SPLUNK ENTERPRISE ARCHITECT
Career Overview

Highly skilled Cyber Security Engineer offering vast knowledge of network security at desktop, server and internet levels.

Qualifications

- Security Clearance: Top Secret/SCI.
- Administration experience of Microsoft Windows O/S and Microsoft Office suite.
- McAfee HBSS administration; ePO, Virus Scan Enterprise, Policy Auditor, Asset Baseline Monitor, SolidCore, and RSD.
- Security Information and Event Management (SIEM) administration and management; Splunk, HP ArcSight & McAfee Nitro.
- Administration and configuration of ArcSight ESM, Loggers, Connectors, Connector Appliances, and Flex Connectors.
- Splunk Windows Universal Forwarder, Search Heads, Forwarders.
- Experience with variety of IA devices; Niksun NetTrident, Bluecoat Proxies, Wireshark, Snort Network IDS, and Cisco firewall, Cloudshields, Load Balancers, RSA Interceptors, RSA Enterprise Manager.
- Information Assurance Analysis and data correlation
- Data Loss Prevention, (RSA and McAfee).
- INFOSEC, OPSEC and COMSEC expertise.
- Network Operations.
- In-depth working experience with DoD agencies.
- PII, PCI.PHI experience.
- Medical environment experience, HIPAA.
- Intrusion Prevention experience; Network IPS (NIPS) McAfee Intrushield
- Endpoint Solutions: McAfee HIPS, Symantec Endpoint
- Application Whitelisting: McAfee SolidCore
- UNIX/Linux (RHEL) administration.

Accomplishments
Top 10% of class, member of National Honors Society, awarded Presidential Award of National Excellence
Work Experience
Splunk Enterprise Architect 11/2014 ï¼ Current Iron Mountain Odenton , MD

- Project Manager for the development team to design and implement new SIEM (Splunk) infrastructure
- Responsible for troubleshooting, configuring, and installing Splunk.
- Manage Splunk knowledge objects (Apps, Dashboards, Saved Searches, Scheduled Searches, Alerts, Reports)
- The ability to de-code and debug complex Splunk queries.
- Ensuring the Splunk environment continuously meets specification in terms of business requirements (SLA's), application design (standards), and infrastructure performance (KPI's)
- Build strong relationships with internal technology partners, and provide coaching & mentorship to technology teams
- Provide technical expertise and consultancy to the Splunk implementation team(s)
- Governance of change to ensure solution integrity and platform stability
- Partnership with the Service Management teams to develop solution roadmaps for the various functions that the platform supports
- Execute a plan to educate Service Managers and Shared-service leaders on the benefits and use cases for the Splunk platform.
- Engagement with avenues of influence (Splunk product managers, user groups, etc.) to align platform capabilities with business requirements

Security Technology Consultant 11/2013 ï¼ 11/2014 Apogee Sacramento , CA

- Work as an Endpoint (McAfee, Symantec), SIEM (Arcsight, Nitro), or Data Protection (McAfee, RSA) Consultant to fully deploy multiple software and hardware technologies that are supported by the Endpoint/SIEM/ or Data Protection Technology Practice at customer sites along with training and knowledge transfer.
- Collect and document technical requirements from customers and configure Endpoint Technologies and software to work within the capabilities of the applications and hardware for those requirements.
- Review the configuration decisions that are available to customer and provide expertise and guidance on best practices.
- Provide in-depth onsite and remote technical guidance to both new and existing Endpoint Solutions Practice customers to ensure a successful implementation.
- For small and medium engagements, perform project management functions including, but not limited to, project planning and definition, project scheduling, project tracking and status/completion reporting.
- Provide market and product feature input to product management and engineering.
- Work closely with other members of the services team evaluating, testing and rolling out future product releases.
- Responsible for best practices material development and maintenance in concert with Endpoint Solutions software and hardware product releases.

