

Mr. Reguerin has over 25 years of executive leadership with profound and extensive hands-on experience in security, including specialties in Systems Engineering, Enterprise Cross Domain Solutions (ECDS), Cloud/Kubernetes-native Security, Zero Trust Architecture (ZTA), SD-WAN Security, Telco Cloud, Quantum, Artificial Intelligence such as ChatGPT, AWS Kiro/Bedrock as well as implementing Cyber Security controls as part of the Systems Delivery Life Cycle in heterogeneous environments (*NIX and Windows) and Multi-Cloud/Hybrid Environments. His professional Subject Matter Expertise (SME) also includes a diverse **executive management and leadership background**.

QUALIFICATIONS SUMMARY

- Cyber Security Mentor and Instructor
- Infrastructure automation using Microservices and Serverless technologies in support of Artificial Intelligence tooling and Machine Learning (ML)-based software/infrastructure services on multi-cloud/hybrid environments.
- Hybrid and Multi-Cloud Security Architecture/Engineering and Security Control Implementation automation following NIST 800-53 and blending ConMon practices delivered through Agile and DevSecOps methodologies.
- Small Business and Start-up growth **and product development using Agile methodologies**.

EDUCATION

- MS (Information Security. Concentration in Enterprise Architecture), Johns Hopkins University, MD. 2008
- BS (Information Security. Concentration in Software Architecture), Johns Hopkins University, MD. 2005
- AAS (Web Technologies), Montgomery College, MD. 2003

CERTIFICATIONS

- ITIL v3 Foundation Certified, SCSECA, Security +, CISSP, CCSP, ICAgile Professional, SOA Professional, GIAC Cloud Penetration Tester (GCPN), AWS Solutions Architect – Associate, OPSWAT CIP

SECURITY CLEARANCES

- TS/SCI w/CI Poly – Last Poly July 2025 (Active)

