Ray Caparros
ray.caparros@netsectap.com
(209) 740-2725

Summary

Experienced Security Architect and Engineer with a proven track record in the information technology and services industry, with expertise spanning both defensive and offensive security disciplines. On the defensive side, experienced in next-generation firewalls, vulnerability management, intrusion detection and prevention (IDS/IPS), SIEM and network monitoring platforms, endpoint protection, zero-trust architectures, security operations, incident response, and security automation/orchestration. On the offensive side, skilled in penetration testing, red teaming techniques, adversary emulation, exploit analysis, and security assessment of complex networked and cloud environments. Additionally, experienced in applying AI and machine learning to cybersecurity, including threat and anomaly detection, behavioral analytics, and automation of security workflows, as well as evaluating and securing AI-driven systems against adversarial threats.

Education

- Strayer University
  Masters of Business Administration
  Concentration in Artificial Intelligence Systems Management
- Strayer University Graduated in 2018
  Masters Information Systems
  Major Computer Security Management
- Strayer University Graduated in 2007
  Bachelor of Science in Computer Information Systems

Certifications

- Information Technology Infrastructure Library (ITIL v4)
- EC-Council Certified Security Analyst (ECSA)
- CompTIA Cybersecurity Analyst (CYSA+)
- CompTIA Advanced Security Practitioner CE (CASP+)
- EC-Council, Certified Ethical Hacker (CEH)
- Google AI Essentials

Professional Experience

Mantech International (June 2020 – Current) – Sr. Cyber Security Engineer / R&D Manager

- Cybersecurity Lab Infrastructure Management: Led the design, implementation, maintenance, and evolution of a cutting-edge cybersecurity IT lab infrastructure, incorporating both on-premise and cloud-based resources. This included selecting, deploying, and managing a diverse suite of security tools and technologies, continuously evaluating industry trends to optimize the lab's capabilities.
- Cloud Administration and Security: Managed and secured cloud environments, including infrastructure provisioning, configuration, security hardening, and cost optimization. Implemented cloud-specific security best practices and tools to protect data and applications in the cloud.

- Security Operations Center (SOC) Enhancement: Provided engineering expertise to address complex security challenges, with a focus on enhancing SOC capabilities. Drove advancements in Intrusion Detection, Full Packet Capture, NetFlow analysis, Malware Analysis, and Network Forensics.
- Vulnerability Management: Conducted enterprise-wide vulnerability assessments, coordinated mitigation efforts, and managed patch deployments to minimize security risks.
- Security Assessment and Authorization (A&A): Performed Security Assessment and Authorization activities to ensure compliance with relevant security standards and regulations.
- Security Infrastructure Administration: Administered and maintained critical security infrastructure components, including Intrusion Prevention Systems (IPS), VMware infrastructure, SSL decryption systems, Cross Domain Systems, SIEM solutions (e.g., Splunk), Firewalls, Proxy servers, Load Balancing appliances, Switches, and Routers.
- Windows Domain Administration: Maintained and administered Windows Domain infrastructure, encompassing Active Directory, DNS, SCCM, WSUS, and related services.
- VMware Infrastructure Management: Managed VMware infrastructure, including building, upgrading, and administering ESXi hosts and vCenter servers.
- Splunk Infrastructure Management: Built, maintained, and administered Splunk infrastructure, including installation, configuration of Splunk servers/clusters, upgrades, and administration of dashboards, reports, and alerts.
- Security Hardening and Mitigation: Supported security system hardening and vulnerability mitigation efforts to strengthen the organization's security posture.
- Documentation and Compliance: Developed and maintained system documentation, including System Security Plans, Concepts of Operations, system architectures, and diagrams, ensuring compliance with relevant standards and regulations.
- Mentorship and Training: Provided mentorship and training to junior engineers, fostering their professional development and contributing to team growth.

