## Jason R. Gill

|  |  |
| --- | --- |
| Eagle Scout | Navy Veteran | Email: jasongill@jrgcybersecurity.com |
| Humanitarian | Family Man | Site: https://jrgcybersecurity.com |
|  | Mobile: 832-907-0414 |

|  |
| --- |
| **Solutions Architect • Information Security Architect • Cyber Security SME** |
| Innovative IT Security Architect with over 18 years of experience in analyzing, designing, and implementing security solutions to protect over $30 billion in IT assets for clients in the Oil & Gas, Cloud Services, Financial, and Telecommunications industries, as well as the US Navy. A subject matter expert known for advising senior leadership on PCI DSS/NIST/CIS compliance, cloud/container and on-premises cybersecurity approaches, resolving complex issues, and architecting highly effective risk mitigation solutions to guard against known and zero-day threats. Qualifications include certifications in Cybersecurity, Network Security, and Networking, along with experience in all eight CISSP domains, threat hunting, CI/CD pipeline security, and secure software development lifecycle management for cloud, containerized, and traditional IT systems. Recognized as a strategic leader for spearheading enterprise-level initiatives, building high-performance teams, driving continuous improvement, reducing security costs, and delivering results for industry-leading organizations such as VMware, H&R Block, Visa Inc., Chevron, Orange Business Services, Accenture, EOG Resources, and the US Navy. |
| **Top 10 Accomplishments** |
| * Utilized the NIST Cybersecurity Framework for multiple organizations to discover, mitigate, and reduce risk. Developed unique control implementation and testing strategies that balanced risk reduction with associated costs, optimizing budgets concerning the effectiveness and prioritization of CSF related controls. * Fully automated the vulnerability assessment process for Tanzu Kubernetes Grid at VMware by integrating the vulnerability management solution with Jenkins and Jira. This automation scanned each Tanzu Kubernetes Grid build then created and assigned tickets for vulnerabilities discovered in each component. * Secured multiple enterprise-level applications through the implementation and testing of numerous controls within Microsoft Purview. * Conducted in-depth threat modeling for numerous applications and network designs using the STRIDE and DREAD methodologies. Developed threat mitigation and remediation strategies to reduce attack vectors and ensure Visa’s solutions operated safely and securely. * Implemented Managed Detection and Response services, saving EOG approximately $320,000 in personnel costs while enhancing the organization's response capabilities and ensuring response personnel remained trained in the latest threats and incident response techniques. * Designed and deployed Palo Alto firewalls at EOG’s network perimeter to secure north/south traffic. Collaborated with multiple teams to determine firewall rule requirements, then configured and tested all firewall rules. * Delivered IT security solutions for Chevron’s $300M worldwide enterprise. Leveraged subject matter expertise to develop solutions and provide recommendations for both OT and business networks. * Saved Visa $100,000 annually by optimizing threat modeling and risk assessment processes. Evaluated and improved efficiency, defined strategies to enhance the execution and accuracy of these processes. * Successfully guided multiple organizations through achieving various compliance standards including STIG, NIST, CIS, PCI, GDPR, and FedRAMP. * Protected Hess Oil from a malicious insider attempting to steal $40M in scientific research data through the implementation and testing of controls within the DLP solution. |

|  |  |  |
| --- | --- | --- |
| **Core Competencies** | | |
| * Eagle Scout & US Navy Veteran | * OWASP Top 10 | * Symantec CASB & DLP |
| * AI Prompt Engineering | * Vulnerability Assessments | * Security Roadmap Development |
| * Security Solution Design & Development | * NIST CSF Framework | * STRIDE & DREAD Threat Modeling |
| * Cloud Security Architecture Design | * Security Solution Optimization | * Threat Intelligence & Hunting |
| * Kubernetes Security (AKS/TKG) | * Asset Management | * Defense Automation |
| * Strategy Development & Implementation * Emotional Intelligence & Critical Thinking * Technical Writing * Security Controls Assessment | * Cloud Security Controls Assessment * Security Initiative Prioritization * Vendor Analysis & Management * End-user Security Awareness Training | * Team Development & Coaching * CIS, PCI, GDPR, CCPA Compliance * Proxies & Traffic Decryption * Problem Solving & Creativity |