CURRENT SOFTWARE/TOOLS SKILLS

Artificial Intelligence:	ChatGPT, Kiro, Amazon Q, Claude
Cloud Service Provider (CSP):	AWS, Azure, GCP, Oracle, IBM
Containers:	Solaris Containers, *BSD Jails, Traditional Docker, OpenShift, Kubernetes, CSP-Managed: AWS ECS/ECR
CI/CD	Terraform, Ansible, SaltStack, Git, GitLab, Bitbucket, GitHub and SourceTree
Machine Learning:	Solid understanding of ML algorithms such as ensembles, boosting, adaboosting, bagging, decision trees, and anomaly detectors/predictors. Libraries supported: Pandas, Numpy, Seikit-learn TensorFlow. Tools: Orange and KNIME
Application and Web Server technologies:	JBoss EAP, Microsoft IIS, Apache, Tomcat, Nginx
Development Environments and Libraries:	PyCharm, Cloud Shells (AWS, Google, Azure), AWS Cloud 9, Visual Studio Code, AWS Kiro
Collaboration Development tools:	Atlassian Suite (Jira, Confluence, Stash, Source Tree, Crowd, BitBucket), Slack, ServiceNow
Programming/Scripting Languages:	Bash shell scripting. Python, mainly in conjunction with YAML and Jinja2 in SaltStack state development
High Speed File Transfer:	Aspera and OpenSSH w/HPN. Contributed to the HPN community during the OpenSolaris good old days.
Operating Systems:	Window 11/Server 2025, RPM-based (RHEL/Fedora), MacOS, iOS, iPadOS
Enterprise Identity and Access Management:	Active Directory and Directory Services (DNS and DHCP), Forefront (FIM), Group Policy Object (GPO), LDAP, Directory Server, Likewise, and Centrify. Deep understanding of PKI and PKI/E using CAC, SSL/TLS, and NSS.
Remote Management:	OpenSSH, Remote Desktop Services, Avocent KVM/IP, SaltStack (for Remote Execution)
Network and System Monitoring:	Nagios/Icinga2, Splunk, Elastic Search, LogStash, Kibana, Syslog, Syslog-ng, Rsyslog, SNMP
Server/Node Provisioning:	RHEL Kickstart, Windows Imaging Format (WIM), Cobbler, PXE., Packer, GCP Compute Engine, AWS Cloud formation
Firewalls:	IPTables, FirewallID, MS Forefront, GCP VPC Network Firewall, AWS Firewall / Security Groups. Etc.
Enterprise Email:	Microsoft Exchange and used Postfix for relaying to MTA
EA Frameworks and Tools:	SABSA (Security) and Zachman, FEAF, DoDAF. Tools: MEGA, System Architect, Visio
Cross Domain Solutions - Guards:	Raytheon High Speed Guard (HSG), BAE XTS/DataGate, OWL, Radiant Mercury, TDX., Cubic
Troubleshooting utilities:	TCPDump, WireShark, nslookup, netstat, watch, htop, strace, route, ifconfig
Virtualization Technologies:	VMware (vSphere, vCenter, ESXi, Fusion), Vagrant, VirtualBox, Virtualization using Hypervisors type 1-2 KVM/XEN, RHEV, Open Stack, Solaris Zones/Containers, Hyper-V
CND Tools for log-based telemetry:	Splunk, NMap, TCPdump, WireShark, Elastic Search, LogStash, Kibana, OpenSearch
ICD 503 Security Compliance:	eEye Retina, McAfee Enterprise Policy Orchestrator (ePO), Host-Based Security System (HBSS), XCCDF, STIG, SRR., Security Checklists, SCAP compliance tools such as openSCAP, ACAS and commercial Nessus, HubbleStack
Penetration Testing:	WHAX, Knopix, Backtrack, Kali, Fedora Labs
Distributed Computing:	Apache Storm, Apache Zookeeper, ZeroMQ (used with SaltStack), Kafka, AWS Kinesis
DevSecOps:	jFrog Artifactory and X-Ray, Jenkins, SonaQube, AWS Developer Tools (CodeDeploy, CodeCommit, etc.), Snyk
MacOS tools:	PyCharm, virtualbox, vagrant, MS Office Mac, TexMate, iTerm2, Evernote, tmux, xcode, homebrew, cask, zsh, OmniGraffle
Zero Trust Architecture tools:	Azure AD, Sailpoint, Radiant Logic, OPA, Hexa

PROFESSIONAL EXPERIENCE

Talon Security Engineering LLC. Gaithersburg, MD, '22 May – Pres. Founder/Chief Engineer. **Company Website:** <http://talonsec.co>

- ⇒ Lead and direct a specialized cybersecurity engineering and executive advisory practice supporting federal agencies and mission-critical programs. Provide C-suite leaders with strategic guidance to modernize and secure complex enterprises through **Quantum-ready networking, multi-cloud platform engineering, AI-driven cybersecurity, and Zero Trust modernization**. Deliver hands-on expertise in secure systems design, IT security automation, cloud-native transformation, and advanced application security testing across IL4/IL5 environments.
- ⇒ AI-native innovation initiatives in support of commercial start-up companies. More info in our case studies: <https://talonsec.co/casestudies.html>
- ⇒ Operate as a senior technical advisor and solution architect, offering services through C2C or 1099 engagements. Responsibilities include shaping cybersecurity strategies, maturing engineering programs, and building secure cloud platforms aligned with **NIST RMF, DoD Zero Trust**, and emerging **AI-security governance** frameworks.
Professional Services including Security and Software Engineering are available for sub-contracting as a C2C or independently as 1099.

Invictus International Consulting (Invictus), LLC. Alexandria, VA, '18 May – Pres. Chief Security Engineer / Cloud Security SME.

