GRAYLON HAMPTON

Clearwater, FL | graylonhampton@gmail.com | 352-678-9207 | linkedin.com/in/graylonhampton

PROFESSIONAL SUMMARY

CISSP-certified Senior Security Engineer and U.S. Army wartime veteran with 20+ years of progressive experience across enterprise security operations, cloud security architecture, and program management. Currently building and operating the full-spectrum InfoSec program at InvestCloud — spanning cloud security posture, vulnerability management, Zero Trust network access, identity governance, endpoint protection, data security, and incident response. Proven ability to translate technical risk into executive decision frameworks, build security automation tooling, drive cross-functional remediation programs, and architect secure environments at enterprise scale. Active U.S. Secret Security Clearance.

CERTIFICATIONS & CLEARANCE

- **CISSP** — Certified Information Systems Security Professional (ISC^2)
- **Active U.S. Secret Security Clearance**

TECHNICAL COMPETENCIES

Cloud Security Posture & CNAPP/CSPM Cloud-Native Application Protection (Wiz), Cloud Security Posture Management, AWS Security Hub, Azure Defender for Cloud, multi-cloud risk governance

Vulnerability Management Agent-based and network scanning (Tenable.io, Nessus), SLA-driven remediation programs, risk prioritization, executive reporting

Identity & Access Management / PAM Identity Governance & Administration (Microsoft Entra ID), Conditional Access policy, Privileged Access Management (Delinea, CyberArk), AWS IAM, MFA governance, ITDR

Zero Trust Network Access (ZTNA) / SASE / SSE Zero Trust Architecture (ZTA), Secure Service Edge (Cato Networks), Secure Web Gateway, network segmentation

Network Access Control (NAC) & Enterprise Networking Identity-Based Network Access Control (Cisco ISE), Network Management (Cisco DNA Center, Meraki), RADIUS, micro-segmentation

Endpoint Detection & Response (EDR/XDR) Endpoint & Server Protection (Microsoft Defender for Endpoint), managed device compliance, threat response

SIEM & Managed Detection & Response (MDR) Log Management & Detection Engineering (Splunk), Managed Detection & Response (Expel.io), alert tuning, incident triage & investigation

Data Loss Prevention (DLP) & Data Security Enterprise DLP (Microsoft Purview), M365 compliance, data classification, sensitive data governance

Web Application & Edge Security WAF, DNS Security, and Edge Controls (Cloudflare)

Security Automation & DevSecOps Python scripting, GitLab CI/CD, Ansible, Git — custom security tooling, workflow automation, data pipeline development

Compliance & Governance Frameworks NIST 800-53, PCI DSS 4.0, SOC 2 Type 2, Zero Trust Architecture (ZTA), MITRE ATT&CK

Cloud Platforms Amazon Web Services (AWS), Microsoft Azure

EXPERIENCE

SENIOR SECURITY ENGINEER, INFOSEC OPERATIONS — INVESTCLOUD INC.

September 2024 – Present

InvestCloud is a global fintech platform serving the wealth management industry, operating a hybrid multi-cloud infrastructure across AWS and Azure.

- Own the enterprise **Cloud-Native Application Protection (CNAPP/CSPM)** program using Wiz, including cloud posture management, vulnerability prioritization, and risk-based remediation governance across AWS and Azure environments.
- Operate the enterprise **Vulnerability Management** program end-to-end (Tenable.io) with SLA-driven remediation workflows spanning cloud, hybrid, and on-prem infrastructure; produce weekly executive risk reports translating posture data into leadership-level decisions.
- Architected and deployed **Zero Trust Network Access (ZTNA) and Secure Service Edge (SSE)** (Cato Networks) replacing legacy VPN infrastructure — implementing Zero Trust access controls and Secure Web Gateway enforcement for a globally distributed workforce.
- Built a **Python-based security automation toolkit** to streamline vulnerability reporting, asset tagging, risk metrics, and recurring operational workflows — reducing manual effort and improving data consistency across security deliverables.
- Lead **Privileged Access Management (PAM)** governance (Delinea) across cloud and on-prem environments, enforcing least-privilege, just-in-time provisioning, and privileged session accountability.
- Administer **Endpoint Detection & Response (EDR/XDR)** (Microsoft Defender for Endpoint) across hybrid endpoints and cloud-hosted servers, including threat response, policy governance, and managed device compliance.
- Govern **Identity & Access Management** (Microsoft Entra ID) including Conditional Access policy, managed device enforcement, and identity risk reduction across the enterprise.
- Oversee **Data Loss Prevention (DLP)** (Microsoft Purview) protecting sensitive financial and client data across M365 environments.
- Serve as primary escalation contact for incident triage and response in partnership with **Managed Detection & Response (MDR)** provider Expel.io.
- Maintain **SIEM** environment (Splunk) including detection engineering, alert tuning, and log pipeline oversight.
- Author and own the security operations playbook library in Confluence, documenting incident response procedures, runbooks, and SOPs across all security domains.