|  |
| --- |
| **Professional Experience** |

**Broadcom, Remote: 05/2022 – Present**

***Senior Staff Security Architect/Engineer (Full Time)***

Led all aspects of the organization’s container security and vulnerability management program for 16 releases of the Tanzu Kubernetes Grid solution, each comprising over 100 components and hundreds of packages per release. Collected detailed information from over 30 teams and 100+ component code repositories to analyze and assess over 2,000 critical and high vulnerabilities, determining exploitability, impact, likelihood, and remediation/mitigation strategies.

* Saved the organization $200,000 annually by overseeing the development, implementation, and use of a custom in-house vulnerability management solution, created from a combination of open-source and proprietary tools.
* Saved VMware $800,000 annually in personnel costs by fully automating the vulnerability assessment process for Tanzu Kubernetes Grid. Integrated the vulnerability management solution with Jenkins and Jira to automatically scan each Tanzu Kubernetes Grid build then create and assign tickets for discovered vulnerabilities.
* Configured the vulnerability management solution to read the in-house vulnerability database and update Jira tickets based on triage and status information from the database.
* Conducted 16 compliance assessments of the Tanzu Kubernetes Grid solution, designed remediation strategies, and provided ongoing guidance and instruction throughout the remediation process.
* Developed, implemented, and documented the process for assessing, reporting, triaging, and remediating vulnerabilities, used by over 30 teams.
* Created impact statements and mitigation strategies for each vulnerability, shared these with customers to address reported issues, and worked closely with customer success teams to ensure timely resolution of security concerns.
* Wrote extensive technical documentation around the design of the TKGm security assessment process and triage process.

**H&R Block, Remote: 11/2020 – 05/2022**

***Senior Security Architect/Engineer (Full Time)***

Coordinated with cross-functional teams to gather architectural, procedural, policy, and technical information to design and implement robust cybersecurity solutions, strengthening enterprise infrastructure and significantly enhancing defenses against known and zero-day threats. Developed and presented comprehensive documentation to educate all organizational levels on the value of investing in cybersecurity technologies, including the designs, processes, and procedures for implementing and operationalizing these solutions. Calculated the current and projected ROI for each deployed technology.

* Secured multiple enterprise level applications through the implementation and testing of numerous controls within Microsoft Purview. Developed an Azure cloud security architecture that focused on delivering high availability Microsoft services while addressing security concerns by identifying risks and attack vectors then implementing controls to remediate them.
* Managed assets such as clusters, nodes, pods, and containers deployed within the Azure Kubernetes environment.
* Led the AKS container security initiative to implement Lacework, coordinating with application development, container management, image management, vulnerability management, security architecture, and SOC teams to integrate Lacework’s capabilities into each team's processes.
* Led H&R Block through the continuous process of maintaining PCI DSS compliance for the traditional enterprise environment and led the initiative that achieved PCI compliance for the Azure Kubernetes Environment including deploying and auditing a significant amount of security controls in and around the AKS environment.
* Achieved STIG compliance for the Azure Kubernetes Environment through the processes of working with multiple teams to assess the environment, developing Plans of Actions and Milestones (POA&Ms) for each finding, implementing remediations, and guiding teams through the exception process as needed.
* Evaluated current data loss prevention architecture to identify gaps, inefficiencies, and design flaws that created strain on both the workforce and the infrastructure and drafted multiple plans of action and milestones to address these issues.
* Collaborated with cross-enterprise teams to develop role and responsibilities documentation including RACI matrixes to address the variances in container management responsibilities.
* Drafted one-year and three-year roadmaps for the data loss prevention program, incorporating growth requirements, organizational impact, and ensuring that timeframes, alert volume, and DLP policies caused minimal disruption.
* Wrote policies and standards as well as technical procedures and playbooks for security implementation, assessment, and remediation for the Azure Kubernetes environment.

