# CHRISTOPHER BIASSEY

cbiassey@masonlive.gmu.edu
Alexandria, VA / Mount Pleasant, SC

http://www.linkedin.com/in/cyberguychris

## CERTIFICATIONS

- CEH – Certified Ethical Hacker
- CISM – Certified Information Security Manager
- CISSP – Certified Information Systems Security Professional
- Cribl Certified Observability Engineer (CCOE) | Admin
- Cribl Certified Observability Engineer (CCOE) | User
- CSM – Certified Scrum Master
- GCIH – GIAC Certified Incident Handler
- Linux+
- Network+
- SA Certified SAFe® 6 Agilist
- Security+
- Splunk Core Certified Power User
- Splunk Core Certified User
- Splunk Enterprise Certified Admin
- Splunk Enterprise Certified Architect

## EDUCATION

### Marymount University

***May 2019*** MS, Cybersecurity

### George Mason University

***December 2015*** BS, Criminology, Law, and Society

- Concentration in Homeland Security and Justice
- Minor in Intelligence Analysis
- 27 Elective credits in Information Technology
- Dean's List Spring 2014 and Fall 2014

## EXPERIENCE

### Grey Wolf Security | Alexandria, VA

***Splunk Engineer / Security Engineer*** *11/2020 – Current*

TekStream Solutions (7/2023 – Current)
Configuration of Splunk within a MSSP/VSOC environment.
Educational facility customer base.
Custom content development.
Splunk Cloud Enterprise Security setup and configuration.
Setup appropriate parsing in Splunk for custom log sources and types.

MUFG / UnionBank (1/2022 – 4/2023)
Migration of Splunk from on-prem to Cloud.
Custom content development.
ServiceNow integration and configuration.
Setup appropriate parsing in Splunk for custom log sources and types.
Test and validate the logs for proper parsing.
Document the final configurations for log parsing into Splunk.

Department of Justice (DoJ) (11/2021 – 7/2022)
Capacity and resource management of Splunk.
Configuration and deployment of apps.
Executive briefings to senior management regarding progress, status and best practices.
Maintenance of lab infrastructure for testing and reproducing production configurations.
Management of 8 cluster Splunk deployment for DoJ agencies (ATF, BOP, DEA, USMS etc.)
Onboarding of standard and non-standard log sources into Splunk.
Reviews and recommendations for new products and capabilities to stakeholders and management.
Upgrade Splunk from 7.x to 8.x.

Department of State (8/2021 – 11/2021)
Consulting work performed under Knowledge Management Inc
Support State Department's production and non-production Splunk instances.
Splunk documentation regarding best practices.
Configuration and deployment of apps.
Onboarding standard log sources into Splunk.
Troubleshooting and error recovery of Splunk.

Army Intelligence and Security Command (INSCOM) (12/2020 – 7/2021)
Consulting work performed under GuidePoint Security.
Support INSCOM's geographically separated Splunk instances.
Architecture design and best practices for Splunk.
Migrate Splunk from RHEL 6 to RHEL 7.
Upgrade Splunk from 7.x to 8.x.
Executive briefings to senior management regarding progress, status, and best practices.
Splunk Enterprise Security configuration and management.
Vet and deploy apps as requested by customer.
Provide training to analysts on proper configuration and use of Splunk.
Remain on call to support issues as they arise.

## Leidos, Inc | Springfield, VA

***Senior SIEM Subject Matter Expert*** *8/2019 – 12/2020*

Defense Information Systems Agency (DISA) Joint Regional Security Stacks (JRSS).
Support DISA's ArcSight and Splunk instances located across the world.
Architecture design and best practices for both ArcSight and Splunk.
Elastic migration from ArcSight and Splunk.
Executive briefings to senior management regarding progress, status, and best practices.
Splunk Enterprise Security configuration and management.
Vet and deploy apps as requested by customer.
Provide training to engineers on proper configuration of ArcSight and Splunk.
Remain on call to support issues as they arise.
Completed Elastic Engineer training.

## AnaVation, LLC | Washington, DC

***Solutions Architect*** *4/2019 – 8/2019*

Subcontract with GDIT.
Federal Bureau of Investigation (FBI) Enterprise Security Operations Center (ESOC).
Support ESOC's ArcSight and Splunk instances.
Install and configure ArcSight connectors and Splunk forwarders.
Migrate data feeds from ArcSight to Splunk.
Provide architecture design and best practices for move from on premises to cloud based Splunk.
Configure and maintain Splunk integrations with products such as Remedy.
Splunk Enterprise Security configuration and management.
Vet and deploy apps as requested by customer.
Upgrade Splunk from 7.2 to 7.3 release.
Provide training to analysts on proper usage of ArcSight and Splunk.
Remain on call to support issues as they arise.
Support AnaVation on bids and proposals from a technical and business perspective.