Adjunct Professor – Strayer University (August 2023 – Current)

- Teach assigned undergraduate computer science courses within the B.S. program. This may include courses in areas such as Network Security, Database Management, Management of Information Systems, Cybercrimes Techniques and Reponses, etc.
- Develop and deliver course materials, including lectures, assignments, and exams.
- Contribute to the department's curriculum development and assessment activities.
- Provide timely and effective feedback to students on their work.
- Assist students with course material and academic advising.

HackerUSA/ThriveDX (June 2020 – June 2023)

- Teach assigned courses and deliver engaging courses in core cybersecurity domains, including Network Security, Digital Forensics and Incident Response, Cloud Security, and Ethical Hacking.
- Provide timely and effective feedback to students on their work.
- Assist students with course material and academic advising.

Federal Home Loan Banks Office of Finance (September 2018 – June 2020) Sr. Cyber Security Engineer

- Implementation, administration, and support and monitoring of the preventative and detective IT security controls within the Office of Finance.

- Administer Firewalls, Proxy servers, Intrusion Detection Systems, Web Application Firewalls (WAFs), SIEM, and Endpoint solution.
- Perform all related software and hardware upgrade to all security devices.
- Build, maintained, and administer Splunk infrastructure on both on-prem and cloud (installing, configuring Splunk servers/clusters, upgrades, administration of dashboard, reports, and alerting, etc.)
- Maintain tools such as Rapid 7 Nexpose and Sonatype IQ used for conducting vulnerability scanning and application security testing
- Review, asses, and mitigate results of penetration tests and vulnerability assessments on information systems and infrastructure.
- Perform continuous diagnostic and mitigation through vulnerability management lifecycle.
- Perform event log reviews and incident response.
- Perform security tests on web-based applications, networks, and systems.
- Assist to enhanced FHLB-OF's next generation vulnerability management program including but not limited to, formalized assessment criteria, integration with asset inventory, enterprise vulnerability scanning, and remediation tracking and regulations.
- Perform dynamic by the use of malware analysis platforms and technologies to identify malware techniques, tactics, and procedures as needed.

Arion Systems Inc. (May 2016 -September 2018) – Sr. Cyber Security Engineer

- Lead architect for the design, implementation, and deployment of Cross Domain systems.
- Lead support engineer for Cross Domain systems across multiple enterprise networks.
- Lead engineer for Secure Socket Layer (SSL) decryption project.
- Developed and architected solutions to solve complex/unique problems that focus on Security Operation Centers (SOC), concentrating on Intrusion Detection, Full Packet Capture, Net flow, automated malware analysis, and network forensic capabilities.
- Lead, deployed, and administering Intrusion Prevention systems, VMware infrastructure, SSL decryption systems, Cross Domain systems, and SIEM solutions such as Alien Vault and Splunk.
- Proficient in designing, deploying and operating highly available, scalable and fault tolerant systems in Amazon Web Services (AWS).
- Proficient in designing, deploying and operating highly available, scalable and fault tolerant systems in Google Cloud.
- Worked on Firewalls, Proxy servers, and Load Balancing deployments and installations.
- Maintained and administered Windows Domain infrastructure.
- Supported security system hardening and vulnerability mitigation efforts.
- Supported efforts for system documentations such as but not limited to, System Security Plans, Concept of Operations, System architectures and diagrams, etc.
- Providing mentorship / training for new engineers.

Lockheed Martin (February 2016 – May 2016) - Cyber Architect for Defense Threat Reduction Agency

- Developed and architected solutions to solve complex/unique problems that focus on Security Operation Centers (SOC), concentrating on intrusion detection, full packet capture, net flow, malware analysis, and forensic capabilities
- Architected, deployed, and administered Intrusion Prevention/Detection Systems such as Cisco Sourcefire, Arcsight, Splunk and SOC related network devices.

- Installed, tested and deployed monitoring solutions with Splunk and ArcSight services.
- Created and maintained Splunk Dashboard, Reports, and Panels.
- Provided training and support for new employees and security analysts.