Cyber Security Engineer 11/2011 ï¼ 11/2013 Apex Systems Central Islip , NY

- Develop modules on ArcSight platforms that address the latest security scenarios, threats, and regulatory compliance issues
- Research and develop content for ArcSight Solution Packages, including the formation of content-specific queries, templates, reports, rules, alerts, dashboards, workflow, visualizations, etc.
- Integrate data and event feeds with ArcSight SIEM.
- Build and implement infrastructure security solutions
- Develop a comprehensive SIEM architecture to support real-time security monitoring operations

- Build and implement SIEM reporting to inform and assist clients' incident response teams and security managers
- Troubleshoot and configure networking devices, various platforms, and database (Oracle) Windows and/or UNIX system administration
- Worked with remote access systems (SSLVPN appliances, network admission control/end point control services, token based authentication, integration with Active Directory and Windows)
- Design, configure, and manage/administer network infrastructures
- Review and assist in development of requirements and technical specs
- Development of end use content in forms of technical specifications, systems solution architectures and white papers establishing solutions guidelines
- Direct experience in customer engagements, business case analysis, go-to-market messaging and planning, and new product introduction
- Proactively monitor and report on current Internet threats, as they relate the company's deployed product base
- Utilize compliance and vulnerability assessment tools to analyze products for configuration and patch vulnerabilities
- Implement security event analysis and intrusion detection (Firewalls, VPNs, VLANs, IDS/IPS Incident response - triage, incident analysis, remediation)

RSA Security Consultant 06/2011 ï¼ 11/2011 Bae Systems Port Hueneme , CA

- Assist customer with their implementation of DLP suite
- Assist client with securing their Data at Rest, Data in Motion, and Data in Use
- Conduct overall day-to-day maintenance of the DLP platform
- Install and configure DLP products; Sensors, ICAP device's, Enterprise Manager, Network Controller, Grid workers, Interceptor's and Endpoint agents
- Provide best-practices subject matter expertise regarding DLP system administration, scanning and remediation processes
- Troubleshoot DLP issues and drive supports cases to resolution
- Upgrade/patch current DLP platform to latest versions
- Optimize DLP performance, including DLP Content Blades, regular expressions, rules, and reports
- Informal knowledge transfer to customer staff

Senior Network Security Engineer 12/2010 ï¼ 06/2011 US Air Force 33 Network Warfare Sqdrn City , STATE

- Provides installation, maintenance and troubleshooting support of voice, video, and/or data communications networks.
- Monitors and responds to hardware and software problems utilizing a variety of hardware and software testing tools and techniques.
- Installs and configures network hardware and software.
- Provides network troubleshooting and support.
- Provides technical support and training to end-users.
- Administers network security.
- Provides complex server maintenance.
- Sets up new users and deletes old users from the network.
- Maintains current knowledge of relevant technology as assigned.
- Participates in special projects as required.
- Acts as IT architecture expert to CSC and 33rd NWS client
- Provides Network and System Administrator functions as required
- May design and develop highly complex, integrated solutions to meet business requirements or enhance performance.
- Recommends moderately complex systems investment(s) to management and customers based on results of independent assessment of current and future performance, stability and systems management/life cycle issues.
- Provides escalated, highly complex technical support to customers by investigating and resolving systems-related matters of significance; provides support telephonically and/or electronically.
- Plans, conducts and oversees the technical aspects of projects; coordinates the efforts of technical support staff in the performance of assigned projects.
- Applies advanced methods, theories and research techniques in the investigation and solution of the complex system requirements and problems. Develops training tools and documentation; oversees implementation of same.
- Reviews literature, patents and current practices to support business requirements and/or new industry technology. Prepares reports regarding new technology to communicate to appropriate personnel.
- Provides technical consultation on current and proposed systems to other organizations and clients.
- Provides leadership and work guidance to less experienced personnel.

Network Security Engineer 12/2009 ï¼ 12/2010 US Army Medical Information Technology Center City , STATE

- In depth management of (HIPS) Host Intrusion Prevention Systems (HIPS) via HBSS, McAfee Anti Virus (AV), Rouge Asset detection (AV), and Data Loss Prevention (DLP).
- Deploy HBSS to more than 90,000 nodes within the MEDCOM enterprise worldwide.
- Evaluate, design, advise, implement, and integrate products and controls into various platforms, network devices, and systems.
- Perform daily monitoring and analysis of the HBSS console event traffic.
- Maintain HBSS to MEDCOM established standards.
- Enforce MEDCOM IA policy via HBSS Policy Auditor.
- User level experience in VMware environment.
- Provide recommendations and solutions for improvements to security posture