- ⇒ Leading a team of Cybersecurity Engineering Subject Matter Experts (SMEs) supporting DoD and IC missions. In this capacity, Mr. Reguerin provides individual unit operating principles to maximize alignment within the company, team, and with others while delivering on client sites. The specific areas Mr. Reguerin is responsible for:
 - **Executive Leadership:** Provides executive leadership, guidance, and vision in the company Cloud Security Engineering capability space, ensuring on-site/hands-on systems delivery support to various DoD/IC client sites with unique DevSecOps/Cloud Engineering, API Management, and Microservices requirements. In support of these areas, my focus has been ensuring security engineering rigor is applied to disruptive technologies - fostering natural cohesion between development and operation teams, and ultimately helping with the success of the customer mission goals and objectives in the Security Engineering space.
 - **Business Development:** Crafts technical and cost volumes in response to RFI/RFP/RFQ requests.
 - **Reporting structures:** Directly manage a large team of ~40 systems/software/security engineers/software testers and data scientists dedicated to the Invictus Cyber Security Engineering on-site delivery practice.
 - **Zero Trust Architecture:** Leads a team of Security Engineers shaping the adoption of Zero Trust Architecture and security policy for DoD/IC cloud environments (IaaS, PaaS, SaaS) across U, S, and TS domains. Provides expertise in Identity and Access Management using a cloud-first approach using Azure AD and leveraging existing legacy technologies such as RadiantLogic and Sailpoint.
 - **New Cloud Service Adoption:** Led a team of Cloud Security Engineers shaping Cyber Security Engineering and security policy for DoD/IC cloud environments (IaaS, PaaS, SaaS) across U, S, and TS domains. Provides expertise in cloud security engineering and support of RMF A&A activities of new cloud services, new cloud providers and environments, and applications and systems deployed to the DoD/IC cloud or platforms. Educate and train Cyber Security Engineering staff on cloud engineering and cloud security best practices. Enhance the DoD/IC client security posture for current and future cloud architectures.
 - **Cloud Service Provider (CSP) Hardening:** Leads engineering effort using DevSecOps and Continuous Monitoring (ConMon) practices to implement and enforce security controls across DoD/IC multi-cloud environments (IaaS, PaaS, SaaS). Developed reference architecture/implementation guides on using policy-as-code and GitOps practices for faster Risk Management determination and obtaining Authorization to Operate (ATO) following the Risk Management Framework (RMF).
 - **Enabled Penetration Testing Environments:** Leads the Cross Domain-enabling capability for transferring pen-testing tools (such as Kali) from low to high environments. Managed IAM Roles/Users to ensure proper access to tooling repos and environment.
 - **Data Science and Experimentation Environments:** Led a team of Security Engineers implementing reference architectures and implementations for DoD/IC Missions trying to use Data Science technologies.
 - **Software Defined-Networking:** Leads an engineering team responsible for a major IC customer doing a digital transformation and network modernization leveraging Software Defined-Networking in a Hybrid and Multi-Cloud environment.
 - **Cloud-Native Infrastructure and CI/CD:** Leading systems implementation and delivery of a unique Cloud-Native CDS capability using several AWS services to scale content filtering, sanitization and transformation. Hands-on, daily use of Terraform and Ansible to build/maintain Infrastructure as Code (IaC) in AWS using DoD DevSecOps Reference Design. In this capacity I've authored several Cloud formation templates, terraform modules, ansible and bash scripts to build and automate the entire system including all networking components such as AWS VPC, Subnets, security groups, as well as perimeter defenses using AWS Firewall and authored several AWS IAM identities (roles, policies, etc). To this end, I leverage Bitbucket Pipelines to build and harden docker images and containers that are then ingested and used in AWS ECS. In addition, I've authored and number of AWS lambdas and Step Functions that are created and maintained using terraform modules to support AWS OpenSearch clusters and assist OPS and Security Teams with overall system health and status as well as Security Information and Event Management (SIEM) and monitor configuration drift.

University of Maryland Global Campus (UMGC), Frederick, MD. '22 Aug – Apr '24. Adjunct Faculty. Cloud Technologies in the Department of Cybersecurity.

- ⇒ Mr. Reguerin is responsible for designing and implementing hands-on and project-based Cloud and Cybersecurity curricula covering topics and technologies to position students to succeed in real-life industry or Gov contracts using cloud-native solutions. Prepares students to pass cloud and cybersecurity certification exams (AWS, Azure, ISC2, CompTIA, etc.).

