between merged organizations.

- Conducted network security audits and access control reviews across enterprise infrastructure, evaluating ACLs, IPsec VPNs, TACACS authentication, and load balancer configurations to ensure compliance with HIPAA and ISO 27001 standards.
- Engineered and deployed high-availability firewall solutions using Fortinet FortiGate, achieving 99.99% uptime and eliminating single points of failure.
- Designed and implemented enterprise network security policies by developing 11,000+ rule sets across routers, switches, load balancers, and network management platforms to harden infrastructure.
- Led cloud security architecture initiatives in Azure, deploying Palo Alto firewalls and integrating load-balanced security services with on-prem infrastructure.
- Detected and remediated network security threats and anomalies, resolving 300+ incidents using segmentation, ACLs, and intrusion prevention systems (IPS), reducing incident rates by 20%.

- Managed secure remote access solutions by configuring and troubleshooting SSL VPNs, supporting enterprise-wide connectivity and split tunneling requirements.
- Administered large-scale firewall infrastructure including 120+ Palo Alto devices, Cisco ASA firewalls, Panorama, and FireMon, securing Layer 3–7 network traffic across geographically distributed data centers.

**Integrated Resources Inc. (TECO Energy)|** Tampa, FL **Jul 2020 – Oct 2021**

**Network Security Engineer/Network Engineer**

Contracted to align TECO Energy network security architecture to requirements dictated by parent company Emera Cyber Security Framework (CSF). Projects included deployment of Network Access Control (NAC) and Network Segmentation technologies with Cisco Identity Services Engine (ISE) and Checkpoint Firewalls. Responsibilities included maintenance and upgrade of Cisco routers and switches.

- Conducted network security compliance audits of DNS infrastructure and firewall configurations, ensuring alignment with Emera Cyber Security Framework (CSF) standards.
- Engineered and implemented network segmentation and access control solutions using Cisco Identity Services Engine (ISE) and Check Point firewalls to strengthen enterprise security posture.
- Upgraded and secured network infrastructure by patching and modernizing switches within the Eastern Operations Center (EOC), improving system reliability and vulnerability management.
- Audited and optimized firewall security configurations to ensure adherence to enterprise security best practices and regulatory requirements.
- Supported critical infrastructure connectivity by maintaining and troubleshooting network systems, including GarrettCom Magnum routers used in electrical substations.

**Ashley Furniture Industries |** Tampa, FL **Nov 2019 – Jul 2020**

**Cybersecurity Engineer**

Maintained secure information infrastructure by managing privileged access management and secure network access controls. Responsibilities included aligning cybersecurity best practices with NIST 800 and ISO 27001 series guidelines. Provided technical services on a variety of technologies to include Palo Alto firewalls, Active Directory user account management and Darktrace Intrusion Detection System (IDS).

- Implemented identity and access management (IAM) and privileged access controls to secure enterprise systems, aligning with NIST 800 and ISO 27001 cybersecurity frameworks.
- Deployed multi-factor authentication (MFA) for Azure cloud applications and Palo Alto GlobalProtect VPN, strengthening authentication security and reducing unauthorized access risk.
- Configured and optimized firewall security policies including ACLs and URL filtering on Palo Alto firewalls to enforce secure access to web resources.
- Led the design and implementation of a centralized log management solution, integrating Syslog-NG with Microsoft Azure Sentinel SIEM to enhance threat detection and monitoring capabilities.
- Engineered secure infrastructure for operational technology (OT) environments, ensuring safe integration of vendor systems within manufacturing networks.
- Developed and administered privileged user account management programs to control access to critical IT systems and enforce least-privilege principles.
- Investigated and responded to security incidents and malware events, performing remediation and system cleanup to maintain system integrity and availability.

**ReliaQuest |** Tampa, FL **Jul 2016 – Nov 2019**

**Network Security Engineer/Security Engineer**

Initially hired as security engineer charged with driving security information event management (SIEM) using a variety of tools and systems, including LogRhythm and ArcSight. Promoted to network security engineer to oversee the development and management of solutions to provide top-level network security for enterprise clients. Partnered with clients on the engineering of solutions for various devices, including firewalls, web proxy servers and IPS/IDS. Created security policies, best practices and roadmaps to ensure optimal results. Coached, trained and supported new hires.

- Engineered and managed security information and event management (SIEM) solutions using LogRhythm and ArcSight to support threat detection, monitoring, and incident response across enterprise environments.
- Designed and implemented network security architectures for enterprise clients, deploying firewalls, intrusion prevention systems (IPS/IDS), and web proxy solutions to secure critical infrastructure.
- Developed security policies, standards, and technology roadmaps to strengthen client security posture and ensure alignment with industry best practices.

- Researched, evaluated, and deployed emerging security technologies, introducing 3–5 new solutions annually to enhance threat prevention and detection capabilities.
- Authored statements of work (SOW) and service-level agreements (SLAs) for managed security services, supporting Palo Alto firewalls and F5 ASM web application firewall (WAF) solutions.
- Configured and deployed application delivery and load balancing solutions using F5 Local Traffic Manager (LTM) to support secure application access.
- Led large-scale VPN and network security initiatives, coordinating with 150+ enterprise clients (including SeaWorld and Marriott) to implement IPsec encryption and redundancy solutions.
- Architected and implemented Zero Trust security frameworks across on-premises and AWS environments, aligning identity, network, and endpoint controls with NIST 800-207 standards.
- Collaborated with cross-functional stakeholders to deliver enterprise security solutions, influencing over $2M in infrastructure security investments.
- Deployed and optimized next-generation firewall solutions (Palo Alto, Fortinet) to improve network segmentation and secure access to external networks.