## MicroSys, LLC | Reston, VA

***Cyber Security Solutions Architect*** *10/2018 – 4/2019*

Subcontract with ManTech.
Department of Homeland Security (DHS) Continuous Diagnostic Mitigation (CDM) Program.
Support NPPD/CISA efforts and lead solution delivery for FDIC and SEC.
Provide team support to EPA, HUD, NRC, NSF, SBA.
Vendor agnostic solution design and delivery.
Perform discovery sessions to gather information for solution design.
Design, build and implement enterprise-class security systems for a production environment.
Align standards, frameworks and security with overall business and technology strategy.
Identify and communicate current and emerging security threats.
Solution proposals with multiple stakeholders including C-level executives and SMEs.
Design security architecture elements to mitigate threats as they emerge.
Create solutions that balance business requirements with information and cyber security requirements.
Identify security design gaps in existing and proposed architectures and recommend changes or enhancements.
Train users in implementation or conversion of systems.

Maintain vendor relationships so that solution deliveries are seamless to customers.

## Zachary Piper Solutions | Fort Belvoir, VA

***Cyber Security Architect*** *1/2017 – 10/2018*

Subcontract with Leidos.
Defense Threat Reduction Agency (DTRA).
Computer Network Defense Sustainment (CND-Sustain).
All work within Network Operations & Security Center (NOSC).
Leidos Team Award July 2017 (For teamwork in passing CCRI with “Excellent” score).
Team lead promotion in Feb 2018.
Architecture of systems while detailing potential threats and mitigations to management.
Change Control Board (CCB) documents for new installations and configurations.
Brief senior leadership on configurations and capabilities.
Mentor and train junior employees on tools and procedures.
Create content to assist analysts in reviewing and detecting notable security events.
Manage and deploy Sourcefire Intrusion Detection Systems (IDS) at locations worldwide.
Configure Linux systems to DoD specifications including STIGs.
ArcSight Subject Matter Expert (SME) for agency and contract.
Build and configure Enterprise Security Manager (ESM) version 6.9.
Perform migration of Windows Unified Smart Connectors to Native Smart Connectors.
Upgrade all ArcSight Smart Connectors to version 7.7.
Configure Connectors for ePolicy Orchestrator, Syslog, Sourcefire 4.x/5.x and Microsoft software.
Lead Implementation of PKI certificates on ArcSight to bring agency into compliance with DoD initiative.
Create active/active ESM setup using 2 different sites for a primary and backup (failover capability).
Translate content from Splunk into ArcSight ESM.

## Hewlett Packard Enterprise | Washington, DC

***ArcSight Security Consultant*** *1/2016 – 1/2017*

Professional services consultant primarily handling Federal Civilian customers.
Train customers on product features and uses.
Present products and capabilities to future customers.
Install and troubleshoot ArcSight ESM, SmartConnectors, Forwarders, Logger, and Connectors.
Perform administration, upgrades, and troubleshooting on all aspects of the ArcSight platform.
Conduct use case development leveraging all features of the ArcSight platform (reports, rules, dashboards, network and asset model, trends, pattern discovery, etc.).

## Defense Point Security, LLC | Washington, DC

***Senior Security Engineer*** *7/2015 – 1/2016*

Prime contract with U.S. Immigration and Customs Enforcement (ICE).
All work in ICE’s Security Operations Center (SOC).
Configure and deploy ACAS/Nessus scanners to field offices around the United States.
Manage and configure Suricata IDS.
Custom rule creation, testing and implementation for Suricata IDS.
Lead deployment of McAfee NSP IDS across entire agency including configuration and tuning.
Troubleshooting of Splunk connectivity issues for log collection.
User management of Splunk.
Perform Splunk searches for troubleshooting and security incidents.
Setup and configure VMWare ESXi hosts for security applications.
Manage Windows 2012 and CentOS Linux mixed environment for security tools.

All system configurations involved applying DHS hardening guides.