Steel Point Solutions, LLC. Calverton, MD, '16 – '18 May. Director of Research & Development (R&D).

- ⇒ As the R&D Director, Mr. Reguerin spearheaded two critical strategic growth areas. **First**, I provided executive leadership, guidance, and vision in R&D product development, focusing on innovative software and security engineering efforts hosted in multiple cloud providers while targeting commercial markets. In this capacity, Mr. Reguerin was also responsible for planning and managing all programs across the R&D unit, from the definition, requirements planning, budgeting, scheduling, and product delivery. **He second** provided SME on-site/hands-on systems delivery leadership in various DoD/IC client sites with unique DevOps/CDS Engineering and Cloud technology requirements. In support of these two areas, Mr. Reguerin focused on using disruptive technologies that foster natural cohesion between development and operation teams and ultimately help with the success of the customer mission goals and objectives in the Cybersecurity space and CDS niche market. Key to these growth areas is Delivering Machine Learning-based products to the cybersecurity operations community to deploy and operate effective new cybersecurity capabilities and services quickly. Through innovation, Mr. Reguerin built products to detect and mitigate adversaries launching malicious cyber activities. Specific areas Mr. Reguerin was responsible for:
 - **Hybrid cloud environment administration:** Maintained Corporate IT services (Recruiting, HR, Business Development, Finance, etc.) using VMware 6.5, AWS, and GCP.
 - **Business Development:** Crafted technical and cost volumes in response to RFI/RFP/SBIRs/STTR requests.
 - **Process Engineering:** Drove the creation of process-related initiatives to enhance business performance outcomes.
 - **Mentoring and Coaching:** Lead and inspire by example while reinforcing individual team operating principles to maximize alignment within the company, team, and with others while delivering on client sites.
 - **Reporting Structures:** Directly managed mid-sized teams of ~15 systems/software/security engineers/software testers and data scientists dedicated to the Steel Point-developed platform/product engineering. Also managed ~10 Sr. Delivery System Engineers and Site Reliability Engineers on client sites supporting various sub-contracts and reported directly to the company CEO.
 - **Cloud Providers:** Managed several cloud service providers used for hosting company IT infrastructure and product development and used AWS core services such as EC2, S3, VPC, Route 53, IAM, CloudTrail, CloudWatch, and CloudFormation to host production, product integration, and **bug bounty** environments. Uses and manages a smaller node cluster for testing in Google Cloud Platform leveraging Cloud Shell, Cloud Launcher, Compute Engine, App Engine, SQL, VPC Network, Network Services (Cloud DNS and Load Balancing), StackDriver (Monitoring, Logging and Debugging). Also used and managed company IT infrastructure using VMware 6.5, focusing on VMware Software-defined Data Center products: vSphere 6.5 vCenter and vSphere Hypervisor (ESXi) and built a volatile offline demo, dev and test environments with Vagrant/salt-cloud and coupling VirtualBox. Took advantage of Terraform to create a cloud-agnostic and cloud-based CI/CD environment to integrate with Bitbucket and Slack.

