##### Professional Summary Of Qualifications

* A results-driven, well-rounded and seasoned Professional with 10+ years of extensive hands-on experience in various fields of Computer Science and Cybersecurity.
* Many of the fields I have worked in and/or have taken graduate level course in are the following: Network Administration (LAN/WAN), Network Security, **Application Security**, Network Security Operations, Network Analysis, Systems Administration, Technical Support, Penetration Testing, SDLC, Help Desk Administration, Service Now Admin, Computer System Security, IT Architectures, Security Management, Disaster Recovery, Cybersecurity Architecture, API Security and Computer Programming.
* Monitor emerging cybersecurity threats, technologies and vulnerabilities including risks specific to supply chain operations, to ensure applications and systems maintain a proactive and resilient security posture.
* Highly effective at communicating plans, requirements, and results to professionals at all management levels and technical backgrounds.
* Designed and implemented secure systems and network architectures in collaboration with IT and software development teams, embedding security throughout technical systems and processes.
* Identify areas within Application Security which can be made more efficient through automation, contributing ideas and solutions related to our transition to continuous delivery and integration while working closely with the team to contribute to the creation and implementation of such programs/projects.
* Created automated solutions for application and cloud monitoring, with focus on exception-based alerting; Leverage open-source tools and commercial software like Dynatrace, Datadog, Splunk, and logic monitor wherever practical.
* Collaborate on change implementation plans and strategies, performing risk and impact assessments prior to change implementation.
* Hands-on experience in Security Design and Architecture. Responsible for complete security lifecycle architecture and technical assessments, including but not limited to design requirements assessment, threat modeling, code review and risk assessment. Guiding security requirements and objectives for product features and ensuring that the security program is aligned with product strategy and objectives
* Providing high quality documentation for internal customers and technical support teams, while managing team mailboxes and ticking systems.
* Continuously evolve corporate security policies, supporting their implementation across IT and software development teams. Maintain evidence of policy enforcement to support audits and certifications (e.g., GDPR, SOC1, SOC2 and customer security reviews).
* Provided regular updates to the executive team on KPIs, metrics, and the status of security initiatives, threats, and incidents, highlighting the effectiveness and areas for improvement in security controls. Establish and track security metrics to measure the performance of initiatives, ensuring ongoing refinement of security strategies and alignment with business goals.
* Continuously develop, harden and test an incident response plan to ensure swift and effective handling of security warnings, alerts, or attacks, ensuring that the company can respond quickly and effectively to minimize damage.

##### Professional Certifications/Education

##### Education

* Colorado Technical University ~ Sioux Falls, Colorado: Master of Science in Computer Science, Concentration in Software Engineering 2012, GPA: 3.50
* Colorado Technical University ~ Sioux Falls, Colorado: Bachelor of Science in Information Technology, Concentration in Security 2011, GPA: 3.50

# Colorado Technical University

* Security+, Network+, Software Engineering Methods, Computer Networks and Telecommunication, Client Java Programming, UNIX Network Administration, Object Oriented Methods, Software Engineering Application, Web page development - [University Awarded], VoIP (CHN, CDV, Call Manager/Call Unity/Unified Communications Services/Phones), Field Technician, Boson NetSim 14.0 (Routers, Switches, Stations), Remedy and ServiceNow Ticketing Engine

**Certifications**

* CompTia A+
* Network+
* CCENT (CSCO12392774), CCNA (CSCO12392774), CCNP (CSCO12392774)
* Security+
* Certified Ethical Hacker

