Scott Lynch

Cybersecurity Leader | Network Engineering & IT Governance Expert

lynch@packetengineer.com | 267-621-9865

LinkedIn: www.linkedin.com/in/packetengineer/ | **GitHub:** www.github.com/slteksystemsllc | **X:** www.x.com/packetengineer

---

With over 27 years of experience in cyber security 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.

Highly Skilled in the Areas Of:

- Team Management and Mentoring: Leadership in building, managing, and mentoring teams to drive operational excellence
- Compliance & Audit: PCI/PII/CPNI/SOX | NIST 800-53/800-171 | CMMC | BSIMM Findings Remediation | Mitigation Strategies
- Cyber Security Management: Vendor Security Risk Management | Vulnerability Management
- Process & Policy Development: Process Development & Evolution | InfoSec Policy Development | Security in SDLC
- Threat Detection & Engineering: Threat Hunting | Detection Engineering | SIGMA | NSM
- Programming/Scripting and Software: PowerShell | Python | Elasticsearch | Kibana | Logstash | GROK | Docker | Docker Swarm

- Log and Network Monitoring: Event Logs | Security Onion | Zeek/Bro | Linux & Windows

Professional Experience

SANS Institute

Author & Course Lead, SEC555 SIEM and Tactical Analytics *(2022 – 2024)*

- Developed and led SEC555 course content development, influencing SIEM strategies and enhancing tactical analytics practices.

Certified Instructor, SEC555 SIEM and Tactical Analytics *(2018 – Present)*

- Deliver expert training on SIEM and Tactical Analytics, empowering security professionals with actionable skills.

SLTek Systems, LLC (2022 – Present)

Independent Cyber Security Consultant ***(2022 – Present)***

- Provide cybersecurity consulting with a focus on threat detection, compliance, and network security.

Swedish Space Corporation – US (SSC) (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 cyber security 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 – 2008)*

- **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.

Operations Engineer, Satcom ***(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.

Ground Systems Engineer, Satcom ***(2002 – 2004)***

- **Infrastructure Expertise:** Specialized in ground system infrastructure, ensuring secure and reliable satellite communications across critical mission operations.
- **Antenna Maintenance & Support:** Conducted on-site maintenance, upgrades, and enhancements of 13-meter full-motion tracking antennas, supporting consistent, high-quality signal transmission and reception.
- **Technical Oversight:** Managed and maintained baseband radios, down/upconverters, RF switches, and high-power transmitters, ensuring optimal performance and minimal downtime.
- **System Integration & Testing:** Collaborated with cross-functional teams to test, troubleshoot, and integrate new hardware components and firmware updates, enhancing system resilience and communication quality.
- **Operational Efficiency:** Implemented process improvements and maintenance protocols that minimized signal disruption, increased antenna lifespan, and reduced repair time.
- **Field Support & Training:** Provided hands-on training and technical support to junior engineers and technicians, establishing best practices for maintenance and emergency troubleshooting.

Systems Engineer, Satcom *(2000 – 2002)*

- **Satellite System Design & Management:** Designed and managed critical satellite system components with an emphasis on operational security, performance, and integration within a global communication network.
- **Satcom Lab Environment Oversight:** Established and maintained a dedicated satcom lab environment for testing and development of new customer satellite systems, ensuring seamless integration with the global ground network.
- **Testing & Calibration Expertise:** Conducted maintenance, calibration, and operational testing of advanced satcom test equipment, ensuring reliability and precision for customer deployments.
- **RF Interface Development:** Built, integrated, and tested essential RF support equipment, including RF switches, baseband radios, and satcom modems, enhancing system robustness and connectivity for satellite communications.
- **Collaboration for System Optimization:** Worked alongside cross-functional teams to refine and validate satellite communication solutions, supporting continuous improvement and adaptability within the satcom ecosystem.

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.

Cyber Security 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.