- React to and provide preventive measure for outbreaks / abnormal behavior.
- Assist remote Medical Treatment Facility (MTF) administrators in resolving HBSS issues.
- Assist remote MTF administrators with deploying new systems and configuring the systems to comply with MEDCOM IA / HBSS policy.
- Modify and add policy within HBSS as directed by MEDCOM policy and procedures.
- Support 24 x 7 operations of MEDCOM
- Utilize Implement and configure software and appliance-based products within the Army MEDCOM Theater Architecture.
- Work within MEDCOM/USAMITC to develop and implement effective network, product, and application solutions.
- Maintain security monitoring and reporting appliances; leading and analyzing security reporting.
- HIPAA certified.

Senior Information Assurance Engineer 03/2007 ï¼ 12/2009 33rd Network Warfare Squadron City , STATE

- Provide network security monitoring; correlation analysis via Intrusion Detection System (IDS); preventative measures via vulnerability assessments, malicious logic monitoring, analysis; reporting and handling, incident response forensics, battle damage assessments, and countermeasures analysis operations.
- In depth log analysis of Niksun Net detectors packet capture and session recreation.
- Utilization of tcpdump tool; Wireshark for network protocol analysis for Unix and Windows
- Used Snort network intrusion detection system for UNIX and Windows
- Analysis of Bluecoat Proxies and Ironmail logs.
- Management and configuration of McAfee HBSS v. 3.0 EPO Server
- Implement Network and Asset Models to build a custom business-oriented view within an
- ArcSight ESM environment.
- Utilize both standard and custom reference resources such as the online ArcSight
- Knowledge Base and Reference Pages available within the ArcSight ESM product to research and document selected events and event management processes.
- Navigate the ArcSight ESM Console and Web Components to effectively Correlate,
- Investigate, Analyze, and Remediate both exposed and obscure vulnerabilities to give situational awareness and real time incident response.
- Customize an ArcSight ESM environment by creating Active Channels, Data Monitors, and
- Dashboards to visually manage security event data sources in an enterprise environment.
- Utilize ArcSight ESM Stock Content, such as standard Filters, Rules, Active Lists and reports, which make ArcSight ready to use upon initial installation.
- Design and implement custom Filters, Rules, Session Lists and Active Lists, along with Integrated Case Management and Workflow, to identify, categorize, and, if needed, escalate events of interest and manage event data streams flowing into ArcSight ESM.
- User level experience with UNIX environment and access through Sun systems thin client.
- Coordinate actions with Air Force Network Operations Center (AFNOC) and the Major Command Network Operations and Security Centers (MAJCOM NOSCs).

Education and Training
San Antonio Community College - Information Technology San Antonio Community College, 37credit hours in Information Technology, Jan-Dec 03
US Air Force Airman Leadership School - Air Force City , State , US US Air Force Airman Leadership School, Lackland Air Force Base, TX, Feb-Mar 06
US Air Force Intelligence School - Air Force City , State , US US Air Force Intelligence School, Goodfellow Air Force Base, TX, Aug-Sep 06 Finished with 97% rating; third in class of 35.
US Marine Corps Electronics Computers School City , State , US US Marine Corps Electronics Computers School, Twenty-nine Palms, CA, Mar-May 01
High School Diploma : Roosevelt HS City , State , US High School Diploma, Roosevelt HS, San Antonio TX, Graduated Jun 00 Top 10% of class, member of National Honors Society, awarded Presidential Award of National Excellence
Military Experience
Major 11/2011 ï¼ 11/2013 Company Name 11/11 -11/13: Air Force ISR Agency, Lackland AFB. TX. Cyber Security Engineer Develop modules on ArcSight platforms that address the latest security scenarios, threats, and regulatory compliance issues Research and develop content for ArcSight Solution Packages, including the formation of content-specific queries, templates, reports, rules, alerts, dashboards, workflow, visualizations, etc. Integrate data and event feeds with ArcSight SIEM. Build and implement infrastructure security solutions Develop a comprehensive SIEM architecture to support real-time security monitoring operations Build and implement SIEM reporting to inform and assist clients' incident response teams and security managers Troubleshoot and configure networking devices, various platforms, and database (Oracle) Windows and/or UNIX system administration Worked with remote access systems (SSLVPN appliances, network admission control/end point control services, token based authentication, integration with Active Directory and Windows) Design, configure, and manage/administer network infrastructures Review and assist in development of requirements and technical specs Development of end use content in forms of technical specifications, systems solution architectures and white papers establishing solutions guidelines Direct experience in customer engagements, business case analysis, go-to-market messaging and planning, and new product introduction Proactively monitor and report on current Internet threats, as they relate the company's deployed product base Utilize compliance and vulnerability assessment tools to analyze products for configuration and patch vulnerabilities Implement security event analysis and intrusion detection (Firewalls, VPNs, VLANs, IDS/IPS Incident response - triage, incident analysis, remediation) 06/11 -11/11: TX Department of Health and Human Services, Austin, TX. RSA Security Consultant Assist customer with their implementation of DLP suite Assist client with securing their Data at Rest, Data in Motion, and Data in Use Conduct overall day-to-day maintenance of the DLP platform Install and configure DLP products; Sensors, ICAP device's, Enterprise Manager, Network Controller, Grid workers, Interceptor's and Endpoint agents Provide best-practices subject matter expertise regarding DLP system