**Visa, Remote: 3/2020 – 9/2020**

***Cyber Security Architect (Contract)***

Conducted security assessments and security architecture design reviews in a high-tempo environment for over 50 cloud-based applications and their associated infrastructure. Led multiple teams, including SSDLC, Penetration Testing, Mobile Security, PCI Assessment, IAM, Third Party Risk, and Cyber Engineering, to ensure all aspects of new and existing applications were evaluated for risk, and developed remediation initiatives to address each identified risk.

* Developed comprehensive security architecture diagrams illustrating communication flows between multiple enterprise-level environments and applications.
* Performed in-depth threat modeling for numerous applications and network designs using STRIDE and DREAD methodologies, and developed threat mitigation strategies to reduce attack vectors, ensuring Visa’s solutions operated securely.
* Developed and hardened cloud infrastructure for multiple VISA applications and platforms, including the Cloudview platform.
* Created extensive documentation to streamline the security assessment and architecture review process, improving speed, accuracy, and information reliability.
* Leveraged team building exercises and activities to increase collaboration and communication among the many teams that must be engaged to effectively address the ever-changing risks associated with Visa’s cyber landscape.
* Consistently applied critical thinking to develop innovative threat mitigation solutions, reducing costs for Visa.
* Collaborated with the SSDLC team to ensure adherence to coding practices and proper code testing for vulnerabilities.
* Applied various standards, laws, and best practices to ensure internally developed code was compliant and secure.

**AT&T, Austin, TX: 9/2019 – 11/2019**

***Senior Security Architect/Engineer (Short-term Contract)***

Evaluated NIST and HIPAA compliance for DADS applications under the HHSC umbrella. Identified the controls required for the 39 DADS applications to meet NIST medium system category compliance and HIPAA overlays.

* Created templates for use during the control evaluation phase of the project that were applicable across multiple control families.
* Evaluated applications for NIST and HIPAA compliance, identified gaps, and formulated remediation POA&Ms.
* Authored System Security Plans for 39 DADS applications.
* Analyzed Palo Alto firewall rules to identify risks from poorly designed or overly permissive configurations and provided remediation guidance.

**State of Texas Comptroller of Public Accounts, Austin, TX: 5/2019 – 9/2019**

***Data Loss Prevention Architect (Contract)***

Designed and implemented the Data Loss Prevention (DLP) program for the Office of the Comptroller’s enterprise network, collaborating with multiple divisions to secure data at rest, in motion, and in use through Exact Data Matching (EDM), custom regex matching, proximity rules, data tagging, and egress thresholds. Cultivated cross-divisional collaboration and teamwork.

* Reduced EDM processing time from 2 months to 1 week by restructuring data sets for more efficient processing and improved accuracy.
* Reduced DLP system maintenance time by consolidating DLP policies while maintaining the required granularity for the Information Security Operations division.
* Decreased complexity of the DLP system by reducing the number of rules required in each policy through the process of optimizing the data set design of the EDM data.
* Implemented cloud integration for the DLP system to protect SharePoint data and enhance email resiliency during a disaster recovery scenario.

**Family Sick Care, Katy, TX: 10/2018 – 4/2019**

***Caring Husband (Lifelong)***

Took time off to take care of my wife when she was first diagnosed with a chronic illness.

**EOG Resources, Houston, TX: 4/2018 – 9/2018**

***Cyber Security Architect/Engineer (Contract)***

Enhanced the cybersecurity posture of EOG Resources using the NIST Cybersecurity Framework by evaluating security needs at both architectural and granular levels, identifying gaps, and leading multiple security projects that significantly increased resilience to external and internal threats.