- **Windows Server Hardening:** Engineered an automated deployment and hardening methodology using Windows Server 2016 nodes hosted on VMware, AWS, GCP, and Azure
- **Health Status & Monitoring:** Used various tools to gain efficiencies when monitoring hundreds of nodes and applications. **PRTG:** Used and developed PRTG sensors for monitoring application health status. **Splunk:** Engineered Splunk forwarders, search heads, and indexers across hundreds of Linux nodes. Created dashboards to have better situational awareness. **Elastic:** Engineered and implemented an ELK-based solution as an alternative to Splunk; also used Elastic Beats to collect and aggregate logs from thousands of web-based applications supporting Modern Honeypot Network sensors. **Google StackDriver:** Used and implemented StackDriver to monitor the development server stack. **AWS CloudWatch:** Engineered solution to relay on-premises server and application logs to CloudWatch for increased fidelity and reliability of log collection, metrics, and Executive Level consumption.
- **Computer Network Defense (CND) Engineering and Administration:** Engineered a distributed Honey Pot using Open-Source tools such as Modern Honeypot Network (MHN) and Elastic. Used research tools such as censys.io, Virus Total, zmap.io for large-scale analyses. Worked with the product development team to produce meaningful indicators of compromise reports using open standards such as STIX, TAXII, and CybOX. Uses threat intelligence tools such as mnemonic
- **Malware Analysis:** Used several tools to understand malware mutex attributes such as Inetsim, GFI Sandbox, ThreatExpert API, **RegShot**, and FakeNet. Developed and uses YARA signatures. Leverages situational awareness tools such as contagio dump blog, malwar.com, urlquery.net. Worked with malware analysts to create better strategies and analyses around auto-pivoting techniques. Uses reverse DNS tools such as whoisology.com, whoismind.com. Understands and uses private web-surfing methods and tools such as robtext.com, chrome private mode, etc. Leverages knowledge of managed attribution network techniques for masking identity while conducting security research. Understand how to use tools for determining previous snapshots in time of potential targets: archive.org. Uses web-sniffer.net and other open-source tools to conduct security research on websites/applications. Uses IDA Disassembler for debugging and tracing of malware in sandboxes.
- **Firewall Management:** Designed, built from scratch, and managed firewall rules using Vyatta Firewall CLI and Juniper vSRX
- **Network Management:** Managed a small Juniper QFX. Cluster for L2/L3 routing and switching among several private VLANs
- **Bug bounty:** Organized bug bounty projects and collaborated with security researchers using HackerOne, BugCrowd, and SynAck

Booz Allen Hamilton., Rockville, MD. '07-'08. re-hired '10 - '16. Sr. Lead Technologist in DevSecOps/CDS. Engineering.

- ⇒ Provided DevSecOps/CDS. Engineering and Cloud technologies SME, technical leadership, guidance, and vision across various DoD/IC clients. In that capacity, I'd used my cybersecurity technical background and worked on projects with start-up company drive/mentality and fast-changing/growing requirements. Specifically, my focus was:
- **ECDS SME:** Led secure design, architecture, engineering, and automation of a large-scale Cloud/SOA-based Enterprise Cross Domain Solutions in a cloud-based environment. In this capacity, Mr. Reguerin pioneered the engineering, architecture, and implementation efforts for standing up a CDS. Software Security and Infrastructure testing lab using cloud IaaS/PaaS platforms, which consisted of a distributed and heterogeneous (*NIX and Windows) networking environment in support of several Cross Domain guard technologies such as HSG., Datagate, TDX., Radiant Mercury, OWL., DSG., etc. I also directed the continuous evolution of the architecture, development, and integration of Deep Content Inspection (PDI) tools such as Purifile, Apache Tika, DCF, OPSWAT MetaScan, FireEye detonation chamber as well as other mission-specific filtering capabilities such as clean and dirty-word checks, MIME Type and File Type checks in support of many CDS guard vendors.
 - **DevSecOps SME.:** Pioneered the implementation of a Software Supply Chain (SCRM) of application builds, deployment, and release management using VMware, vagrant, SonaType Nexus, Bamboo, and Saltstack with custom bash and python scripts in support of a Continuous Integration (CI) and pre-production ready Continuous Deployment environment (CD). I also engineered a tailored event-driven infrastructure solution using autonomic principles of self-healing. Used Saltstack reactor system and beacons.
 - **Agile team coach and collaboration tools engineer:** Introduced, architected, installed, configured, and maintained Atlassian tool suite (JIRA, Confluence, Stash, Source Tree, Bamboo, HipChat, Crowd) in support of my DevOps team. Tools were used daily during stand-up meetings, bi-weekly planning, and retrospective meetings.
 - **Health Status & Monitoring:** Developed, configured, installed, and maintained an event-based monitoring solution used by Site Reliability Engineers using syslog-ng, rsyslog, Nagios/Icinga2 with tailored traps for SNMP and a customized Splunk dashboard. At the same time, he architected, engineered, and deployed a log-based telemetry platform to extract operational insights around Insider Threat Detection and Advanced Persistent Threats.
 - **System Automation:** Automated Operating Systems (RHEL/CentOS 5/6/7, Windows XP/7/2008) hardening, patching, and remediation using Saltstack, openscap following STIG and security best practices. Also, automated machine image creation using vagrant packer in conjunction with custom-developed kickstart scripts (bash and Python) for building Just Enough OS (JeOS) platforms and provisioned images to VM, or bare-metal using customized bootstrapping scripts – all driven and orchestrated with Saltstack. Automated the creation of custom PKG and RPMs using FPM. Led the requirements and architecture of an automated test harness using Selenium.
 - **PKI and PKI/E:** Deep understanding of Identity Management using PKI/E, LDAP, Windows Active Directory integration, PAM, sudoers, and role separation. PKI-enabled Jboss EAP. using DoD PKI and NSS PKI Trust Anchors. Piloted the automation builds of PKI RootCA and PKI SubCA using Windows Server 2008 and RHEL 5 with Thales and SafeNet Hardware Security Modules.
 - **Business Development:** Authored technical and cost volumes in response to RFP/RFIs.
 - **Management:** Managed small/large geographically distributed teams. Standardized collaboration tools such as Atlassian, Google Hangouts, and Slack. Career Manager and mentor to interns and new employees. Also, timesheet approver for several staff members.