**Arkansas Blue Cross and Blue Shield** | Little Rock, AR **May 2014 – Jul 2016**

**Network Engineer**

Provided technical expertise for the support and management of various systems, devices and applications. Held full responsibility for maintaining all network systems and technologies, working directly with end users to identify and resolve all issues. Created VPN connections, configured systems and components, integrated security tools and maintained all system applications, including firewalls, IPS and anti-malware. Trained new hires on Cisco ASA firewalls and network security tools.

- Managed and maintained enterprise network infrastructure and security systems, supporting firewalls, intrusion prevention systems (IPS), anti-malware solutions, and secure application environments.
- Engineered and deployed secure remote access solutions by configuring SSL/TLS VPNs with multi-factor authentication to support enterprise user connectivity.
- Administered public key infrastructure (PKI) certificates (Symantec, GlobalSign) to secure internal and external web applications and reverse proxy services.
- Designed and implemented network security architectures for test environments, supporting development and validation of new security technologies and controls.
- Collaborated with stakeholders and technical leadership to evaluate and integrate new network security tools, improving overall infrastructure security posture.
- Configured and enforced firewall access control policies using identity-based services and Context Directory Agent (CDA) integration.
- Developed network documentation and topology diagrams, mapping data center and regional network infrastructure to support operational visibility and troubleshooting.
- Implemented SSL proxy and traffic inspection solutions using Blue Coat Proxy to analyze encrypted traffic and enhance threat detection capabilities.
- Created standardized firewall request processes and documentation, improving change management and access control governance across secure network environments.

**Arkansas Air National Guard** | Ft. Smith, AR **May 2012 – Oct 2016**

**Cyber Systems Operations (*Honorable Discharge*)**

Supervised team responsible for maintenance and support of information and network systems within a Top Secret Sensitive Compartmented Information Facility (TS/SCI). Ensured the implementation and administration of systems and tools in alignment with strict security standards. Oversaw trouble ticket responses, system rollouts and enhancement projects.

- Supervised network and systems operations within a Top Secret / Sensitive Compartmented Information (TS/SCI) environment, ensuring security, availability, and integrity of critical infrastructure.
- Monitored and maintained system performance and availability, proactively identifying issues and executing remediation plans to ensure continuous operations.
- Managed user account provisioning and access control for 150+ systems, enforcing security policies and maintaining system integrity.
- Installed and configured network, computer, and surveillance systems to support mission-critical intelligence operations.
- Developed and delivered training programs on TCP/IP networking and security principles, improving team technical proficiency and operational readiness.
- Coordinated system upgrades and infrastructure enhancements, supporting secure system rollouts and ongoing operational improvements.

# Michael Keenan

## Side Projects

**Founder & Content Creator — Michael Keenan LLC** | Tampa, FL
**YouTube Channel: https://www.youtube.com/@mnaneek**

- Create and publish technical content on network security, systems engineering, and cybersecurity best practices via YouTube platform.
- Educate and engage a growing audience on real-world security implementations and engineering concepts.

## Education & Certifications

- **Education:**

**University of Tampa, Tampa, FL**
Master of Science, Cyber Security — **Expected – May 2027**
**Park University Parkville, MO**
Bachelor of Science, Information & Computer Science: Networking & Security — **Aug 2012 – May 2015**
**Embry-Riddle Aeronautical University, Daytona Beach, FL**
Bachelor of Science, Aeronautics: Management — **Aug 2008 – May 2012**

- **Certifications:**

**ISC(2)**
Certified Information Systems Security Professional (CISSP) — **Expired – Apr 2023**
**Microsoft**
Azure Fundamentals — **Does not expire**

## Technical Skills

**Firewalls & Network Security**
- Palo Alto Networks, Fortinet FortiGate, Cisco ASA
- Web Application Firewalls (F5 ASM)
- Intrusion Prevention Systems (IPS/IDS), NGIP Cisco Secure Firewall Threat Defense (FTD)

**SIEM & Security Monitoring**
- Splunk, IBM QRadar, ArcSight, LogRhythm
- Cisco Threat Grid, Darktrace
- Microsoft Sentinel

**Networking & Infrastructure**
- Cisco Nexus (7000/5000), Cisco Routers & Switches
- Load Balancing (F5 LTM, NetScaler)
- DNS, CDN, TCP/IP, Network Topology Design

**Cloud & Virtualization**
- Microsoft Azure, Amazon Web Services (AWS)
- VMware vSphere, ESXi

**Security & Access Control**
- Cisco Identity Services Engine (ISE), TACACS+
- Active Directory, Privileged Access Management (PAM)
- Multi-Factor Authentication (MFA), SSL/TLS

**Tools & Systems**
- Wireshark, SolarWinds, GNS3, Cisco VIRL
- Cisco ASDM, Cisco IOS