**Gregg MARTIN**

Vice President, Enterprise Architecture



**AREAS OF EXPERTISE/SKILLS**

* Cyber Security Consulting
* Network Architecture & Design
* Security Architecture & Design
* Audit & Assessments
* Information risk and security management
* Data Center Design
* Security Operations Centers
* Network Operations Centers
* Cloud & Mobile
* Interim CISO as a Service responsibilities

**CERTIFICATIONS**

* Certified Information Systems Security Professional (CISSP®) #312915
* Cisco – CCNA, CCNP, CCIE (Written)
* CCSA
* MCSE
* Technical Training Certification (PwC)

**PROFESSIONAL BACKGROUND**

Gregg Martin currently leads Enterprise Architecture for FishTech. Gregg has over 20 years of experience in Information Technology, and over 18 years of experience in Enterprise Networking and Security. Prior to joining FishTech, Gregg was with Optiv Security for 5 years and PricewaterhouseCoopers (“PwC”) for 10 years and worked as a Network Security Engineer and Network Security Architect, responsible for the architecture of all network and security technologies for the entire global firm. Gregg has delivered the built out of numerous data centers and Security Operations Centers. Gregg is well versed in the design, implementation, and operations of network and security technologies for Security Operations Centers. In addition, Gregg has conducted audits and reviews of data of several well-known industry data centers and Security Operations Centers. Additionally, Gregg has tremendous amount of experience providing consulting services for global clients and has worked in over 12 countries.

**Eric ULLMANN**

Director of Enterprise Architecture



**AREAS OF EXPERTISE/SKILLS**

* Network Architecture & Design
* Security Architecture & Design
* Systems Architecture
* Virtualization
* Security Architecture and Design
* Security Assessments
* Infrastructure Assessments
* Network/Security Operations Center Design
* Cloud Strategy
* Cloud Architecture Design
* Cloud Access Security Broker Design

**CERTIFICATIONS**

* Cisco – CCNA, CCNA-Security
* MCTS
* MCP
* Security+
* VCP-6 NV

**PROFESSIONAL BACKGROUND**

Eric Ullmann has been in the information technology field for over 15 years with multiple roles in network, systems, and security engineering across multiple verticals. Ullmann’s broad technical backgrounds spans multiple verticals to include cloud computing, security policy development, root cause analysis, IDS/IPS solutions, Next Generation Firewall technologies, DDOS, data loss prevention, change management coordination, project management, and virtualization. Prior to going into consulting, Ullmann served as IT Security Manager for a regional financial institution. He previously led the security team, where he was responsible for developing the security framework and developing policy. Additionally, he was responsible for all aspects of the organizations security infrastructure and the adoption of new security tools that will increase the operational efficiency and decrease the likelihood of a security breech. Ullmann was responsible for security and operations for the financial institution’s private cloud environment.

**Joe KRAXNER**

Technical Director for Security Intelligence



**AREAS OF EXPERTISE/SKILLS**

* Security Information Event Management (SIEM)
* Data Loss Prevention (DLP)
* Enterprise Security
* Network Security Architecture and Design
* Network Security and Architecture Assessments
* Security Architecture and Design
* Vulnerability Management
* Routing and Switching, Firewalls, Wireless Security
* Intrusion Prevention, Content Security and Web Application Security
* Systems Architecture including various network and server services

**CERTIFICATIONS**

* Certified Information Systems Security Professional (CISSP®)
* Splunk Certified Architect
* Splunk Certified Consultant I
* Splunk Certified Consultant II
* HP ArcSight Master Accredited Solutions Expert (MASE)
* HP ArcSight Certified Security Analyst (ACSA)
* LogRhythm Certified Professional Services Consultant (LCPSC)
* LogRhythm Certified Deployment Engineer (LCDE)
* Aruba Certified Mobility Professional (ACMP) - inactive
* Juniper Networks Certified Associate (JNCIA) – inactive

**PROFESSIONAL BACKGROUND**

With two decades’ experience in information technology, Joe Kraxner is a security professional focused on network and enterprise security. Joe has maintained security operations for organizations in nearly every vertical, including health care, federal government, biotech, and energy. Joe has experience with switching and routing, wireless, firewalls, security information and event management (SIEM), data loss prevention (DLP), security assessments, IP packet analysis, systems hardening, URL/web filtering, intrusion detection/prevention systems (IDS/IPS), and vulnerability management. This experience allows him to solve complex security issues and offer solutions beyond a product-focused approach.

