Dillon T. Gonzalez

Atlanta, GA
678-713-6039 — dillon@dillongonzalez.com
www.linkedin.com/in/gonzaleztd — www.github.com/thepeachydill-talent

PROFESSIONAL SUMMARY

Senior Security Engineer focused on building scalable, automated security controls that neutralize complex threats at the script and registry levels. I specialize in deploying "Security-as-a-Service" models that integrate deep technical engineering with business continuity, recently achieving notable reductions in operational noise and manual labor. Proven at navigating high-stakes environments while maintaining alignment with global regulatory standards.

Security Engineer | City of Atlanta Dept. of Watershed Management | Nov. 2024 - Jul. 2025

- Led the implementation and integration of a privileged access management (PAM) solution for SCADA systems, enhancing critical infrastructure security across roughly 20 large enterprise environments and water treatment facilities, along with about 150 total vendors and external access users.
- Utilizing Azure and AWS, audited and corrected role based access controls (RBAC) for over 200 users within the city's water department, resulting in a 15% compliance with User Access Policy.
- Reduced organizational vulnerabilities by 30% across critical OT & IT infrastructure by designing and executing a comprehensive vulnerability management program that included prioritized patch management and threat modeling.
- Led a transition project from Forescout to Cisco Identity Services Engine to improve network access control and visibility across 2500+ endpoints, network appliances, and security monitoring tools.
- Aided in the integration and tuning of Microsoft Defender and SecureWorks TaegisXDR, increasing endpoint protection surface area by approximately 10%.

Cybersecurity Analyst | General Motors | Jul. 2022 - Aug. 2024

- Ensured compliance of over 30 internally developed applications with internal and NIST business continuity and disaster recovery policies and during use life and effective failover testing.
- Led cross-functional efforts to enhance compliance with SOX controls by 20%, addressing business continuity and unsanctioned software policies. This mitigation strategy effectively reduced organizational risk within a DevSecOps environment, employing PowerBI, Tenable Nessus, and ServiceNow GRC toolsets.
- Participated in SOX and CCPA data security audits, ensuring adherence to specific controls and corporate security policies pertaining to data retention, authentication, and access control.
- Led cross-functional efforts in executing vulnerability assessments and remediation strategies, resulting in a 15% reduction in organizational vulnerabilities.
- Led patch management efforts for about 50 retiring on-premises servers operating Oracle Linux and Oracle WebLogic middleware.

Technical Support Specialist | CloudPlus | Nov. 2019 – Jan. 2020

- Conducted rigorous quality control and compliance testing on proprietary platforms, ensuring
- adherence to industry standards and mitigating potential risks.
- Resolved over 400 customer support inquiries monthly, achieving a 10% increase in customer satisfaction through effective troubleshooting and problem-solving.
- Tooled and tuned proprietary platforms to ensure compatibility with Azure AD, GCP IAM, and Linux Access permissions tools.

Security Analyst Intern | Geographic Solutions | Feb. - May 2019

- Executed monthly system vulnerability assessments using Tenable, Qualys, and HP Fortify with 95% accuracy, identifying and remediating vulnerabilities to protect organizational assets.
- Collaborated with cross-functional stakeholders to ensure PCI-DSS, SOC II, and FedRAMP audit compliance, creating documentation and conducting controls and risk assessments.
- Aided in the creation of dashboards and security baselines and control environments, using McAfee SEIM, and later SentinelOne EDR tools for threat hunting and intelligence gathering.

PROJECTS

Palo Alto Firewall Deployment | City of Atlanta, Dept. of Watershed Management | Mar - July 2025

- Aided in the configuration of OT and IT next-generation and ruggedized firewalls with strict dynamic filtering for email, internal web traffic, and internet blocking for OT devices.
- Integrated Panorama into other security tools and software (Azure, MS Defender, Cisco ISE, MS Sentinel, etc) to test filtering compliance and increase network security visibility.

Dillon T. Gonzalez

Atlanta, GA
678-713-6039 — dillon@dillongonzalez.com
www.linkedin.com/in/gonzaleztd — www.github.com/thepeachydill-talent

TECHNICAL SKILLS
Automation & Scripting: Python, PowerShell, Bash, SQL
Cloud Platforms: Azure (Sentinel, Networking, Azure AD), AWS (Lambda, EC2), GCP (IAM, Compute)

Security Operations (SecOps):

- SIEM: Microsoft Sentinel, McAfee SIEM, Elastisearch, Splunk
- EDR: Microsoft Defender, SentinelOne, Taegis XDR
- IAM: Active Directory, Azure AD/Entra, PAM (CyberArk, PAM360), LDAP
- Cloud Security: Defender for Cloud, Wiz, Cisco Umbrella, Zscaler
- Network Security: Palo Alto Firewalls, Cisco ISE, VPNs, IDS/IPS, SASE concepts
- Vulnerability Management: Tenable Nessus, Qualys, Burp Suite,
- Compliance Frameworks: HIPAA, SOX, PCI-DSS, ISO 27001, NIST CSF, FedRAMP, CCPA, GDPR
- Blue Team: Continuous Monitoring,

System Administration (SysAdmin)
Server Management: macOS, Windows Server, Virtualization (VMWare ExSI, Horizons, etc)
Linux Administration: Kali/Parrot Linux, Wireshark, nmap,

CERTIFICATIONS: CySA+, Security+, Azure Security Engineering, AWS System Admin
EDUCATION: Bachelor of Science in Cybersecurity | St. Petersburg College