Scott Lynch

Cybersecurity Leader | Security Operations | IT Governance

SANS Certified Instructor and Course Author SEC555, SANS GDSA, GCDA, GCIH, GNFA, CCNP Security, Cisco Academy Instructor

Security Clearance: DoD TS/SCI Clearance| Total Years of Experience: 27 Years

lynch@packetengineer.com | LinkedIn | 267-621-9865

Philadelphia, PA

A Navy Veteran with over 27 years of experience in cybersecurity management, network engineering, and IT governance, I bring a proven track record in leading and developing global security teams. My career spans impactful security projects in both government and commercial sectors, including supporting U.S. Department of Defense (DoD) missions, USAF, USSF, and prestigious space and aerospace organizations like NASA, ESA, Telespazio, CNES, and DLR. I have successfully managed a $3M USD budget to ensure the strategic allocation of resources, aligning security initiatives with organizational objectives.

As a SANS Certified Instructor and course author, I am dedicated to cultivating team capabilities through knowledge-sharing and practical training. My experience includes building and managing Security Operations Centers (SOCs) globally, implementing vendor security risk management frameworks, and deploying comprehensive network security solutions. With a focus on regulatory compliance (NIST 800-53/800-171, CMMC), threat detection, and vulnerability management, I offer a balanced approach to risk management, ensuring resilient operations and measurable protections.

With a strong emphasis on collaborative leadership and cross-functional team coordination, I am well-prepared to drive your organization's security strategy, ensuring that security investments enhance both organizational resilience and business outcomes.

Summary of Experience and Qualifications

- Team Management and Mentoring: Leadership in building, managing, and mentoring teams to drive operational excellence
- Compliance & Audit: PCI | NIST 800-53/800-171 | CMMC | Mitigation Strategies
- Cybersecurity Management: Vendor Security Risk Management | Vulnerability Management
- Process & Policy Development: Process Development & Evolution | InfoSec Policy Development | Incident Response Planning
- Threat Detection & Engineering: Threat Hunting | Detection Engineering | SIGMA | NSM | Endpoint Analysis
- Incident Response and Digital Forensics (DFIR): Incident Response Planning | Digital Forensics | Endpoint Analysis for Threat Hunting
- Programming/Scripting and Software: PowerShell | Python | Elasticsearch | Kibana | Logstash | GROK | Docker | Docker Swarm | Nessus
- Log Management and Analysis Tools: Sysmon | Winlogbeat | Filebeat | Hayabusa | Security Onion | OpenSearch | Elasticsearch
- Log and Network Monitoring: Windows Event Logs | Syslog | Security Onion | Zeek/Bro | Linux & Windows Events of Interest

Relevant Professional Experience

SANS Institute - Certified Instructor, Author & Course Lead, SEC555 SIEM and Tactical Analytics

2018-Present

- Course Development and Leadership: Developed and authored the SEC555: SIEM with Tactical Analytics course, focusing on real-world, tactical analytics to empower security professionals in detecting, analyzing, and responding to advanced threats. This course emphasizes hands-on learning to harness the power of SIEM platforms for proactive threat detection and response.
- Instructor of Tactical Analytics for SIEM: Deliver expert instruction on advanced SIEM and threat detection techniques, teaching security professionals to identify and respond to complex attack patterns and use-case driven SIEM deployment. Known for translating technical concepts into actionable skills that enhance detection and incident response capabilities.
- Real-World Scenario-Based Training: Designed labs and course content based on real-world scenarios, covering essential skills in log management, correlation rules, and alerting for faster and more effective incident response. Emphasizes using tactical analytics to maximize SIEM efficacy in detecting and responding to adversary behaviors.
- Threat Hunting and Detection Engineering: Trained professionals in building threat-hunting methodologies and leveraging SIEM platforms to identify and mitigate threats. Emphasized techniques such as behavioral analysis, data correlation, and the development of custom detection logic to enhance threat visibility.
- Analytics-Driven Incident Response: Equipped students with the knowledge to conduct analytics-driven incident response using tools like Elasticsearch, Kibana, Logstash, and GROK, with a focus on parsing, analyzing, and visualizing security data for effective threat detection.
- Technical Leadership in SIEM Implementations: Provided thought leadership on SIEM best practices, covering everything from data onboarding and log source configuration to correlation and threat intelligence integration, preparing students to optimize SIEM deployments for organizational security needs.

