

Patrick Nguyen

nguyen.c.patrick@gmail.com | [linkedin.com/in/paatricknguyen](https://www.linkedin.com/in/paatricknguyen) | paatrick.com | (925) 285-0288 | New York, NY

Professional Summary

OT Security Engineer with 5+ years of NERC CIP compliance and ICS security experience at a NextEra Energy subsidiary, specializing in Purdue Model network segmentation, Check Point firewall administration, and secure remote access across IT/OT boundaries. Brings a proven track record of audit-ready compliance governance and hands-on security controls implementation to OT security programs across critical infrastructure environments.

Work Experience

Trans Bay Cable (NextEra Energy Subsidiary)

Aug 2021 – Mar 2026

OT Security Engineer – Remote

- Integrated and enforced Purdue Model network segmentation across Levels 2–5, protecting OT/ICS assets and isolating operational environments from corporate networks in alignment with NERC CIP-005 ESP requirements.
- Deployed and administered Check Point firewalls managing 250+ rules and RBAC policies to enforce segmentation aligned with NERC CIP requirements across IT/OT environments.
- Maintained NERC CIP-005 firewall rule governance by documenting business justifications and source references for each permitted rule, supporting audit-ready evidence for compliance reviews.
- Configured firewall rules and Active Directory integration to support Dragos deployment, enabling passive OT-specific threat detection and monitoring across segmented control and DMZ networks.
- Hardened ICS Active Directory environment by enforcing least-privilege policies and restricting administrative access to critical control systems.
- Designed secure remote execution pathway between segmented networks using Just Enough Administration (JEA) for PowerShell.
- Triaged SIEM alerts in Tripwire Log Center by correlating firewall, endpoint, and OT system logs to assess operational impact and validate or dismiss threats within ICS environments.
- Deployed Trend Micro Apex One across Windows-based endpoints in ICS and DMZ networks, enhancing endpoint visibility and malware protection within segmented OT environments.

Trans Bay Cable

May 2018 – Aug 2019

IT Security Intern – SF Bay Area

- Assisted in implementation of NERC CIP-007-6 controls, designing firewall rulesets to restrict unnecessary logical ports and services.
- Supported enterprise-wide implementation of MFA (DUO) across company endpoints integrated with Active Directory.

Technical Skills

Firewalls and Networking	Check Point, Cisco Firepower, Network Segmentation, VPN, ACLs, TCP, IP Networking, Network Security, Information Security
OT / ICS Security	Purdue Model Architecture, NERC CIP, SCADA/ICS Environments, Asset Visibility
Security Operations	SIEM Analysis, Vulnerability Management, Endpoint Protection, Tripwire Log Center
Identity and Infrastructure	Active Directory, Group Policy, RBAC, Windows Server, Check Point, Linux, Cisco ISE, TACACS+, PowerShell
Cloud	AWS S3, CloudFront, Route 53, DynamoDB, Lambda, API Gateway

Education

Business Administration, B.S.: Information Technology

California State University East Bay

2021
Hayward, CA

Certifications

AWS SAA (Solutions Architect Associate) – Oct 2024

[Certification Link](#)

AWS CCP (Certified Cloud Practitioner) – Mar 2023

[Certification Link](#)