##### Professional Experience

**Dexcom** 09/2023 – Present

*Application Security Architect*

* Work closely with the Site Reliability Engineering (SRE) team to continually monitor and maintain the security of production cloud systems.
* Managed, balanced and communicated business risk with security risk and vulnerabilities, and developed mitigation plans. Created and Developed Application Threat Model Capabilities, Software Assurance Maturity Model projects
* Worked to understand business requirements and apply security without adversely affecting the desired application functionality via technical security assessments, penetration tests, code audits and design reviews
* Performed product security feature specific implementation reviews (or penetration testing whole applications where applicable), API security testing and code reviews to identify vulnerabilities and provide critical security guidance to engineers
* Enhance our security automation, leveraging or building software security tooling to help scale product security operations and support overall vulnerability management practices
* Served a crucial role in identifying potential vulnerabilities, implementing robust security measures, and developing strategies to protect our digital assets from unauthorized access and cyber threats
* Assist in developing and implementing post-mortem and root-cause analysis processes to enhance controls and testing scenarios
* Managed and built the application security team including creating the team’s road maps and priorities.
* Full-scope reviews of current and future portfolio. This includes white-, grey- and blackbox assessments. Working with OffSec teams, engineers, and other members of the InfoSec org to harden products against very dedicated adversaries.
* Programming within multiple languages such as Java, C#, NodeJS, Python, Scala, Golang, and understand how to detect and remedy related security
* Lead Security Champion Programs aimed at community development and engagement with developers
* Working in AWS environments, with proficiency in AWS CLI, EC2, IAM, and related AWS services.
* Drive the adoption of advanced security technologies, including AI-driven threat detection, blockchain, and quantum cryptography where applicable.
* Standardized Secure Patterns, design and implement reusable patterns that promote security best practices and compliance across all engineering teams.

**Freddie Mac** 04/2023 – 09/2023

*Application Security Architect*

* Provided security architecture and design consultations to product teams, to help build applications that are secure from the start.
* Managed, balanced and communicated business risk with security risk and vulnerabilities, and developed mitigation plans. Created and Developed Application Threat Model Capabilities, Software Assurance Maturity Model projects
* Ability to understand business requirements and apply security without adversely affecting the desired application functionality via technical security assessments, penetration tests, code audits and design reviews
* Implemented complete security lifecycle architecture and technical assessments, including but not limited to design requirements assessment, threat modeling, code review and risk assessment. Guiding security requirements and objectives for product features and ensuring that the security program is aligned with product strategy and objectives
* Assess and improve existing security standards, practices, and controls to reduce vulnerabilities and enhance the organization’s security posture.
* Served a crucial role in identifying potential vulnerabilities, implementing robust security measures, and developing strategies to protect our digital assets from unauthorized access and cyber threats
* Proposed, designed, built, and deployed security solutions, frameworks, automation, and orchestration to secure cloud applications
* Managed and built the application security team including creating the team’s road maps and priorities.
* Provided understandable and transparent rationale for security decisions to all stakeholders, working with security team to maximize security coverage via team meetings/standups
* Advance Secure Software Delivery: Promote secure delivery practices by embedding security in the build and design phases, emphasizing fast feedback, observability, and operational excellence
* Created Security Champion Programs aimed at community development and engagement with developers

**Shipt, Inc** 06/2022 – 09/2023

*Staff Security Engineer*

* Lead security architecture and design consultations for product teams, to help them build applications that are secure from the start.
* Lead hands on security testing of products and services to proactively discover risk and track them to resolution with tools like Burp Suite, ZAP, Veracode, Invicti, Fortify, Nessus, Tenable or another intercepting proxy
* Served a crucial role in identifying potential vulnerabilities, implementing robust security measures, and developing strategies to protect our digital assets from unauthorized access and cyber threats
* Managed, balanced and communicated business risk with security risk and vulnerabilities, and develop mitigation plans. Created and Developed Application Threat Model Capabilities, Software Assurance Maturity Model projects and Security Champion Programs
* Drive and deliver security solutions across AWS cloud, container security (ECS/Kubernetes), CICD, and secure cloud-native architectures while ensuring compliance with standards such as PCI-DSS, ISO27001, SOC 2, NIST 800-53, and COPPA.
* Created and Developed security practices within the SDLC lifecycle via manual/automation methodologies using tools such as Check Marx, Veracode, & Whitehat (SAST), Snyk, Fortify, Contrast Security (MAST), SecureNow, Sonarcube, Hackerone, and API security tools.
* Designed and implemented secure operations and systems in a creative environment where security has not traditionally been a priority
* Designed and implemented security controls for networks, servers, storage, cloud, and virtualization platforms to protect against cybersecurity threats and exposed vectors
* Served as the primary point of contact and liaison for our Security Operations Center (SOC) partner, ensuring effective collaboration, communication, and coordination of security incident response efforts.
* Investigated and analyzed security incidents, conducted forensic analysis and provided incident response to minimize the impact of security breaches
* Worked with JIRA, Confluence, Gitlab, and GitHub. Ability to analyze programming languages such as C#, NodeJS, Golang, Python, Java, JSON, SQL, C++, API’s as well as open-source programs. Ability to express findings in formal reports
* Administered security awareness training program for employees to promote a culture of security and ensure compliance with security policies and procedures