Through SEC555, I have trained hundreds of cybersecurity professionals, instilling a deep understanding of SIEM capabilities and empowering them to transform raw data into actionable intelligence. This course has become a core part of the SANS curriculum, highly valued for its hands-on approach to modern threat detection and response.

Swedish Space Corporation – SSC-US – *Multiple Roles*

2000-2023

Security Operations Manager

2012-2023

- Leadership in Security Operations & Incident Response: Led security operations, incident response, and vulnerability management across enterprise networks, ensuring timely threat detection and mitigation.
- Established & Directed Network/Security Operations Center (NSOC): Designed and launched the company's first integrated NSOC, centralizing monitoring and enhancing the organization’s incident response capabilities.
- Developed SECOPS Framework: Pioneered the Security Operations (SECOPS) concept within the global organization, creating a unified approach to threat management and operational security that served as the foundation for future security strategies.

- Global Security Operations Leadership: Acted as the organization's Security Operations lead, overseeing cybersecurity initiatives and aligning them with business objectives before the Chief Information Security Officer (CISO) was appointed.
- Network Security Monitoring (NSM) Implementation: Maintained and optimized a robust NSM platform leveraging Security Onion, Zeek/Bro, network taps (e.g., Gigamon), and SPAN ports, enabling full packet inspection, NetFlow collection and analysis, and DNS monitoring to proactively identify and address threats.
- Corporate SIEM Deployment: Led the development and deployment of a corporate Security Information and Event Management (SIEM) platform, advancing the organization's global security posture through centralized event correlation and real-time threat visibility.

Network Manager

2008-2012

- Network Architecture & Security Leadership: Directed network architecture design and implementation to ensure high availability, security, and resilience across all operational sites, supporting seamless business continuity and scalable growth.
- Cross-Functional Team Management: Led a diverse team of engineers across IT disciplines, including server infrastructure, virtualization, wireless networks, desktop support, and cybersecurity. Fostered collaboration and knowledge-sharing to drive innovation and elevate team performance.
- Budget Management & Strategic Investment: Managed a $3M USD budget, strategically allocating resources to technology updates, greenfield deployments, and enhancements of existing (brownfield) infrastructure. Focused investments on areas that improved performance, ensured cybersecurity compliance, and aligned with industry standards.
- Cybersecurity Compliance Alignment: Integrated cybersecurity best practices and compliance measures into all network upgrades and deployments, proactively meeting regulatory and organizational security standards.
- Operational Efficiency & Performance: Established and enforced best practices for network management, leading to a significant reduction in downtime, enhanced response efficiency, and increased system reliability.
- Stakeholder Collaboration: Partnered with executives and department heads to ensure network capabilities aligned with business requirements, delivering secure, efficient solutions that supported mission-critical applications and services.

Network Engineer

2006-2012

- Network Infrastructure Optimization: Maintained and enhanced network infrastructure to ensure seamless, high-performance connectivity and robust security across all systems, meeting demanding uptime and reliability standards.
- Global Network Deployment: Strategically deployed firewalls, routers, and switches as part of a global network architecture, facilitating secure, reliable customer connectivity to remote ground stations and supporting mission-critical operations.
- Advanced Troubleshooting & Support: Provided comprehensive troubleshooting across network components, quickly identifying and resolving issues to minimize downtime. Collaborated directly with customers to validate and fine-tune operational capabilities, ensuring network configurations met stringent performance requirements.
- Security Enhancement: Implemented network security protocols to safeguard data transmission, proactively addressing vulnerabilities and optimizing defenses in alignment with organizational

security policies.

- System Testing & Validation: Conducted rigorous end-to-end testing and validation with customers, confirming network resilience and operational readiness for diverse scenarios and environmental conditions.

SATCOM Operations Engineer

2004-2006

- Satellite Communications Operations Support: Ensured high uptime and reliability for satellite communication systems, providing critical operational support and rapid issue resolution to maintain service continuity.
- Customer-Centric Project Integration: Collaborated closely with customers and internal engineering teams to integrate and deploy customer-critical projects, including end-to-end planning, resource allocation, and ground station coverage optimization.
- Comprehensive Project Execution: Led efforts in technology integration, including system upgrades and deployment of new capabilities, ensuring alignment with customer requirements and operational standards.
- Operations & Controller Training: Developed and delivered targeted training for satellite operations and controllers, enhancing team readiness and proficiency with new technologies and procedures.
- Communications Plan Development: Designed and implemented comprehensive communications plans, aligning project goals with technical requirements to ensure seamless information flow and efficient project execution.