Guidepoint Security (June 2015 – February 2016) Sr. Security Engineer

- Supported all aspects of customer's Security Information and Event Management (SIEM) initiatives including, but not limited to, stress testing, overcoming deployment challenges, scalability, and providing technical reviews and recommendations
- Developed and architected solutions to solve complex/unique problems that focus on Security Operation Centers (SOC), concentrating on intrusion detection, full packet capture, net flow, malware analysis, and forensic capabilities
- Provided technical services to implement hardening best practices that conforms with Center for Internet Security (CIS) and National Institute for Standards and Technology (NIST).
- Reviewed security infrastructure and configuration to identify points of vulnerability and suggested recommendations for remediation
- Provided pre- and post-sales technical engineering services to all Federal, Department of Defense and Commercial sectors to maximize compatibility, budget, and effectiveness.
- Assisted client on systems security matters and took on complex projects requiring additional specialized technical knowledge
- Provided technical expertise for new and re-compete USG proposals and to develop compelling cyber capabilities to strengthen, or differentiate GuidePoint Security (or partner) bid from our competitors
- Maintained industry visibility to the cyber threat landscape and evolution of nation-state and criminal attack efforts

Knight Point Systems (January 2015 0 June 2015) - Sr. Security Engineer for Export and Import Bank

- Provided technical oversight of security and systems administration to manage the execution of daily enterprise operations, while driving the identification, prioritization and fulfillment of new tasks/projects that provide value to the customer while increasing the performance, availability, supportability, and/or security of customer systems and services.
- Provided specific oversight and direction of IT security to ensure policies and technical configurations are implemented in manner that best protects the customers' services and data across the enterprise network.
- Supported and maintained Palo Alto Firewalls, McAfee Endpoint Protection, and Cisco ASAs

Northrop Grumman (October 2013 0 January 2015) - Sr. Cyber Security Engineer / Manager for Department of Homeland Security

- Oversees projects and tasks assigned to the engineering and information assurance group
- Provides direction to subordinates based on general policies and management guidance
- Maintains a working knowledge of relevant hardware and software applications, including emerging technologies.
- Provides technical consultation in new systems development, and enhancements of existing systems
- Provides technical and operational support to evaluate problems and provide technical solutions that revolves within Cyber Security Operations.

- Participates in meetings, focus groups and configuration boards to ensure client and agency needs are met
- Participates in technical design reviews, system integration testing, load testing, and provide assistance during user acceptance testing
- Works with a team of security engineers and developers to design, test, deploy, and administer Network Mapping application.
- Works with the Computer Network Defense team to develop and provide solutions/recommendations for numerous Federal and Civilian agencies.
- Reviews security infrastructure and configuration to identify points of vulnerability and suggested recommendations for remediation.
- Good working knowledge and experience with firewall devices such as PfSense, Palo Alto Networks, Juniper, and Checkpoint NG.
- Experienced in architecting, deploying, and administering Intrusion Prevention/Detection Systems such as Cisco Sourcefire, Snort, and Palo Alto Networks devices.
- Experienced in using compliance application tools such as RedSeal and SkyBox.
- Good working knowledge and experience architecting and managing Cloud solutions from Amazon Web services and Microsoft Azure.

Guidepoint Security (March 2013 – October 2013) - Sr. Security Engineer

- Supported all aspects of customer's Security Information and Event Management (SIEM) initiatives including, but not limited to, stress testing, overcoming deployment challenges, scalability, and providing technical reviews and recommendations
- Developed and architected solutions to solve complex/unique problems that focus on Security Operation Centers (SOC), concentrating on intrusion detection, full packet capture, netflow, malware analysis, and forensic capabilities
- Reviewed security infrastructure and configuration to identify points of vulnerability and suggested recommendations for remediation
- Provided pre- and post-sales technical engineering services to all Federal, Department of Defense and Commercial sectors to maximize compatibility, budget, and effectiveness.
- Assisted client on systems security matters and took on complex projects requiring additional specialized technical knowledge
- Provided technical expertise for new and re-compete USG proposals and to develop compelling cyber capabilities to strengthen, ghost, or differentiate GuidePoint Security (or partner) bid from our competitors
- Maintained industry visibility to the cyber threat landscape and evolution of nation-state and criminal attack efforts