Prior to joining Fishtech Labs, Joe was a principal security consultant in Optiv's Center of Excellence for Situational Awareness where he built and led a team of SIEM consultants while delivering on projects and providing escalation assistance. Joe was also part of the FishNet Security Network Security (NetSec) team delivering on several offerings while helping to build delivery practices around emerging technologies. Joe excelled at filling in the gaps for projects where Sales had opportunities but FishNet Security lacked the "perfect" offering or consultant to execute. Joe has established himself as a thought-leader in SIEM technologies. He strives to help clients build SIEM as an overall strategy, rather than a compliance checkmark.

**Kylen GRIFFIN**

Principal Consultant, Enterprise Architecture



**AREAS OF EXPERTISE/SKILLS**

* Federal Information Security Management/Modernization Act (“FISMA”)
* Federal Risk and Authorization Management Program (“FedRAMP”)
* National Institute of Standards and Technology Special Publications 800 Series (“NIST SP800 series”)
* National Institute of Standards and Technology Cybersecurity Framework (“NIST Cybersecurity Framework”)
* Center for Medicare & Medicaid Services (“CMS”) Information Security Acceptable Risk Safeguards
* Internal Revenue Service (“IRS”) Publication 1075
* International Organization for Standardization (“ISO”) 27001/2:2013
* Health Insurance Portability and Accountability Act (“HIPAA”) Security and Privacy Rule
* Information Security Risk Management
* Risk Assessment Program Development
* Security and Privacy Policy Development
* Security Awareness and Training
* Security Program Development

**CERTIFICATIONS**

* Certified Information Systems Security Professional (“CISSP”)
* ITIL v3 Foundations
* Chemical-terrorism Vulnerability Information (“CVI”)

**PROFESSIONAL BACKGROUND**

Kylen Griffin currently is a Principal Consultant within Enterprise Architecture for Fishtech. Kylen Griffin has more than 16 years of information technology and information security experience working in government defense contractors, with a demonstrated ability to align business strategic goals with a myriad of regulatory compliance and internal policy requirements. Prior to joining Fishtech, Kylen was a Senior Security Consultant with Optiv/Fishnet Security for almost 4 years. Kylen is skilled at accurately assessing security risks and communicating analysis results, both verbally and in writing, to technical and business personnel. During the past ten years, Kylen focused his career on the risk management, regulatory and contractual compliance, and policy areas of information security. While experienced in some of the more technical information security areas, Kylen’s passion lies in analyzing and assessing NIST and FISMA security reviews and explaining compliance roadmaps to business personnel in a way that enables them to make informed decisions how to appropriately apply time, money, and resources to remain or obtain compliance. Kylen enjoys interfacing with all levels of stakeholders and transferring knowledge to stakeholders to enhance and prioritize their efforts.

**David CHAPMAN**

Director of Enterprise Architecture

**AREAS OF EXPERTISE/SKILLS**

* Cloud Architecture
* Virtualization
* Software Defined Data Center (SDDC)
* Software Defined Networking (SDN)
* Micro-Segmentation
* Client Access Security Brokers (CASB)
* Disaster Recovery Strategies
* Active Directory
* OS Security
* Messaging Systems
* Orchestration & Automation
* Storage
* Citrix NetScaler & XenApp
* Public Key Infrastructure (PKI)

**CERTIFICATIONS**

* VMware Certified Professional (VCP6-NV)
* VMware Certified Professional (VCP3 & 4) -inactive
* Microsoft Certified Systems Engineer (MCSE) NT, 2000, 2003
* Citrix Certified Administrator (CCA)
* Six Sigma Green Belt Certified (SSGBC)

**PROFESSIONAL BACKGROUND**

With 18 years of experience in information technology, David Chapman is a IT professional focused on IT infrastructure, cloud, and enterprise security. David helps organizations develop strategic and tactical goals to solve both infrastructure and operational efficiencies in all sizes and verticals. As a subject matter expert in infrastructure architecture as well as private cloud computing and storage strategies. David’s broad technical background spans multiple verticals to include virtualization, cloud computing, client access security brokers, application delivery controllers, root cause analysis, Active Directory, messaging systems, software defined data centers, software defined networking, micro-segmentation, disaster recovery and DDI.

David has helped organizations off all sizes across multiple verticals develop complex private cloud strategies that included designing Infrastructure as a Service (“IAAS”) solutions where the enterprise could gain operational efficiencies and shorten delivery time of virtual machines from hours to minutes. This included OS deployment, application deployment, server hardening, and standardization. Furthermore,

David developed and implemented disaster recovery strategies to ensure business continuance.

Prior to joining Fishtech Labs, David served as an Infrastructure Enterprise Architect for a national education institution. He previously led the enterprise services team, where he was responsible for developing all aspects of the infrastructure, to include storage, virtualization, cloud, and automation. Additionally, he was responsible for all aspects of the organizations infrastructure and the adoption of new technologies that increased the operational efficiency. David was responsible for infrastructure and operations for the education institution’s private cloud environment.