administration, scanning and remediation processes Troubleshoot DLP issues and drive supports cases to resolution Upgrade/patch current DLP platform to latest versions Optimize DLP performance, including DLP Content Blades, regular expressions, rules, and reports Informal knowledge transfer to customer staff 12/10 -06/11: US Air Force 33 Network Warfare Sqdrn. Lackland AFB. TX. Senior Network Security Engineer Provides installation, maintenance and troubleshooting support of voice, video, and/or data communications networks. Monitors and responds to hardware and software problems utilizing a variety of hardware and software testing tools and techniques. Installs and configures network hardware and software. Provides network troubleshooting and support. Provides technical support and training to end-users. Administers network security. Provides complex server maintenance. Sets up new users and deletes old users from the network. Maintains current knowledge of relevant technology as assigned. Participates in special projects as required. Acts as IT architecture expert to CSC and 33rd NWS client Provides Network and System Administrator functions as required May design and develop highly complex, integrated solutions to meet business requirements or enhance performance. Recommends moderately complex systems investment(s) to management and customers based on results of independent assessment of current and future performance, stability and systems management/life cycle issues. Provides escalated, highly complex technical support to customers by investigating and resolving systems-related matters of significance; provides support telephonically and/or electronically. Plans, conducts and oversees the technical aspects of projects; coordinates the efforts of technical support staff in the performance of assigned projects. Applies advanced methods, theories and research techniques in the investigation and solution of the complex system requirements and problems. Develops training tools and documentation; oversees implementation of same. Reviews literature, patents and current practices to support business requirements and/or new industry technology. Prepares reports regarding new technology to communicate to appropriate personnel. Provides technical consultation on current and proposed systems to other organizations and clients. Provides leadership and work guidance to less experienced personnel. 12/09 -12/10: US Army Medical Information Technology Center Ft. Sam Houston, TX. Network Security Engineer In depth management of (HIPS) Host Intrusion Prevention Systems (HIPS) via HBSS, McAfee Anti Virus (AV), Rouge Asset detection (AV), and Data Loss Prevention (DLP). Deploy HBSS to more than 90,000 nodes within the MEDCOM enterprise worldwide. Evaluate, design, advise, implement, and integrate products and controls into various platforms, network devices, and systems. Perform daily monitoring and analysis of the HBSS console event traffic. Maintain HBSS to MEDCOM established standards. Enforce MEDCOM IA policy via HBSS Policy Auditor. User level experience in VMware environment. Provide recommendations and solutions for improvements to security posture React to and provide preventive measure for outbreaks / abnormal behavior. Assist remote Medical Treatment Facility (MTF) administrators in resolving HBSS issues. Assist remote MTF administrators with deploying new systems and configuring the systems to comply with MEDCOM IA / HBSS policy. Modify and add policy within HBSS as directed by MEDCOM policy and procedures. Support 24 x 7 operations of MEDCOM Utilize Implement and configure software and appliance-based products within the Army MEDCOM Theater Architecture. Work within MEDCOM/USAMITC to develop and implement effective network, product, and application solutions. Maintain security monitoring and reporting appliances; leading and analyzing security reporting. HIPAA certified. 03/07 -12/09: 33rd Network Warfare Squadron Lackland AFB, TX. Senior Information Assurance Engineer Provide network security monitoring; correlation analysis via Intrusion Detection System (IDS); preventative measures via vulnerability assessments, malicious logic monitoring, analysis; reporting and handling, incident response forensics, battle damage assessments, and countermeasures analysis operations. In depth log analysis of Niksun Net detectors packet capture and session recreation. Utilization of tcpdump tool; Wireshark for network protocol analysis for Unix and Windows Used Snort network intrusion detection system for UNIX and Windows Analysis of Bluecoat Proxies and Ironmail logs. Management and configuration of McAfee HBSS v. 3.0 EPO Server Implement Network and Asset Models to build a custom business-oriented view within an ArcSight ESM environment. Utilize both standard and custom reference resources such as the online ArcSight Knowledge Base and Reference Pages available within the ArcSight ESM product to research and document selected events and event management processes. Navigate the ArcSight ESM Console and Web Components to effectively Correlate, Investigate, Analyze, and Remediate both exposed and obscure vulnerabilities to give situational awareness and real time incident response. Customize an ArcSight ESM environment by creating Active Channels, Data Monitors, and Dashboards to visually manage security event data sources in an enterprise environment. Utilize ArcSight ESM Stock Content, such as standard Filters, Rules, Active Lists and reports, which make ArcSight ready to use upon initial installation. Design and implement custom Filters, Rules, Session Lists and Active Lists, along with Integrated Case Management and Workflow, to identify, categorize, and, if needed, escalate events of interest and manage event data streams flowing into ArcSight ESM. User level experience with UNIX environment and access through Sun systems thin client. Coordinate actions with Air Force Network Operations Center (AFNOC) and the Major Command Network Operations and Security Centers (MAJCOM NOSCs).