General Dynamics (February 2010 – March 2013) - Sr. Security Analyst Team Lead/Engineer, Security Operations Center (SOC)

- Hand-selected to be a mentor and lead within GD's mature cyber intelligence SOC, responsible for designing, deploying, managing, monitoring, and troubleshooting of various cyber detection platforms
- Worked with and initiated team of security engineers and developers to design, test, deploy, and administer Snort, Netwitness, and Lancope within enterprise-wide development
- Worked with the GD SOC engineering team to develop content for a complex and growing ArcSight and Splunk Security Information Event Management infrastructure. This includes but

not limited to, use cases for Dashboards, Active Channels, Reports, Rules, Filters, Trends, and Active Lists
- Developed Splunk infrastructure and related solutions for GD SOC environment.
- Life-cycle management of ArcSight and Splunk platforms including coordination and planning of upgrades throughout GD business units for new deployments, and maintaining current operational data flows
- Implemented Splunk forwarder configuration, search heads and indexing.
- Provided technical engineering and architectural services to all General Dynamics Business Units
- Participated on strategic design process to translate security and business requirements into technical designs
- Assists with implementation of counter-measures or mitigating controls

L-3 Stratis (September 2008 – February 2010) - Sr. Security Engineer/Analyst for Nuclear Regulatory Commission

- Supported Nuclear Regulatory Commission's Security Operations Center protecting the network security of the entire agency
- Designed, deployed, managed, and maintained variety of security appliances for the NRC's Security Operation Center
- Spearheaded the replacement of legacy Intrusion Detection throughout the agency
- Led a team to implement McAfee Host Intrusion Protection to mission critical systems
- Performed daily security event analysis from all IDS and Security Event Information Management Tools
- Evaluated new security products and technologies to improve security posture and defense in - depth
- Assisted a team on performing vulnerability assessments throughout the agency
- Tasked to perform security baselines and security assessments of mission critical systems

Northrop Grumman (September 2006 – September 2008) - Manager/Engineer, Security Operations Center (SOC) for Federal Aviation and Administration

- Supported Federal Aviation Administration's Cyber Security Management Center in Leesburg, VA
- Managed core groups (Response, Detection, and Protection) of CSMC that are providing incident response functions and coordinating activities within the operations center and Lines of Businesses
- Coordinated new task and responsibilities for the operation center
- Led a team of Research and Development to make recommendation to various system owner and program managers in today's fast ever changing technology and security threats
- Performed daily security event analysis from all IDS and Security Event Information Management Tools
- Provided recommendations, new strategies, and guidance to increase security in-depth
- Supported on publishing incidents, alerts, advisories and bulletins
- Provided training and mentoring for federal employees and new security analyst
- Managed hiring and coordinated training for new hires

Various Employers (June 2001 – September 2006) - Systems Engineer / Security Engineer

- Performed daily Intrusion Detection Sensor monitoring to ensure all sensors were active and creating logs
- Managed, monitored, and troubleshot variety of firewalls and intrusion detection devices
- Provided incident response functions and coordinating activities with field site personnel when directed
- Conducted research on latest worms, vulnerabilities, viruses, etc.
- Supported on publishing incidents, alerts, advisories and bulletins when required
- Worked with corporate staff on IT projects and supported other divisions with network implementations and configurations
- Configured and implemented a new correspondent management application for various Federal agencies
- Installed, Configured and Implemented records management application for the several Department of Defense agencies