Matthew Bowman

matthewjaybowman@gmail.com | 512-507-1349 | Austin, TX — relocating to NYC, available in-office

SENIOR INCIDENT RESPONSE ENGINEER · Cloud & Endpoint Security · SentinelOne EDR · Multi-Cloud · Python/Bash

PROFESSIONAL SUMMARY

Hands-on incident responder and cloud security engineer, 15+ years across security, multi-cloud, and endpoint operations. Operated SentinelOne EDR across 100+ client environments — triaging behavioral detections, isolating compromised endpoints, and remediating to clean state. Resolve production failures at the Kubernetes/container layer under pressure and harden posture across AWS/GCP/Azure. Deep operator experience in gaming/media (Certain Affinity, Cerberus, EA, Sony Music) — the environment Rockstar defends. CompTIA Security+ / Network+; former Confidential clearance (VA); strong Python/Bash/PowerShell for log analysis, detection, and response.

CORE COMPETENCIES

Security Operations & IR: SentinelOne (EDR), incident triage & remediation, endpoint threat response, malware detection & endpoint isolation, log correlation & parsing, telemetry & anomaly analysis, security audits, vulnerability & patch management, IAM (AWS / GCP / Azure), PKI, access reviews, security-policy enforcement · exposure: Carbon Black, Wiz.io, Rapid7 IDR, Lacework

Detection, Logging & Observability: Prometheus, Grafana, Datadog, Stackdriver (GCP), Nagios, centralized logging & alerting pipelines, anomaly & degradation detection, dashboards & runbooks

Cloud & Distributed Systems: AWS (EC2, S3, Lambda, IAM), GCP (GKE, IAM, Cloud Functions, Billing), Azure (AD, AKS, DevOps), Kubernetes, Docker, Helm, Rancher, HashiCorp Nomad, Terraform, Terragrunt, Ansible, CloudFlare

Scripting & Automation: Python (Flask, PyTest, log parsing, automation), Bash, PowerShell, Go, PKL, MySQL / PostgreSQL / MongoDB, Git (GitHub, GitLab), Jenkins, GitLab CI/CD, Spinnaker

PROFESSIONAL EXPERIENCE

Redapt (contracted to Apple) | Remote | Aug 2024 – Present

Senior Cloud Architect — Dev-to-Production Team

- Lead infrastructure migration of a payment-compliant (PCI-relevant) application from on-prem data centers to AWS, enforcing security and regulatory controls and validating production readiness across environments.
- Diagnose and resolve 2–4 production incidents per sprint at the container and network layer — root-cause analysis across HashiCorp Nomad pod failures and container-networking breakdowns, restoring service availability under deadline pressure.
- Perform host-level configuration and posture analysis across PCI-relevant environments — correlating configuration drift, network-policy gaps, and deployment-state discrepancies to identify misconfigurations that introduce security exposure.
- Design and operate monitoring and alerting pipelines (Grafana, Prometheus, in-house telemetry) to reduce detection latency for service degradation and anomalous behavior.
- Partner with DevOps and security teams to phase out legacy deployment surfaces and reduce attack surface across cloud accounts; standardize infrastructure as code (Terragrunt, Go, Python, PKL) across 8+ discrete tasks per 1–2 day deployment.
- As team lead, close assigned issues faster than any engineer on the team and unblock stuck teammates ~3×/week (more during deployments); provide incident triage and escalation support during critical events and mentor cloud architects.

Certain Affinity | Austin, TX | Feb 2020 – Apr 2024

IT Cloud Systems Architect — AAA game studio (Halo, Call of Duty co-development)

- Designed and operated Kubernetes-backed game backend services (Halo / Call of Duty co-development) across AWS, GCP, and Azure — fault isolation, live-service stabilization, and post-deployment recovery under production load.
- Built centralized monitoring and alerting (Datadog, Prometheus) enabling early detection of service anomalies and performance-degradation events.

- Conducted cloud configuration reviews and security hardening across multi-cloud environments, improving baseline posture and reducing exposure; automated provisioning with Terraform/Ansible to cut manual-misconfiguration incidents.

Kony, Inc. | Austin, TX | Jul 2018 – Nov 2019

Senior Systems Administrator

- Administered Azure Active Directory and critical intranet applications, managing identity and access for global users.
- Built infrastructure monitoring with Nagios and managed AKS workloads with Spinnaker/Jenkins pipelines and rollback strategies to mitigate deployment-related incidents.
- Hardened system security through next-gen AV deployment and recurring security audits across managed systems.

Cerberus Interactive, Inc. | Austin, TX | Nov 2017 – Jul 2018

Development & Operations Engineer — game production backends

- Stood up Kubernetes clusters across AWS, GCP, and Azure for game production backends, emphasizing resilience, observability, and fault tolerance under load.
- Deployed Prometheus monitoring to detect cluster-health anomalies and service-degradation patterns; automated provisioning/recovery with Terraform to cut time-to-restore, supporting live production troubleshooting in an Agile environment.

Innovative Computing Systems (MSP) | Austin, TX | Feb 2016 – Apr 2017

Remote Monitoring & Management / Security Administrator

- Operated endpoint detection & response (SentinelOne) across 100+ client environments — first responder to behavioral detections, malware, and endpoint intrusion attempts.
- Triaged high-severity security detections in the SentinelOne console, isolated compromised endpoints (network quarantine), enriched indicators via VirusTotal hash/reputation lookups, and remediated confirmed threats to clean state.
- Established baseline security posture for every new client at onboarding (EDR enrollment, patch policy, access controls), closing exposure windows from day one.
- Administered patch management (WSUS) across a diverse client base to reduce vulnerability exposure, troubleshot escalated infrastructure incidents across AWS, Citrix, and on-prem/vSphere, and authored PowerShell/MySQL automation to extend monitoring coverage.

Evolve IP | Austin, TX | Apr 2015 – Oct 2016

Service Desk / RMM Administrator

- Provided 24/7 monitoring and after-hours on-call response for 100+ companies' servers and workstations; top-performing helpdesk engineer by daily ticket resolution and coordinated patch management to minimize disruption.

Financial Services Center — U.S. Department of Veterans Affairs | Austin, TX | Oct 2009 – Jul 2012

Lead IT Specialist — Confidential Clearance

- Investigated and documented security-policy violations in coordination with ISO/TSO to safeguard network integrity across nationwide VA federal systems.
- Conducted quarterly access reviews under ISO/TSO guidance, enforcing least-privilege access levels and maintaining compliance across systems.
- Installed and maintained Public Key Infrastructure (PKI) for secure email per VA standards; used SCCM for patch management and remediation, improving security and compliance posture.

EARLIER EXPERIENCE

Electronic Arts — Game Advisor, gaming/media (2014–2015) · Sony Music Entertainment, NYC — Help Desk, 2,000+ users incl. WAN security reviews (2006–2009) · TBG Partners (2012–2013) · Underground Computer Technologies (2004–2006) · Multek/IBM (2002–2004) · Dell Inc. (2000–2002).

CERTIFICATIONS, CLEARANCE & EDUCATION

Certifications: CompTIA Security+ (2016) · CompTIA Network+ (2015) · Confidential Clearance — U.S. Dept. of Veterans Affairs (2009–2012) · ConnectWise Automate Certified Expert (2017) · Jamf 200 (2022)

Education: The New School University — New York, NY (2007–2009) · CNCF KubeCon (2019, 2021)