**Joe MENDYGRAL**

Principal Security Consultant



**AREAS OF EXPERTISE/SKILLS**

|  |
| --- |
| * Business Impact Analysis * Security Program Development * Vulnerability and Threat Management * Security Policy Development * ISO 27001/27002 * Physical Security Specialist * Information Security Risk Management * FISMA / NIST |

**CERTIFICATIONS**

|  |
| --- |
| * CISSP * CISM * GIAC – (GLEG) Legal Issues in IT & Security * CHPSE - HIPAA Privacy Security Expert |

**PROFESSIONAL BACKGROUND**

Joe Mendygral has over 16 years of experience in the information security field and over 20 years as an information technology manager. As a security professional, he has developed and driven policies and procedures with the intent of maturing the security posture of the organizations. He has performed a wide variety of functions as a security consultant and in operations either as a technical resource or as a manager.

Joe’s specialty is working with organizations to develop and improve their security framework. He has successfully helped organizations become compliant with several standards such as ISO 27001/2, HIPAA, NERC / CIP, FISMA, NIST 800-53, DIACAP and DIARMF/RMF. Additionally, he has assisted organizations by developing Incident Response and Vulnerability Management plans.

Prior to joining Fishtech, Joe developed a major consulting organization’s Third Party Risk Management program delivery capability as well as working as a Principal Security Consultant for an Enterprise Risk and Compliance program. As an Information Security Officer for the Department of Defense (DoD), supporting the Air Force’s space program, he successfully helped the program’s information security personnel transition from DIACAP to RMF. Prior to that, Joe was the Director of Security for the IRS’s Electronic Federal Tax Payment System where he enhanced the information security program by developing the business continuity plan for a critical infrastructure program and by developing vulnerability management processes.\

**Jim HOUCK**

Senior Consultant

|  |  |
| --- | --- |
|  |  |

**AREAS OF EXPERTISE/SKILLS**

* Enterprise Security
* Network Security Architecture and Design
* Network Security and Architecture Assessments
* Security Architecture and Design
* Vulnerability Management
* Routing and Switching
* Firewalls
* Wireless Security
* Intrusion Prevention, Content Security and Web Application Security Systems Architecture

**PROFESSIONAL BACKGROUND**

With over a decade of experience in information technology, Jim Houck is a security professional focused on network and enterprise security. Jim has implemented, operated, and maintained network and security solutions across multiple industries. Jim has maintained security operations for organizations in nearly every vertical, including health care, federal government, biotech, and energy. Jim has experience with switching and routing, wireless, firewalls, security assessments, IP packet analysis, systems hardening, URL/web filtering, intrusion detection/prevention systems (IDS/IPS), and vulnerability management. This experience allows him to solve complex security issues and offer solutions beyond a product-focused approach.

Prior to joining Fishtech Labs, Jim was a network security consultant with Optiv's Center of Excellence for Enterprise Architecture and Implementation, delivering post sales implementation of enterprise architecture network and security solutions, as well as providing project oversight and escalation assistance. Jim was also part of the FishNet Security Network Security (NetSec) team delivering on a number of offerings while helping to build delivery practices around emerging technologies.

**Arif FAIZ**

Director of Enterprise Architecture

**AREAS OF EXPERTISE/SKILLS**

* Architecture Design and Assessment
* Firewall and VPN
* Software Defined Networking (SDN)
* Micro-Segmentation
* Routing and Switching
* Disaster Recovery Strategies
* Content Security
* Email and Messaging Security
* Authentication and Authorization
* Load Balancers
* SSL VPNs
* Intrusion Prevention

**CERTIFICATIONS**

* CCSE
* CCSE +
* SFCP
* JNCIA-SSL
* F5-LTM
* WCSE
* RSA-CE
* CCNA

**PROFESSIONAL BACKGROUND**

Arif has over 20 years of experience in information technology of which last 17 years focused on information security. His background includes design, implementation, and management of multi-vendor security products within diverse clients ranging from medium to large and global Fortune 500 companies. Arif is a technical team leader who is focused on security architecture planning and gap analysis, risk assessment, engineering, client deliverables, cost containment, and vendor relationship management. Arif has expertise in multi-vendor security solutions such as Check Point Technologies, Pulse Secure, Juniper Networks, Sourcefire, Blue Coat, F5 Networks, Cisco Systems, RSA Security, Forcepoint and Nessus and Qualys (Network Scanners).

Arif is a senior security architect at Fishtech and also performs Network Architecture Assessments, Network Risk Assessments, designing, planning, integrating and managing best of breed Security Solutions – including review of client networks as part of consulting work and making strategic security recommendations in implementing secure, reliable and efficient Perimeter and Wide Area Networks.

Arif has served as the resident security architect for various large firms within Financial, Healthcare, Energy, Retail and Consumer industries.