**JASON GILL – Eagle Scout – US Navy Veteran**

Jason.r.gill8@gmail.com

832-907-0414
Austin, Texas

|  |
| --- |
| **Information Security Architect – Senior Cyber Security Engineer – Security SME** |
| Innovative IT Security Architect with 13+ years of experience leading teams to protecting $14B+ in IT assets for clients in the Oil & Gas, Cloud Services, and Telecommunications industries in addition to the US Navy. Subject matter expert known for advising senior leadership on risk mitigation strategies, resolving issues, and architecting complex solutions to protect organizations from both internal and external threats. Exceptional qualifications include certifications in Cyber Security, Network Security, and Networking as well as experience in all 10 CISSP Domains, Threat Intelligence, and SCADA Security. Strategic leader highly regarded for spearheading program initiatives, building high-performance teams, driving continuous improvement, and delivering results for industry-leading organizations such as Chevron, Accenture, and EOG Resources. Prioritization  |

|  |
| --- |
| **Selected Highlights**  |
| * Implemented Managed Detection and Response services allowing EOG to save approximately $320,000 in personnel costs while increasing the organizations response capabilities and ensuring that response personnel remain trained in the latest threats and incident response techniques.
* Directed multiple teams involved in IT security for Orange Business Services’ $100M platform of offerings through comprehensive project and personnel management as well as performed optimization of security systems and applications.
* Resolved issues 80% faster by managing 40 tier 1, 2, and 3 support personnel, troubleshooting problems, performing root cause analysis, repairing issues, and outlining a strategy to prevent future recurrences thereby saving Orange $150K in SLA breach costs and creating a high customer satisfaction rating.
* Delivered IT security solutions for Chevron’s $300M worldwide enterprise. Leveraged subject matter expertise to develop solutions and made recommendations for both the process control and business networks.
* Saved Chevron $200K in security equipment replacement costs by creating proactive maintenance procedures that allowed the equipment to remain in good working order past expected lifecycle.
* Managed Intrusion Prevention/Detection Systems to secure Hess Oil’s $250M global enterprise network. Implemented IT security architecture best practices and other improvements.
* Protected Hess Oil’s $40M scientific research data from a malicious insider attempting to steal sensitive scientific data.
 |

|  |
| --- |
| **Core Competencies**  |
| * Eagle Scout & US Navy Veteran
 | * OWASP Top 10
 | * Data Loss Prevention
 |
| * Intrusion Prevention & Detection
 | * Vulnerability Assessments
 | * Root Cause Analysis
 |
| * Forensic Analysis
 | * NIST Framework
 | * Threat Modeling
 |
| * APT & Malware Defense
 | * Incident Response Protocols
 | * Infrastructure Design
 |
| * Infrastructure Planning
 | * Project Management
 | * Software Architecture & Analysis
 |
| * PCI DSS Compliance
* Emotional Intelligence
 | * Cloud Security
* Critical Thinking
 | * Team Development & Coaching
* Strategic Planning
 |

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

**ATT/HHSC, Austin, TX: 10/2019 – Present**

***Senior Cyber Security Engineer (Contract)***

Evaluating NIST and HIPPA compliance for the DADS applications now under the umbrella of HHSC. Determining the controls required for the 39 DADS applications to meet the compliance level of the NIST medium system category and the related HIPPA overlays.

* Created multiple templates for use during the control evaluation phase of the project that were applicable across multiple control families.
* Evaluated multiple applications for NIST and HIPPA compliance, determined gaps, and formulate remediation POA&Ms.
* Designed solutions to meet compliance requirements as needed by the DADS applications.
* Writing multiple System Security Plans for the 39 DADS applications.

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

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

Designing the Data Loss Prevention (DLP) program for the Office of the Comptroller’s extensive enterprise network by working with multiple divisions to secure data at rest, in motion, and in use through the use of Exact Data Matching (EDM) and pattern matching. Breaking down traditional divisional barriers to promote teamwork and cooperation between divisions and departments.

* Reduced EDM processing time from 2 months to 1 week by restructuring the data sets in a way that allowed for easier processing and greater accuracy.
* Decreased maintenance time of the DLP system by consolidating the policies while maintaining the required granularity needed by 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 simplifying the data set design of the EDM data.
* Designing cloud integration for the DLP system to protect SharePoint data and create greater email resiliency during a disaster recovery scenario

**Family Sick Care, Katy, TX: 9/2018 – 2/2019**

***Caring Husband (Lifelong)***

Took time off to take care of my wife who was recently diagnosed with a chronic illness. We have recently setup additional care for her and now I am seeking employment.

