BRYAN D. SWAINSTON

Director of Information Security | Cybersecurity Architect

West Olive, MI · 616.401.2674 · bryandswainston@gmail.com

GSEC GDSA

PROFESSIONAL SUMMARY

Cybersecurity Architect and sole owner of the full security function at SoundOff Signal — a 600-employee, employee-owned manufacturer of emergency warning equipment serving law enforcement, fire, and EMS customers with CMMC Level 2 and government/public-safety contract obligations. Built the security program from zero: designed governance, stood up SOC operations, implemented vulnerability management, established phishing triage workflows, and delivered executive-facing risk infrastructure across a converged corporate IT and manufacturing OT environment — breadth that would typically span a 4–6 person security team. Equally at home in architecture, hands-on detection engineering, and executive communication: built automation pipelines, authored XQL threat-hunt playbooks, drove multi-vendor platform decisions, and translated complex risk posture into board-level briefings. GIAC-certified (GSEC, GDSA) with operational depth in NIST CSF 2.0, CMMC, PCI-DSS, and cloud/AI security controls across Palo Alto, Microsoft, and ManageEngine stacks.

CORE COMPETENCIES

FW	**Frameworks & Compliance**	NIST CSF 2.0 · CMMC Level 2 · PCI-DSS · ITIL 4 · COBIT 2019
GV	**Governance & Risk**	Risk Register Design · Third-Party Risk (TPRM) · Executive Risk Reporting · Security Budget & Vendor Strategy · Policy Authoring · eDiscovery / Legal Hold
SO	**Security Operations**	Cortex XSIAM · AI-Driven SOC · Incident Response · XQL Threat Hunting · Check Point Email Gateway · Phishing Triage (PhishER · KnowBe4) · Security Awareness
CI	**Cloud & Identity**	Microsoft Azure · Microsoft Defender · Azure Front Door · Azure Logic Apps · CASB · AI/SaaS Governance · Entra ID · Conditional Access
VE	**Vulnerability & Endpoint**	ManageEngine Endpoint Central · Vulnerability Manager Plus · CISA KEV Automation · Automated Patch Management
NI	**Network & Infrastructure**	Palo Alto NGFW · Prisma Access · Network Segmentation · IT/OT Boundary Security · Active Directory
AU	**Automation & Integration**	Azure Logic Apps · Atlassian Assets (AQL) · Jira API · SharePoint REST · Static Site Architecture (Astro · Bun)

PROFESSIONAL EXPERIENCE

SoundOff Signal · Hudsonville, MI

Cybersecurity Architect — 2024 – Present

First and only dedicated security hire; sole owner of security strategy, architecture, GRC, and operations for a global manufacturer of life-safety equipment with government and public-safety customer obligations.