SECURITY ANALYST, INFOSEC OPERATIONS — INVESTCLOUD INC.

May 2022 – September 2024

- Led enterprise **Vulnerability Management** operations (Tenable.io), building SLA-driven remediation workflows and driving accountability across engineering and infrastructure teams.
- Managed enterprise **password vault migration**, standardizing access management practices and improving credential governance across the organization.
- Administered and enhanced **Privileged Access Management (PAM)** configurations (CyberArk) to strengthen privileged access governance across client-facing environments.

PLATFORM SUPPORT ENGINEER — INVESTCLOUD INC.

September 2021 – May 2022

- Maintained AWS EC2 environments, **Web Application Firewall and Edge Security** (Cloudflare), DNS, and NGINX web platforms serving global clients.
- Automated infrastructure deployments and configuration management using GitLab CI/CD, Jenkins, and Ansible.

CO-FOUNDER & CO-OWNER — CLOUDAMROY LLC

February 2024 – 2026 | Ownership acquired, 2026

Co-founded a Managed Service Provider (MSP) delivering full-spectrum IT and cloud security solutions exclusively to fintech clients on AWS infrastructure.

- Co-owned and managed the full IT stack for fintech clients — cloud infrastructure, security architecture, IAM, networking, and compliance — with end-to-end accountability across all service domains.
- Led **PCI DSS 4.0** compliance programs for clients two consecutive years, executing gap assessments, controls implementation, and audit readiness across all twelve PCI requirements.
- Achieved **SOC 2 Type 2** certification for clients through risk analysis, controls design, evidence collection, and independent audit coordination.
- Architected and governed multi-tenant **AWS** environments including IAM policy frameworks, network security controls, logging, and cloud governance standards aligned to financial services requirements.

NETWORK TECHNICAL ANALYST III — PASCO COUNTY BOARD OF COUNTY COMMISSIONERS

January 2019 – September 2021

- Deployed **Network Access Control (NAC)** and identity-based segmentation (Cisco ISE, DNA Center) implementing RADIUS authentication and micro-segmentation across county infrastructure.
- Managed enterprise wireless (Cisco Meraki) rollout to 50+ locations with centralized policy enforcement.
- Maintained Multi-Factor Authentication (Duo), firewall policy, and VPN infrastructure for government operations.

TECHNICAL TEAM LEAD / SYSTEMS ADMINISTRATOR — KFORCE INC.

March 2017 – April 2019

- Led a four-person infrastructure support team; redesigned incident response protocols and mentored junior engineers.

- Administered Exchange, Active Directory, and end-user systems infrastructure across enterprise teams.

EARLY MSP CAREER — METRO TECH / VOLOGY

February 2015 – August 2016 | Field Service Engineer & Service Desk Technician

- Delivered engineering support for 100+ SMB and municipal clients across VMware, Citrix, Windows Server, and Exchange environments; managed backup and recovery systems (Datto) and conducted weekly security audits.

MILITARY SERVICE

NETWORK SYSTEMS OPERATOR — UNITED STATES ARMY (RESERVE)

November 2003 – 2024 | Wartime Veteran, Operation Iraqi Freedom

- Served 20+ years as a Reserve Network Systems Operator alongside a full civilian career in IT and cybersecurity.
- **Combat Deployment (2008–2009):** Activated for active-duty service in support of Operation Iraqi Freedom; served as **Night Shift Supervisor for the theater-wide communications network spanning Iraq and Kuwait** — accountable for satellite communications, tactical networking, and signal infrastructure sustaining mission-critical military operations around the clock.
- Led signal platoon operations at the **brigade level** as acting Platoon Sergeant, overseeing personnel readiness, equipment accountability, and OPSEC enforcement.
- Trained and mentored junior soldiers on communications security, tactical networking protocols, and mission-essential signal operations.