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

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

Advanced the Cyber Security posture for EOG Resources through the process of evaluating the security needs of EOG resources from an architectural standpoint as well as on a granular level, determining gaps in the security posture, then creating and completing multiple security projects resulting in a greatly increased resiliency to both external and internal threats.

* Managed the vendor selection and filtering process for multiple projects including Application Security, Managed Detection and Response, and Data Loss Prevention.
* Utilized the OWASP Top 10 to harden web applications against attacks and threats of various types.
* Implemented Managed Detection and Response services allowing EOG to save approximately $320,000 in personnel costs while increasing the organizations response capabilities and ensuring that response personnel remain trained in the latest threats and incident response techniques.
* Performed extensive proof of concepts for multiple security technologies including determining the success criteria for each security technology, setting up testing environments/selecting test equipment, configuring security applications, and performing exercises/gathering evidence to determine what success criteria is met.
* Used EOG Resources Data Loss Prevention technology to gather and report valuable information needed by legal for multiple investigations.
* Performed application security assessments using multiple tools and managed a project to integrate vulnerability management with the SDLC to secure applications early during development and throughout the development lifecycle.
* 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 saving EOG $50,000 in professional services.

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

***Information Security Operations Manager (Contract)***

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

* Led the CASB vendor selection project researching multiple vendors, determining capital and labor investment, key deliverables, software capabilities, and value add summary for executive management.
* Optimized threat reporting by coordinating with the vendor to report new, more extensive and actionable metrics.
* Enhanced the vulnerability management program through improved reporting and increased coordination across multiple teams to remediate vulnerabilities.
* Managed multiple teams involved in the Meltdown and Spectre remediation project by coordinating efforts, creating a project plan and timeline, assigning responsibilities, determining deliverables, and working with vendors.
* Oversaw the Incident Management Program through objective evaluation of possible incidents, coordinating proper response, and delivering key metrics.
* Led multiple other security projects under the supervision of the CISO to achieve an increased security posture and reduce overall risk to MRC Global.

**Orange Business Services, Houston, TX: 3/2017 - 9/2017**

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

Directed IT security for Orange Business Services’ $100M platform of offerings through comprehensive analysis and optimization of security systems, applications, and processes. Led focused strategy sessions with the customer and provided subject matter expertise regarding security services, incident management, and service quality.

* Reduced incidents 75% by developing a comprehensive plan to implement a vulnerability management program, defining implementation schedule, capital and labor investment, key deliverables, software capabilities, and value add summary for executive management.
* Resolved issues 80% faster by managing 40 tier 1, 2, and 3 support personnel, troubleshooting problems, performing root cause analysis, repairing issues, and outlining a strategy to prevent future recurrences thereby saving Orange $150K in SLA breach costs and creating a high customer satisfaction rating.
* Managed, maintained, and administered secure network internet gateway of multiple applications, firewalls, intrusion prevention and detection systems, forward proxies, reverse proxies, SIEM systems, secure remote access systems, routers, riverbeds, switches, and web application servers.
* Increased security 55% by performing root cause analysis for P1 incidents and creating detailed root cause analysis reports for management and introducing fixes to avoid future issues.
* Delivered and maintained 99% uptime for all security devices by ensuring the engineering teams followed all processes, policies, and procedures through careful management and the creation of workflow matrices.

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

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

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

* Improved Chevron’s enterprise anti-virus suite 70% (securing 65,000+ endpoints) by providing and implementing key insights for senior management as a security subject matter expert (SME).
* Saved Chevron $200K in security equipment replacement costs by creating proactive maintenance procedures that allowed the equipment to remain in good working order past their expected lifecycles.
* Managed intrusion prevention system with multiple consoles and 100+ sensors across a global enterprise environment.
* Oversaw health alerts for the intrusion prevention system and remediated issues.
* Directed and maintained a highly sophisticated APT and malware defense system for Chevron’s global network.

**Accenture, Houston, TX: 1/2016 - 4/2016**

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

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

* Directed suspected security incident analysis, determined incident factors at multiple levels, and responded to incidents with extreme proficiency and capability.
* Protected Hess Oil’s $40M scientific research data from a malicious insider attempting to steal sensitive scientific data.
* Managed the Data Loss Prevention system used to control, monitor, and secure data movement globally.
* Improved incident response time 65% by creating Incident Response Plans including forensic tools and analysis procedures.
* Prevented threats by correlating and analyzing data to identify malicious traffic, determine the source, severity, and appropriate remediation strategy.
* Mitigated data theft risk 90% by creating data movement reports to inform on the data egress in the environment.
* Increased project success 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 cyber and network security assessments and testing for DYONYX and its customers by using multiple compliance standards including NIST and STIG.