* Managed the full lifecycle of over 800 incidents, including preparation, detection & analysis, containment, eradication, recovery, and post-event activities.
* Led the vendor selection and evaluation process for multiple projects, including application security, Managed Detection and Response, and Data Loss Prevention.
* Designed and deployed Palo Alto firewalls at the network perimeter to secure EOG's north/south traffic. Collaborated with cross-functional teams to define firewall rule requirements, then configured and tested all firewall rules.
* Performed asset management for the company through SCCM and Network Access Controls (NAC) systems to ensure systems allowed on the network met specific security requirements.
* Leveraged the OWASP Top 10 to harden web applications by reducing attack vectors, implementing controls, and baselining normal traffic.
* Implemented Managed Detection and Response services, saving EOG approximately $320,000 in personnel costs while enhancing response capabilities and ensuring personnel remained trained in the latest threats and incident response techniques.
* Conducted extensive proof of concepts for multiple security technologies, defining success criteria, setting up test environments, configuring security applications, and gathering evidence to evaluate success.
* Utilized Data Loss Prevention technology to gather and report critical information for legal investigations.
* Conducted application security assessments using multiple tools and managed a project to integrate vulnerability management into the SSDLC, securing applications early in development and throughout their lifecycle.
* Led threat hunting exercises to detect ongoing attacks and map attack vectors, while defining and documenting a comprehensive diagram of EOG Resources’ threat landscape.
* Optimized security technologies currently in place by increasing their performance as well as reducing the number of false positives reported for EOG Resources’ NGAV solution and multiple APT defense systems.

**MRC Global, Houston, TX: 12/2017 – 3/2018**

***Information Security Operations Manager (Short-term Contract)***

Managed Security Operations for MRC Global’s advanced security platform and extensive network of vendors through strategic planning, implementation, and oversight of security systems, applications, and processes. Oversaw multiple teams and projects while providing subject matter expertise in security services, incident management, and vendor relations.

* Led the CASB vendor selection project by researching vendors, determining capital and labor investment, defining key deliverables, evaluating software capabilities, and providing a value-add summary for executive management.
* Analyzed the Azure cloud environment and its security controls then developed a strategic roadmap for implementing additional security measures in a manner that would not impact business functions.
* Optimized threat reporting by coordinating with vendors to deliver more comprehensive and actionable metrics.
* Enhanced the vulnerability management program by improving reporting and increasing coordination across teams to remediate vulnerabilities.
* Led the Meltdown and Spectre remediation project by managing teams, coordinating efforts, developing a project plan and timeline, assigning responsibilities, defining deliverables, and collaborating with vendors.
* Oversaw the Incident Management Program by objectively evaluating incidents, coordinating responses, and delivering key metrics.
* Led multiple security projects under the supervision of the CISO to achieve an increased security posture and reduce overall risk at MRC Global.

**Orange Business Services, Remote: 3/2017 - 9/2017**

***Technical Security Manager (Contract)***

Managed IT security for Orange Business Services’ $100M platform by analyzing and optimizing security systems, applications, and processes. Led strategy sessions with customers, providing subject matter expertise on security services, incident management, and service quality.

* Reduced potential security incidents by 75% by developing a comprehensive plan for a vulnerability management program, defining the implementation schedule, capital and labor investment, key deliverables, software capabilities, and providing a value-add summary for executive management.
* Resolved security incidents 80% faster by managing 40 Tier 1, 2, and 3 support personnel, troubleshooting issues, performing root cause analysis, and developing strategies to prevent future recurrences, saving Orange $150K in SLA breach costs and driving high customer satisfaction.
* Managed and maintained a secure network internet gateway, including multiple applications, Palo Alto firewalls, intrusion prevention and detection systems, forward and reverse proxies, SIEM systems, secure remote access, routers, riverbeds, switches, and web application servers.
* Reduced the attack surface and enhanced security by designing and testing new rule sets for Palo Alto firewalls.
* Delivered and maintained 99% uptime for all security devices by ensuring engineering teams adhered to processes, policies, and procedures through effective management and the development of workflow matrices.

**Chevron, Houston, TX: 4/2016 - 7/2016**

***Security & Account Management Systems Analyst (Contract)***

Delivered IT security solutions for Chevron’s $300M global enterprise. Leveraged subject matter expertise to develop solutions and provide recommendations for both process control and business networks.

* Improved Chevron’s enterprise anti-virus coverage by 70% by securing 65,000+ endpoints.
* Saved Chevron $200K in security equipment replacement costs by developing proactive maintenance procedures, extending the equipment’s operational lifespan beyond expected lifecycles.
* Managed the intrusion prevention system with multiple consoles and over 100 sensors across a global enterprise environment.
* Monitored health alerts for the intrusion prevention system and remediated issues.
* Directed and maintained an APT and malware defense system for Chevron’s global network.