## Defense Point Security, LLC | Washington, DC

***Senior Information Assurance Analyst*** *3/2015 – 7/2015*

Prime contract with U.S. Immigration and Customs Enforcement (ICE).
All work in ICE's Security Operations Center (SOC).
Provide technical reviews in conducting Security Controls Assessment (SCA) activities.
Responsible for using Risk Management Framework (RMF) NIST 800-37 and NIST 800-53.
Create list of common findings produced by scans within the agency and their related controls.
Write recommendations for false positives and fixes in the scan analysis provided to the customer.
Conduct interviews of Information System Security Officers (ISSOs) to ensure RMF compliance.
Scans using Nessus, DB Protect and Web Inspect to test security controls.
Travel to perform on-site security scans and assessments for air gapped networks.

## Lockheed Martin Corporation | Fort Belvoir, VA

***Senior Cyber Intelligence Analyst*** *3/2014 – 3/2015*

This position is a continuation of my previous position. Lockheed Martin won the contract award. My responsibilities are indicated in the description below.

## Valador, Inc | Fort Belvoir, VA

***Senior Information Security Engineer*** *10/2013 – 3/2014*

Subcontract with Lockheed Martin.
Defense Threat Reduction Agency (DTRA).
Computer Network Defense Sustainment (CND-Sustain).
All work in Network Operations & Security Center (NOSC).
Install, operate and maintain IDS, IPS and firewall devices.
Administration of Windows 2012, 2008, 2003 and RedHat Linux environment.
Configure and maintain ArcSight Smart Connectors.
User management of ArcSight and Splunk.
Perform searches using Splunk for troubleshooting and security incidents.
Setup, configure and maintain of Solera packet capture devices.
Run ACAS scans and remediate findings for Linux and Windows.
Configure and manage ACAS scanners for our enclave.
Successful migration of SourceFire IDS from version 4.9 to 4.10.
Create custom rules for SourceFire IDS based on new threats.
Set filters, monitor and respond to alerts at both headquarters and remote sites.
Upgrade of entire network infrastructure to new Cisco hardware.
Migration of VPN tunnels from Cisco and Sonicwall platforms to Fortigate devices.
Build of VMWare ESXi with vCenter.
Prepare and deliver briefings on Computer Network Defense (CND) status.
Support Certification and Accreditation testing.
Perform technical interviews for prospective employees.
Work with Computer Network Defense Service Provider (CNDSP) customers to resolve outages or assist in deployment of new sensors around the world.

## Valador, Inc | Fort Belvoir, VA

***Senior Information Security Engineer*** *1/2012 – 10/2013*

Subcontract with Lockheed Martin.
Defense Threat Reduction Agency (DTRA).
Security Testing and Evaluation (ST&E) for Certification and Accreditation (C&A).
Review of Connection Approval Packages (CAP).
Review DISA STIGs for correct security controls on Apple, Windows, and Linux systems.
Serve as main point of contact for security controls on network devices such as Cisco routers, switches, Sidewinder firewalls and Linux systems.
Review Systems Security Plans (SSP).
Track DIACAP packages through SharePoint until completion.
Voting member of DTRA's CCB and ERB boards.
Assist in performing reviews that aided the Agency in receiving a passing CCRI score.
Maintain compliance for agency within Vulnerability Management System (VMS).

### Valador, Inc | Herndon, VA

***IT Manager*** *5/2011 – 1/2012*

### Oracle Corporation | Reston, VA

***Application Systems Administrator*** *7/2008 – 5/2011*

### Pomeroy IT Solutions | McLean, VA

***Site Support*** *5/2005 – 7/2008*

### Net Tech Group | Alexandria, VA

***Lead PC Technician*** *10/2004 – 5/2005*

### Touch Point Media, LLC | Alexandria, VA

***Owner*** *4/2003 – 2/2004*

## CLEARANCE

- Secret – Department of Defense 9/2011.
- Top Secret – Department of Defense 3/2012.
- ICE EOD – Immigration and Customs Enforcement Entry on Duty 3/2015.
- DHS HQ EOD – Department of Homeland Security Entry on Duty 4/2016, 5/2023
- DoJ EOD – Department of Justice Entry on Duty 4/2019, 9/2021.
- DoS EOD – Department of State Entry on Duty 7/2021.
- Senate BI – Capital Police Background Investigation 4/2018.
- House of Representatives BI – Capital Police Background Investigation 6/2022.
- SCI – 4/2018, 8/2019, 7/2020, 12/2020, 8/2022.
- Counterintelligence (CI) Polygraph – 5/2019.