**Disney Streaming Services** 06/2019 – 06/2022

*Sr Security Engineer*

* Lead security architecture and design consultations to product teams, to help them build applications that are secure from the start.
* Lead hands on security testing of products and services to proactively discover risk and track them to resolution. Expert with Burp Suite, ZAP, JFrog, Appknox, DataDome, Synopsis, AppScan, Noname, Hackerone, Github Security, Snyk, Checkmarx, and other application security tools.
* Oversee validation of security controls to ensure adherence with compliance and industry best practices OWASP, PCI, HIPAA, CWE 25 etc.
* Manage, balance and communicate business risk with security risk and vulnerabilities, and develop mitigation plans. Created and Developed Application Threat Model Capabilities and Programs
* Able to understand business requirements and apply security without adversely affecting the desired application functionality via technical security assessments, penetration tests, code audits and design reviews
* Created and Developed security practices within the SDLC via automation using tools sets such as Check Marx, Veracode, & Whitehat (SAST), Qualys & Fortify (DAST), Contrast Security, Snyk, Noname API Security, Zscaler, and Proof Point security tools.
* Used cryptographic processes such as Oauth, SAML, Open Connect, Auth0, key management, seeding, and PKI.
* Work closely with development teams to integrate secure coding practices into the API lifecycle and help design and deploy secure serverless solutions.
* Lead end-to-end application security reviews to ensure critical information is appropriately protected as well as architect, design, implement, support, and evaluate security tools and services.
* Worked with JIRA, Confluence, Gitlab, and GitHub. Ability to analyze programming languages such as C#, C++, .Net, Python, Java, JSON, SQL, Perl, PHP as well as open-source programs. Ability to express findings in formal reports
* Worked with Open-Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP), National Institute of Standards and Technology (NIST) Special and Synopsis

**NBCUniversal** 05/2018 – 06/2019

*Sr Security Engineer*

* Provide security architecture and design consultations to product teams, to help build applications that are secure from the start.
* Perform application security penetration testing of products and services to proactively discover risk and track the resolution.
* Subject Matter Expert on Burp Suite, Kali Linux, ZAP, Docker, JFrog, Cyberark, Tenable, Snyk, Bug Bounty (Hackerone), Rapid 7, One Trust and Splunk. Supported and integrated security services via GRC and Project management tools
* Lead Security Assessments, Threat Models, and Vendor Security reviews to support integration and implementation.
* Developed annual Self-Assessment Questionnaire (SAQ) PCI-DSS requirement with clients and 3rd party security vendors. Provide on-demand SAQ portal support to clients in coordination with 3rd party security vendors. Report status, findings and trends to internal|external leadership.
* Created and developed Application Security Champion’s Program aimed at community development and engagement with developers.
* Co-Created and managed integrated security pipelines within the SDLC by automation using tool sets such as Check Marx, Veracode, & Fortify (SAST), IBM AppScan, Github Security, Sonarqube, Snyk & Fortify (DAST) surrounding Jenkins CI Servers
* Managed Projects and Application Security activities/tasks across multiple teams and organizations ranging from Cloud Security (Wiz.io), Container Security (Nessus), and/or API Hardening.
* Lead internal vulnerability scans for new rogue devices or failed scans. Escalate to relevant information security, technology, operations teams within the organization. Summarize status, findings and trends to internal and external leadership.
* Performed end-to-end application security reviews to ensure critical information is appropriately protected as well as architect, design, implement, support, and evaluate security tools and services.
* Manage and build the application security team including creating the team’s roadmaps and priorities.
* Developed and contributed to the development of policies and procedures related to assigned information security processes. Developed consistent and repeatable processes to support day-to-day operations and meet service levels. Develops, publishes, and communicates operating procedures and guidelines along with any relevant policies and standards to support the assigned information security processes.
* Participate in the team on-call rotation to support engineering teams through timely design consultations, vulnerability analysis, fix verification, etc