United States Navy, Reserve

P-3 Orion Aircrew, In-Flight Ordnance ***(2000 – 2004)***

- **Ordnance Specialist & Aircrew Member:** Served as an essential aircrew member on the P-3 Orion in an active reserve squadron, responsible for handling and managing in-flight ordnance during critical missions.
- **Operational Support for Flight Crew:** Provided direct support to flight crew, pilots, and weapons officers, ensuring smooth coordination and readiness in high-stakes environments.
- **Mission Readiness & Tactical Execution:** Assisted in the execution of mission objectives by supporting ordnance preparation, safety protocols, and real-time adjustments to mission plans as needed.
- **Multi-Role Collaboration:** Actively contributed to the success of in-flight operations by maintaining clear communication and coordination with the flight crew, supporting a cohesive team environment under demanding conditions.

United States Navy, Active Duty

Electronic Warfare Technician ***(1994 – 2000)***

- **EW Technician 2nd Class with TOP SECRET/SCI TK Clearance:** Entrusted with the maintenance, management, and operational oversight of advanced electronic warfare (EW) equipment aboard a Nimitz-class aircraft carrier, ensuring tactical readiness and security compliance.
- **Watch Team Leader:** Supervised a tactical watch team of four EW specialists, directing the collection, identification, and dissemination of EW and Information Warfare (IW) intelligence to cryptologic personnel, intelligence units, and Battle Group Commanders.
- **Information Systems Security Officer (ISSO):** Served as ISSO for a 150-person department, maintaining INFOSEC integrity by enforcing NSA and DOD security

policies, which included system auditing, audit trails, virus protection, and administrative controls across unclassified and classified networks.

- **Technical Proficiency with EW Systems:** Six years of hands-on experience with critical systems such as the Global Command Control System-Maritime (GCCS-M), ELINT Correlator, STRED, Gale Lite, JDISS, ACDS Block 1, and maintenance of the AN/SLQ-32 (v) 4 and AN/WLR-1H (v) 5.
- **Collaboration with Information Warfare Commander (IWC):** Coordinated with the IWC to integrate ELINT and IW data into actionable tactical and strategic insights, providing Battle Group commanders with a comprehensive picture of the operational environment.
- **Mission Briefing & Tactical Analysis:** Briefed senior staff on mission objectives, geo-political intelligence, threat recognition, and counter-tactics, supporting informed decision-making and enhancing mission effectiveness.
- **Training & Mentorship:** Trained junior personnel on EW systems, computer technology, and data analysis techniques, enhancing team capabilities and readiness.
- **Database Development for EW/IW Operations:** Designed databases to streamline access to EW/IW data, enabling operators to retrieve critical information quickly and support time-sensitive mission requirements.

Education & Training

SANS Institute Courses:

- **SEC530:** Defensible Security Architecture and Engineering, **GDSA**
- **SEC564:** Red Team Operations and Threat Emulation
- **SEC455:** SIEM Design & Implementation
- **SEC555:** SIEM with Tactical Analytics, **GCDA**
- **SEC504:** Hacker Tools, Techniques, Exploits, and Incident Handling, **GCIH**
- **FOR572:** Advanced Network Forensics and Analysis, **GNFA**
- **SEC511:** Continuous Monitoring and Security Operations, **GMON**
- **SEC579:** Virtualization and Private Cloud Security
- **SEC580:** Metasploit for Enterprise Penetration Testing
- **SEC560:** Network Penetration and Ethical Hacking, **GPEN**
- **SEC566:** Implementing and Auditing the Twenty Critical Security Controls - In-Depth
- **Offensive Countermeasures:** Defensive Tactics That Actually Work, John Strand

VMware Training:

- **VMware Academy Graduate (VCP5)** – Bucks County Community College

Cisco Certifications:

- **Cisco Network Academy, CCNA** – Cisco Certified Network Associate
- **Cisco Network Academy, CCAI** – Cisco Certified Academy Instructor

- **Cisco CCNP-S (Security)**

Academic Background:

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

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