**Accenture (Hess Oil), Houston, TX: 1/2016 - 4/2016**

***Incident Response Analyst (Contract)***

Managed Intrusion Prevention/Detection Systems to secure Hess Oil’s $250M global enterprise network and implemented IT security architecture best practices and other improvements.

* Led security incident analysis, gathered evidence, identified contributing factors, and responded with proficiency and expertise.
* Protected Hess Oil from a malicious insider attempting to steal $40M in scientific research data through the implementation of controls within the DLP solution.
* Managed the Data Loss Prevention (DLP) system to control, monitor, and secure Hess’ global data movement.
* Improved incident response time by 65% by creating Incident Response Plans for numerous scenarios which included procedures for performing forensic analysis.
* Responded to threats by correlating and analyzing data from multiple systems to identify malicious traffic then determine the source, severity, and appropriate remediation strategy.
* Mitigated data theft risk by 90% by creating data egress thresholds and data usage reports.
* Increased project success by 70% by implementing project management software to enable tracking across numerous IT projects.

**DYONYX, Houston, TX: 11/2014 - 9/2015**

***IT Security Analyst (Contract)***

Managed comprehensive security assessments and testing for DYONYX and its clients, leveraging multiple compliance standards, including NIST, STIG, and FedRAMP.

* Led remediation efforts for gaps, vulnerabilities, and misconfigurations identified during security assessments and testing.
* Designing custom vulnerability management strategies for DYONYX customer environments based on the unique needs of each customer and their environment. Utilized Nessus and WebInspect vulnerability scanning software to perform security assessments and device discovery.
* Produced comprehensive IT security architecture documentation to support continuous monitoring, compliance, vulnerability management, configuration management, disaster recovery planning/testing, incident response, and computer/web use restrictions.
* Developed proof-of-concepts for proposed security solutions, both for internal and external deployment, analyzing and testing specifications for performance issues, security gaps, and unmet expectations.
* Conducted numerous security assessments for multiple customers using NIST CSF methodologies to help organizations understand and mitigate overall risk.

**FROSCH International Travel, Houston, TX: 12/2013 - 9/2014**

***IT Security & Network Administrator (Contract)***

Led comprehensive infrastructure security and network operations management initiatives to resolve cybersecurity incidents, investigate root causes, and implement remediation strategies to prevent future compromises.

* Implemented next-generation firewalls to complement existing network segmentation firewalls, enabling Frosch to monitor user behavior analytics and block an additional 60,000 risky behaviors annually.
* Oversaw network infrastructure and security for 70+ virtual servers and 20 physical servers, including 2008/2012 domain controllers and 2010 Exchange servers across multiple nationwide sites.
* Established a cybersecurity framework program that assessed and addressed risks at the program, policy, procedural, and technical levels.
* Directed the successful achievement of PCI DSS compliance for the enterprise environment by implementing robust security measures, including deploying Nessus for vulnerability management and Symantec Whole Disk Encryption for data protection. Oversaw the setup and validation of all required security controls and collaborated with an Approved Scanning Vendor (ASV) to obtain formal attestation.
* Reduced risk identified by the CSF by 50% through the implementation of Identify Finder DLP for data loss prevention and Retina vulnerability management software to identify and analyze system and network vulnerabilities.
* Saved FROSCH $1.5M by conducting a cybersecurity gap analysis and implementing remediations including Data Loss Prevention and data-at-rest encryption to achieve PCI compliance.
* Managed the implementation of IPS/IDS, Palo Alto firewalls, and enterprise-level antivirus software, and performed broad-scale virus removal and antivirus administration for 1,100+ computers.

**US Navy, Various Locations: 9/2005 – 11/2013**

***IT Security and Network Manager***

Managed IT Security Operations, Network Security, and Cyber Threat Intelligence to protect $100M in assets for the U.S. Navy from internal and external threats. Leveraged multiple threat intelligence sources—including open source, commercial, and military feeds—to provide data inputs to specialized threat intelligence platforms.