**NewsCorp/HarperCollins Publishers** 10/2015 – 05/2018

*Sr Security Engineer*

* Served as security voice to product teams; identifying security gaps before they arise and helping provide remediation recommendations for any issues identified in the platform
* Define the overall visualization strategy to develop a self-service capability enabling the organization to consume or action vulnerability data
* Worked on system and/or web application vulnerabilities and risk assessment methodologies such as Common Vulnerability Scoring System (CVSS) or Open Web Application Security Project (OWASP) Risk Rating Methodology
* Understand, balance and communicate business risk with security risk and vulnerabilities, and develop mitigation plans. SME Application Threat Model Capabilities and Knowledge
* Able to understand business requirements and apply security without adversely affecting the desired application functionality via technical security assessments, penetration tests, code audits and design reviews
* Able to scale security within the SDLC by automation using tools sets such as Check Marx, Veracode, & Fortify (SAST), IBM AppScan & Sonarcube (DAST), Contrast Security, Snyk, Tenable and Qualys.
* Understand, review, and interpret vulnerability assessment and scanning results, reduce false positive findings, and act as security advisor to business unit partners
* Programming Experience with multiple languages and understanding on detection and remedy related security ex: Java, C#, NodeJS, C++
* Performed end-to-end application security reviews to ensure critical information is appropriately protected as well as architect, design, implement, support, and evaluate security tools and services.
* Worked with secrets management systems such as Hashicorp Vault, AWS KMS, GCP KMS, and Azure Key Vault
* Provided understandable and transparent rationale for security decisions to all stakeholders, working with security team to maximize product security coverage
* Effective understanding of security industry best practices such as protocols, cryptography, authentication, authorization, and secure application programming

**OWASP Foundation,** North Jersey Chapter 11/2015 – Present

*Member*

* NJ & NYC Local Chapter Member
* Open-Source Application Security Tester
* Open Source -- Code Reviewer
* OWASP Project Volunteer (Low Code No Code)
* OWASP Project Volunteer (OWASP Security Shepherd Project)
* OWASP Secure Code Review Tool Tester
* Vulnerabilities Assessment & Penetration Testing
* Expert knowledge of emerging API Testing
* Knowledge of Applied Cryptographic Protocols

**AT&T (*Consultant*),** Middletown, NJ 11/2014 - 11/2015

*Application Security Engineer*

* Performing security code reviews of source code repository of critical in-house business applications before deployment to production and after. Daily tasks include writing reports suggesting mediation techniques to remedy security problems uncovered during analysis.
* Supported internal AT&T tools used to catalog and document vulnerabilities that were found during reviews. Supported vendor security scripts used to scan code for problems such as plugins for Audit Workbench, SCA’s and HP WIE, also searched web for technical document findings
* Performed Vulnerability testing to verify whether controls can be bypassed to obtain any unauthorized access, using AT&T-developed tools and leading-edge scan tools from commercial software providers such as Dynamic Application Security Testing, HP Static Code Analysis, CheckMarx Static Application Security Testing and a new DAST tool called Constant Security.
* Responsible for learning and understanding industry’s Best Practices and annual published vulnerabilities to identify top risks to the security of application software. Attention is paid to the OWASP Top 10 software vulnerabilities, including writing reports suggesting mediation techniques to remedy security problems uncovered during analysis.
* Manage threat management platforms and programs like CheckMarx Static Application Security Testing, Mini Threat Model, HP Web Inspect Enterprise, and HP-Fortify Static Code Analysis to provide real-time data correlation, situation awareness reporting, active incident investigation, case management, trending analysis, predictive security alerting, and identifying False Positives.
* Performed penetration testing and SAST on network/system devices as well as applications written in JAVA, C#, J2EE, ASP.NET, PHP, SQL, & Python using AT&T Penetration Methodology. Work with development staff to recommend approaches to remediate security vulnerabilities found during code reviews.
* Worked with application development technologies such as .NET, Java etc. Intermediate to advanced database skills using SQL Server (includes design and scripting of tables, stored procedures, etc. using Visual Studio and SSMS)
* Looking for application security vulnerabilities ex: Cross Site Scripting, SQL Injection, Cookie Manipulation, Buffer Overflows, etc