Certifications

DoD HIPAA CSC Certified ArcSight Logger Administrator Certified RSA Data Loss Prevention Consultant Certified McAfee Host Intrusion Prevention System Engineer (HIPS) Certified as McAfee Host Based Security System (HBSS) Administrator Security + Certification Certified as ArcSight Certified Security Analyst (ACSA) Certified as Electronics Systems Security Analyst, US Air Force Certified Data Network Specialist from US Marine Corps Radio and Electronics School Symantec Endpoint Protection Level II Meritorious Performance Promotion, US Marine Corps Reserve

Professional Affiliations

Top 10% of class, member of National Honors Society, awarded Presidential Award of National Excellence

Additional Information

Reviews literature, patents and current practices to support business requirements and/or new industry technology

Skills

Security, Engineer, Intrusion, Operations, Access, Ids, Incident Response, Intrusion Detection, Unix, Workflow, Solutions, Network Security, Architecture, Siem, Canonical Correlation Analysis, Case Management, Correlation Analysis, Data Sources, Esm, Forensics, Information Assurance, Intrusion Detection System, Network Intrusion Detection, Network Operations, Network Operations Center, Proxies, Real Time, Snort, Sun, Tcpdump, Thin Client, Wireshark, Clients, Remediation, System Administration, Systems Administration, Active Directory, Authentication, Business Case, Case Analysis, Cyber Security, Database, Firewalls, Integration, Integrator, Ips, Networking, New Product Introduction, Oracle, Real-time, Regulatory Compliance, Remote Access, Remote Access Systems, Technical Specifications, Use Case, Vulnerability Assessment, White Papers, Maintenance, Testing, Training, Rsa, Dlp, Best Practices, Data Protection, Product Management, Project Management, Project Planning, Project Scheduling, Scheduling, Symantec, Technical Requirements, Data Loss Prevention, Loss Prevention,

Hipaa, Vmware, Business Requirements, Cases, Csc, Documentation, Life Cycle, Network Troubleshooting, Patents, Software Testing, Systems Management, Technical Support, Testing Tools, Voice, Systems Security, Cisco, Comsec, Dod, Firewall, Infosec, Linux, Microsoft Office, Microsoft Windows, Ms Office, Payment Card Industry, Pci, Unix/linux, Application Design, Benefits, Coaching, Debug, Enterprise Architect, Governance, Project Manager, Splunk, Use Cases, Rest, Scanning, Sensors, Class, Comprehensive Large Array Data Stewardship System, Award