- Aligned the full security control set to NIST CSF 2.0 and scaled the policy library from a single document to 12+ ratified policies — Incident Response, Secure Development, IT Operating Model, Acceptable Use, and more — establishing governance across IT and OT operations.
- Leading the CMMC Level 2 readiness roadmap as sole owner: sequencing controls, evidence collection, and remediation to secure DoD-adjacent contract eligibility for the business.
- Deployed Cortex XSIAM as the consolidated SOC platform with AI-driven detection across endpoint, network, and identity telemetry; concurrently decommissioning Arctic Wolf MDR, eliminating redundant vendor spend and consolidating the security toolchain.
- Designed a 4-tab / 17-widget GlobalProtect usage dashboard in XSIAM covering executive adoption KPIs, connection activity, compliance/HIP enforcement, and auth anomalies including geo-impossible travel and brute-force thresholds.
- Implemented CASB-led AI/SaaS governance via Palo Alto Strata Cloud Manager with tenant-scoped DLP, enabling sanctioned-vs-unsanctioned GenAI controls (including scoped Claude tenant policies) while maintaining audit-grade compliance documentation.
- Operate the daily phishing triage workflow (PhishER → header/URL/payload analysis → verdict → reporter notification → block/quarantine in Check Point and XSIAM); identified and documented an Adobe Sign envelope phishing TTP exploiting legitimate authenticated infrastructure and developed a detection tripwire concept matching envelopes against known AP vendor records.
- Designed and built the enterprise Vulnerability Management program from scratch: led ManageEngine Endpoint Central VMP deployment, authored emergency zero-day patch procedures with pre-deployment process-kill scripting, and produced a scanner platform analysis (Tenable, Rapid7, Qualys, Greenbone evaluated) that redirected ~$20K/year toward higher-impact OT visibility.
- Built an automated CISA KEV → Atlassian Assets → Jira pipeline using Azure Logic Apps and AQL; performs fuzzy product-to-asset matching, deduplication, and confidence scoring before creating RISK ideas in Jira — closing a NIST CSF Detect-to-Respond automation gap without additional headcount.
- Transformed a 116-entry risk backlog into a governed Risk Register with four-tier scoring, seven-state workflow, NIST CSF 2.0 function mapping, and four documented treatment paths; surfaced four T1 Critical risks (legal hold, RADIUS, Kerberos, PIM permanent-active roles) requiring immediate ownership and identified 15 risks lacking assigned owners.
- Architected Azure Front Door Premium fronting the customer-facing marketing site: managed WAF, bot management, Azure-managed TLS, origin lockdown via Service Tag restriction, and XSIAM log ingestion via Event Hub — eliminating the external attack surface while establishing audit-grade visibility.
- Conducted threat-hunting investigations using XQL across developer endpoints and production network traffic; identified privileged domain credentials (Manufacturing, ups) in active use on the manufacturing network during an RC4-deprecation engagement — an OT credential exposure escalated beyond the original project scope.
- Led security input on the VMware-to-hypervisor replatform decision; produced a head-to-head analysis (Scale Computing vs. Azure Local vs. VMware) covering OT air-gap requirements, Cortex XDR continuity, Veeam immutable backup integrity, and CMMC documentation impact; delivered a split corp-IT-vs-OT recommendation adopted by leadership.
- Authored an executive-facing analysis of enterprise AI architecture — custom LLM vs. fine-tuning vs. Azure OpenAI + RAG — framing the decision in cost, security, CMMC compliance, and time-to-value terms; built and delivered an 11-slide AI primer to leadership covering vocabulary, risk posture, and sanctioned use cases.
- Re-architected legacy Stablehost-hosted marketing sites onto a hardened static-site stack (Astro, Bun, Azure Static Web Apps), eliminating an entire class of CMS-borne vulnerabilities while reducing operational overhead.

- Stood up a formal TPRM program and PCI-DSS compliance workflows; serve as the executive security advisor, translating risk posture into business-language briefings for senior leadership and owning end-to-end accountability for the security budget and vendor strategy.

Network Security Engineer
2022 – 2024

Hired as the company's first dedicated security resource; stabilized the environment and built the foundation that enabled the Architect program.

- Identified and remediated critical firewall misconfigurations and legacy technical debt within the first weeks on the job, materially reducing the external attack surface before any formal security program existed.
- Established baseline security controls across identity, endpoint, and network; authored the organization's first formal security policies in partnership with IT, HR, and executive leadership.
- Bridged IT and OT security concerns for the manufacturing floor, where equipment downtime directly impacts production of life-safety emergency vehicle systems.

Progressive Leasing · Draper, UT

Security Engineer
2020 – 2022

- Administered and tuned endpoint security platforms, firewall policy, and identity controls across the enterprise fleet; drove security hardening initiatives and responded to escalated incidents as the team's dedicated security resource.
- Managed MFA enforcement, conditional access policies, and privileged access controls organization-wide; ensured remote access security posture across a distributed workforce.

Information Security Analyst
2018 – 2020

- Monitored security event logs and alerts, triaged incidents, and coordinated remediation across IT and endpoint teams; built foundational threat-detection and response processes.
- Delivered security awareness training to analysts and end users; authored knowledge base documentation and ran patch-readiness diagnostics across 200+ endpoints.

Service Desk Analyst
2016 – 2018

- Resolved enterprise endpoint, identity, LAN/WAN, and VPN issues organization-wide; managed BitLocker/TPM deployment and enforced MFA-protected remote access across the fleet.

EARLIER EXPERIENCE

G4S Secure Solutions — Custom Security Specialist
Salt Lake City, UT · 2015–2016 · Managed physical access control systems (Kantech), reviewed daily access logs, and conducted inspections of restricted areas.

United States Marine Corps — Infantry Section Leader / Sergeant (E5)
29 Palms, CA · 2009–2014 · Led up to 100 Marines across multiple Afghanistan deployments; promoted to Sergeant in 3.5 years. Certificate of Commendation for leadership under direct fire.

CERTIFICATIONS

GIAC Security Essentials (GSEC)
SANS-validated breadth across modern defensive security operations.

GIAC Defensible Security Architecture (GDSA)
SANS-validated expertise in designing layered, resilient, and adversary-aware security architectures.