**Sanofi (*Consultant*),** Bridgewater, NJ 11/2013 - 11/2014

*Network Security Engineer/Application Security*

* Global 4th level incident support and problem resolution for activities related to services provided in collaboration with the 3 Regional Service Delivery teams. ITIL v3 Methodology. Change Control. Incident and Problem Management
* Subject matter expert in technologies related to Web proxy, URL filtering, Log management, file exchange gateway (Keynectis OpenTrust MFT), Content delivery, Network firewalls and routers, System servers, Tibco, Aruba Network Devices, Checkpoint, Application development and integration. Also, Administrator Share point server/client infrastructure by implementing and maintaining environment for over 25 teams
* Provided participation on various projects in development, implementation and operational secure access services and acted as the subject matter expert on: VPN, Firewall, Proxy, SSL/IPsec, IIS Experience in Security, Domain Consolidations and Data Center Consolidation Projects
* Support, maintain and enhance web-based tools developed and deployed in the scope of Access Service and Network Infrastructure (.Net/C#, ASP.Net 4, MVC 4, VB.Net, IIS, MS-SQL JavaScript, HTML5, ADO.NET).
* Strong technical expertise with implementing Zero Trust Security principles, ensuring tight access controls, identity management, and network segmentation across hybrid environments.
* Provide security expertise in API Security, Application Security, Cryptographic Controls, and Networking to ensure the protection of sensitive data across the organization.
* Significant knowledge of technologies like Bluecoat SG products, Riverbed, F5 load-balancing, Log Logic, Keynectis OpenTrust MFT, Aruba Network Devices, Microsoft Direct Access Servers
* Strong working knowledge of common web application technologies such as .NET/C# 5.0, ASP.Net, VB.Net, MVC 4, Razor, IIS, MS-SQL, ADO.NET
* Strong working Knowledge of Windows, Active Directory, Unix/Linux based OS, Perl, PowerShell scripting, Citrix, RSA SecurID and EMC
* Understands complex applications functionality, triage issues and identities and documents resulting resolutions and displaying competent problem solving skills
* Perform security vulnerability assessments (manual & automated) of eCommerce web and mobile applications and systems.
* Analyze web application security scanner reports and validate false positives and false negatives. Create exploits, proof-of-concept for web application vulnerabilities (to prove they are true positives)

##### Professional Technical Expertise

##### Wireless Networking:

* WLANs, Cisco Catalyst Series Wireless Services Module (WiSM), Kismet, WEPcrack, WEPcrack, Wireless Security Auditor, AirMagnet

# Networking:

* LANs, WANs, SAN’s, VoIP, Wireless, Network Infrastructures, IPv4, IPv6, Secure Gateways, ARUBA, IP Addressing Schemes (Subnetting, VLSM/CIDR) MPLS VPN Firewalls/Site to Site (SSL/IPsec), Check Point, Riverbed, F-5 Load Balancing, Microsoft Direct Access Server, Hyper-V, Cloud Technology, Amazon Web Services

**Technologies/Protocols/Servers:**

* TCP/IP Protocol Suite [TCP/IP, TCP/UDP, HTTP/HTTPS, DNS/DHCP, SMTP/POP3], WAN Technologies [Internet, Ethernet (10/100/1000),
* Fast Ethernet, Gigabit Ethernet, Metro Ethernet, Fiber-Optics, Leased Lines, and T1], Layer 2 Technologies [Switches], Layer 3 Technologies
* [Routers, Switches VLAN, RIP, RIPv2, OSPF, BGP, EGP, IBGP], Internet Services (Servers) [Web, E-Mail, FTP, Proxy, E-Commerce, Streaming Media, File, Mobile Info].

**Management Tools:**

* Jira, Confluence, Splunk, Checkpoint Cloud Guard, Orca Security, Crowdstrike Falcon, Aikido Security, ServiceNow, Remedy, Slack, Sharepoint, Trello, Microsoft Teams, DAST, SAST, SCA, ASPM

**Operating Systems:**

* Cisco, IOS, Windows [10/8.1/7/Vista/XP/2003/2000/NT/ME/98/95/3.11/DOS], Android, Docker, AMI’s, Workstations: UNIX, Linux, Windows Server, Citrix Server (Xen-server, Xen-App and Xen-desktop)

**Applications Security Tools:**

* Fortify Security, Checkmarx Security, Snyk Security, Apigee API Security, Cloudflare Web Security, Gitlab Security, Github Security, Burpsuite, Veracode, Sonarcube, Qualys, Contrast Security, Noname Security, Mulesoft, HP Web Inspect, Nessus, Invicti Security, and Synopsys Center.

# Cloud Platforms:

* Oracle Cloud, Google Cloud, Amazon Web Services, Azure Cloud, Custom Machine Language Models

**Languages:**

* Scala, XML, C++, C#.Net, VB.Net, Java, J2EE, JSP, Blue coat CPL, ASP.NET, MVC4, Python, Golang, PHP, Java Script, and SQL.

**Self-Study Courses**

* Website Building & Development, Cloud Service (AWS) Microsoft Azure, Google Cloud, Network Security, Software Development,