WISSE Corp., Bethesda MD, 2008 – 2010 SOA. and Security Solutions Architect.

- Provided entrepreneurial leadership in transforming the company into a premier Enterprise Architecture boutique consulting firm. Aggressively identified Enterprise Architecture and Information Security business opportunities, structuring and participating in strategic proposal development and tactical presentations to DHS Customs and Border Protection (CBP) contract prime, other subcontractors, and CBP clients.
- Mr. Reguerin provided SOA and Security Solutions Architecture SME to the DHS CBP Chief Enterprise Architect. He bolstered the adoption of information security throughout CBP and the Office of Information Technology (OIT). Led the implementation of the following **four major CBP initiatives:**
 1. CBP EA Security Architecture project: Designed, developed, and implemented the first CBP Enterprise Security Architecture and its integration with the CBP EA. Created a modular Enterprise Security Architecture Framework (ESAF) in MEGA, the CBP EA modeling and analysis tool.
 2. CBP EA Release Management project: Architected and implemented an EA Release, Change, and Version Management process using Dimensions 10 and MEGA.
 3. CBP EA SOA project: Developed a methodology for identifying SOA Shared Service Candidates, which consisted of a Service-Oriented process that explains what and how SOA Shared Services need to be identified.
 4. DHS OneNet and CBP LAN project: Used MEGA modeling and analysis to capture the diagrams, models and system design documents of the DHS OneNet, Trusted Internet Connection (TIC), High Assurance Gateway (HAG.), Reverse Proxy, Policy Enforcement Points, CBP LAN system and mapping them to the Performance Architecture, Business Architecture, Service Architecture layers of the Enterprise Architecture for a complete Line of Sight and future gap analysis.

SRA International, Inc. Fairfax VA, 2004 – 2008. Sr. Security Tech Lead/ .NET Software Engineer.

- Sr. .NET Software Engineer and Security technical lead serving on the AITS and RCAS program. Provided software/security engineering leadership, guidance, and vision.:

Northrop Grumman IT/Compex Corp. Arlington VA. 2003-2004. Senior Software Developer.

- Managed SDLC application development and product demos for US ARMY G-3 and HQDA initiatives. Developed several web applications using ASP, ASP.NET, and VML.

Hughes Network Systems (contractor). Germantown MD, 2001-2003. Programmer/Data Analyst

- Led software development activities in the billing department—extensive use of Oracle 8i, TOAD, Crystal Reports 8, and VB 6.0.

E-Com Systems. Gaithersburg MD, 2000-2001. Programmer/Data Analyst.

- Led the E-Commerce client technical support department and contributed to the architecture and design of the web portal.