Other SSC Roles: Ground Systems Engineer (2002-2004), Systems Engineer (2000-2002)

Relevant Instructional Experience

Bucks County Community College

Cisco CCNA Instructor

2006-2013

- Comprehensive Cisco CCNA Instruction: Delivered an in-depth Cisco IT Academy course over a structured 10-month period, focusing on practical networking fundamentals and hands-on skills crucial for real-world applications in network engineering.
- Industry-Ready Preparation: Equipped students with the knowledge and skills necessary to pass the Cisco CCNA certification exam, while also emphasizing the practical implementation of concepts to prepare them for real-world networking environments.
- Applied Learning Approach: Guided students through complex networking topics, including routing, switching, security fundamentals, and troubleshooting, using real-world scenarios and lab-based hands-on exercises to deepen understanding and build confidence.
- Mentorship & Skill Development: Mentored aspiring network professionals, fostering technical problem-solving abilities and critical thinking skills essential for success in the networking industry.

Cybersecurity Adjunct Professor

2012-2020

- Instructor for Security Certified Network Professional (SCNP): Delivered comprehensive instruction in the SCNP certification course, covering critical cybersecurity concepts, best practices, and threat mitigation techniques essential for modern network security professionals.

- Curriculum Development for Network Security Monitoring (NSM): Designed and implemented an advanced NSM course, providing students with hands-on experience using Security Onion and Zeek. This curriculum emphasized practical skills in threat detection, packet analysis, and incident response.
- Real-World Application Focus: Integrated real-world scenarios and lab-based exercises into course content, preparing students to apply network security monitoring techniques in professional cybersecurity roles.
- Skill-Building in Emerging Technologies: Fostered proficiency in cutting-edge tools and methodologies, equipping students to navigate the complexities of modern cyber threats and fortify network defenses.

Military Service

United States Navy, Reserve - P-3 Orion Aircrew, In-Flight Ordnance *(2000 – 2004)*

United States Navy, Active Duty - Electronic Warfare Technician *(1994 – 2000)*

Certifications

- **Cisco Network Academy, CCNA – Cisco Certified Network Associate**
- **Cisco Network Academy, CCAI – Cisco Certified Academy Instructor**
- **Cisco CCNP-S (Security) – Cisco Certified Network Professional (CCNP) Security**
- **GIAC Certifications – GCDA, GCIH, GNFA, GDSA**

Presentations & Talks

Explore my professional presentations and talks covering topics in cybersecurity, network defense, SIEM deployments, threat detection, and satellite communication security:

- **Blue Team Detect and Defend**
  Bucks County Community College, Focus on Security Conference, 2018 Presentation Link
  An in-depth discussion on blue team strategies for proactive defense and incident response.

- **Did You Do Your Homework? Use Case-Driven SIEM Deployments**
  SANS SIEM Team Summit, 2019 Presentation Link
  Explored practical approaches to SIEM implementation, emphasizing use-case development to enhance detection capabilities.

- **How to Prevent Ransomware**
  Bucks County Community College, Ransomware Conference Presentation Link
  Provided actionable insights on ransomware prevention, highlighting effective mitigation strategies for organizations.

- **The Risk to Space: Satellite Communications Systems as Attack Targets**
  SANS ICS Summit, Orlando, FL, 2023 YouTube Link
  Addressed vulnerabilities in satellite communications and ground networks, underscoring emerging threats in space technology.

- **The Many Paths to Cybersecurity**
  Customer Talk for SANS Presentation Link
  A motivational session on diverse career paths in cybersecurity, tailored to inspire newcomers in the field.

- **The Risk to Space: Satellite Communications Systems and Ground Networks as Attack Targets**
  SANS Blue Team Summit, Online, 2023 YouTube Link
  A follow-up talk on satellite network vulnerabilities, focusing on threat detection and defense strategies.

- **Who Goes There? Threat Hunting on Your Home Network**
  Bucks County Community College, Focus on Security Conference, 2021 YouTube Link
  A practical guide to threat hunting at home, showcasing techniques and tools to identify suspicious network activity.

For additional presentations and resources, please visit my GitHub repository:

GitHub https://github.com/slteksystemsllc/Presentations

Education/Training

- Business Administration – Bucks County Community College
- Political Science – Texas Central Community College