* Managed remediations for gaps, vulnerabilities, and misconfigurations discovered while performing cyber and network security assessments and testing.
* Saved clients $250K by designing custom vulnerability lifecycles for DYONYX customer environments using Nessus and WebInspect vulnerability scanning software to perform assessments and host/network device discovery.
* Delivered extensive IT security architecture documentation to support continuous monitoring, compliance, vulnerability management, configuration management, disaster recovery planning and testing, incident response, and computer and web use restriction.
* Developed proof-of-concepts for proposed security solutions for both internal and external (resale) deployment, analyzing and testing specifications for performance and security gaps, failures, and unmet expectations.

**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 cyber security incidents, investigate root causes, and provide remediation strategies to prevent future compromises.

* 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.
* Reduced risk 60% by implementing Identify Finder DLP to support data loss prevention and Retina vulnerability management software to identify and analyze system/network vulnerabilities.
* Saved FROSCH $1.5M by developing cyber security GAP analysis and Data Loss Prevention processes and protocols to obtain PCI compliance.
* Managed the implementation of IPS/IDS, firewalls, enterprise level anti-virus software, and performed broad scale virus removal and anti-virus administration for 1,100+ computers running windows XP, 7, 8, 8.1, and 1,100 end users.

**US Navy, Various Locations: 2005 - 2013**

***IT Security and Network Manager***

Managed IT Security Operations, Network Security, and Cyber Threat Ops to protect $25M in global assets for the U.S. Navy against both internal and external threats. Leveraged multiple threat intelligence sources including open source, commercial, and military feeds to give data inputs to specialized threat intelligence platforms.

* Key Contributions:
	+ Reduced risk 85% by implementing optimized security architectures to ensure an extensive security standard, high performance rating, and consistent availability of network resources throughout the organization while maintaining strict compliance with robust standard.
	+ Saved $750K by writing and championing policies, plans, procedures, and processes for all aspects of network and database security throughout the organization. Many policies are still being used by Navy today.
	+ Increased threat detection capabilities 90% by integrating threat intelligence platforms with network infrastructures to gain and evaluate a full, in-depth understanding of current and developing attack vectors that could compromise the network.
	+ Managed, trained, and developed a team of 25 elite IT security professionals in a multitude of cyber and network security disciplines.
* Risk Mitigation:
	+ Managed all aspects of risk including assessment, analysis, mitigation, and life cycle management for multiple divisions across all departments, formulating risk-based matrices to ensure cyber security was maintained throughout the organization with little to no impact on the organization’s performance.
	+ Oversaw threat intelligence data analysis to determine, categorize, and prioritize risks to the organization on both a technical and architectural level.
	+ Adapted cyber security strategies to an ever-changing threat landscape to ensure maximum resiliency to both known and zero-day attacks.
* Issue Resolution:
	+ Managed vulnerability assessment/remediation using Retina. Performed and analyzed vulnerability assessments and formulated/implemented multiple mitigations and remediations to discover and resolve vulnerabilities.
	+ Directed forensic analysis of malware, advanced persistent threats, and other attacks to determine business function, network, and financial impact as well as root cause and attack vector.

|  |
| --- |
| **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 |

|  |
| --- |
| **Additional Credentials** |
| **Technical Skills** | **IT Security:** BeyondTrust’s Retina, CSIRT, Forensic Analysis, Identity Finder DLP, Nessus, WebInspect, Palo Alto, Cisco, Checkpoint, Juniper, Symantec Anti-Virus and DLP, Digital Guardian DLP, Bluecoat, Barracuda, Arcsight SIEM, FireEye, Metasploit, Wireshark, Splunk, WinF Disk, Cain & Abel, Zed Attack Proxy, and Social Engineering Toolkit, Penetration Testing, CIS Benchmarking, CASB, DDI Vulnerability Scanner**Systems**: Windows Server (2000, 2003, 2008, 2012)**General**: Microsoft Office Suite (Word, Excel, PowerPoint, Outlook, OneNote), Google Applications (Drive, Documents), PCI Compliance, NIST, STIG, CISSP Training |
| **Honors & Awards** | Navy Achievement Medal, Good Conduct Awards x2, Sailor of the Year Nominations x2  |
| **Professional Development** | Certification - Security+, Certification - Network+  |
| **Organizations** | U.S. Navy Veteran, Eagle Scout |