* Key Contributions:
  + Reduced risk by 85% by implementing optimized security architectures to ensure high security standards, enhanced performance, and consistent availability of network resources, while maintaining strict compliance with robust standards.
  + Saved $750K by developing and championing policies, plans, procedures, and processes for all aspects of network and database security across the organization. Many policies are still in use by the Navy today.
  + Increased threat detection capabilities by 90% by integrating threat intelligence platforms with network infrastructures, enabling a comprehensive understanding of current and emerging attack vectors that could compromise the network.
  + Managed, trained, and developed a team of 25 elite IT security professionals across multiple cyber and network security disciplines.
* Risk Mitigation:
  + Utilized the NIST CSF to manage all aspects of risk, including assessment, analysis, mitigation, and lifecycle management across multiple divisions, formulating risk-based matrices to ensure cybersecurity was maintained with minimal impact to organizational performance.
  + Oversaw threat intelligence data analysis to identify, categorize, and prioritize risks at both the technical and architectural levels.
  + Adapted cybersecurity strategies to the evolving threat landscape, ensuring maximum resilience to both known and zero-day attacks.
* Issue Resolution:
  + Managed vulnerability assessment and remediation using BeyondTrust’s Retina product for over 8 years. Conducted and analyzed vulnerability assessments, formulating and implementing remediation strategies to resolve vulnerabilities.
  + Led forensic analysis of malware, advanced persistent threats, and other cyberattacks to evaluate their impact on organizational operations, networks, and financial assets, while identifying root causes and attack vectors.

|  |  |
| --- | --- |
| **Education** | |
| **US Navy Vocational Schools:** Cyber Security, Network Security, Windows Networking, and Linux Networking **John Foster Dulles Highschool:** Graduated with Honors as a Texas Scholar  **Daily Reading & Research:** Cyware News Feeds, Twitter News Feeds, Krebs on Security, Akamai, Paul’s Security Weekly, Security Bloggers Network, Errata Security, Wombat Security, Dark Reading, The Hacker News, Threatpost, Schneier on Security | |
| **Additional Credentials** | |
| **Technical skills** | **IT Vendor Experience:** BeyondTrust, Identity Finder, Nessus, WebInspect, Palo Alto, Cisco, Checkpoint, Juniper, Symantec Antivirus, Digital Guardian, Bluecoat, Barracuda, Arcsight, FireEye, Metasploit, Wireshark, Splunk, WinF Disk, Cain & Abel, Zed Attack Proxy, Social Engineering Toolkit, Azure Kubernetes Service, Tanzu Kubernetes Grid, MS Purview  **Security Technologies:** Network Access Control, Web App Firewalls, Network Firewalls, Forward Proxy, Reverse Proxy, Packet Filters, Spam Filters, DDOS Defense and Damage Mitigation, SIEM, Penetration Testing, Packet Analysis, Container Security,Data Loss Prevention, Vulnerability Management, Forensic Analysis, Code Analysis, Malware Defense, CASB, Threat Modeling |
|  | **Systems**: Windows Server, Linux, NOOBS, Raspbian, Tails, Tor, Python  **General**: Microsoft Office Suite (Word, Excel, PowerPoint, Outlook, OneNote), Google Suite (Drive, Documents, Sheets, Forms), CISSP Training |
| **Compliance Standards Achieved** | Payment Card Industry (PCI/DSS), National Institute of Standards and Technology (NIST) SP 800-53 & 800-171, Security Technical Implementation Guide (STIG), CIS Controls & Benchmarks, OWASP Top 10, ISO 27000 & 27001, HITRUST, SOX, GDPR, CCPA |
|  |  |
| **Honors & Awards** | Navy Achievement Medal, Good Conduct Awards x2, Sailor of the Year Nominations x2 |
| **Professional Development** | Certification - Security+  Certification - Network+  Currently Studying for AZ-900 and CISSP |
| **Organizations**  **Address** | U.S. Navy Veteran, Eagle Scout, Order of the Arrow  3810 Preston Cove Ct, Katy, TX 77494 |