

Supercharge Your SIEM™

CYBRILL Capability Statement

Company Data

SBA-Certified SDVOSB

UEI: WH1FYVLXFJG5

CAGE: 8K0G0

Alexander Brill, Owner

alex@cybrill.io

www.cybrill.io

(772) 202-2788

2054 Vista Parkway, Suite 400,
West Palm Beach, Florida 33411



NAICS

Primary: 541519 Other Computer
Related Services

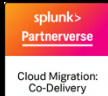
Supporting: 541511, 541512; 541519;
541611; 541618; 541690; 541990;
611430

Key Talent

SIEM Engineer, Detection Engineer,
SecDevOps Engineer, SOC Analyst,
SOC Manager, Incident Responder,
Threat Hunter, Compliance Engineer,
Vulnerability Analyst & more

Tech Expertise

Splunk, Microsoft Sentinel, Cribl,
CrowdStrike, Zscaler, Qualys, Palo Alto
Networks, Tenable, Devo, Elastic,
Cisco & more



Supercharging SIEM™

CYBRILL is a cybersecurity services firm specializing in Security Information and Event Management (SIEM) and SOC support. We serve leading U.S. MSSPs, government agencies, and commercial enterprises with hands-on engineering and elite augmentation talent.

Our deep bench of highly experienced engineers — including U.S. citizens with government clearances — has supported 150+ Fortune 2000 and public sector environments. We deliver tool-agnostic solutions that enhance threat detection, restore SIEM fidelity, and accelerate response.



SIEM Firefighter

Rapidly stabilize
underperforming
SIEMs, restore full
data fidelity, and
get environments
back to green



SIEM Test & Eval

Validate the health,
resilience, and
maturity of SIEM
deployments for
security,
architecture, and
compliance



SIEM Consulting Services

Design and
implement scalable,
secure, and efficient
SIEM and SOAR
architectures
tailored to each
environment



SIEM Expert Services

Push the
boundaries of SIEM
with expert-led
detection,
investigations, and
visionary use cases

Differentiators – Why CYBRILL?

- Elite SIEM & SOC expertise
- Certified, U.S. citizen engineers with government clearances
- Trusted force multiplier to top U.S. MSSPs
- Direct access to hands-on SIEM engineering
- Proven success across 150+ government and enterprise environments





Example Past Performance

- Agencies served: **DHS, DoD, DOE, DOJ, IRS, State OIG, FRTIB** & others
- Federal MSSP (Shared Services)
 - Full SIEM lifecycle for 15+ federal agencies
 - Centralized logging, detection engineering, M-21-31 compliance
- Statewide MSSP (Custom RBAC)
 - Deployed Splunk ES + custom RBAC for 50+ sub-agencies
 - Enabled secure access and cross-agency visibility
- Commercial, Banking industry
 - Built new fraud detection in Splunk for regional bank
 - MDR support across onboarding, detection tuning, and platform ops

CYBRILL Core Capabilities

Supercharging SIEM™

Hands-on engineering. Mission-ready, high-impact talent. CYBRILL helps MSSPs, agencies, and enterprises strengthen threat detection, restore SIEM performance, and scale fast — without vendor lock-in or added overhead.

 SIEM Firefighter Rapidly stabilize underperforming SIEMs, restore full data fidelity, and get environments back to green	 SIEM Test & Evaluation Validate the health, resilience, and maturity of SIEM deployments for security, architecture, and compliance	 SIEM Consulting Services Design and implement scalable, secure, and efficient SIEM and SOAR architectures tailored to each environment	 SIEM Expert Services Push the boundaries of SIEM with expert-led detection, investigations, and visionary use cases
<ul style="list-style-type: none">• Triage broken ingest pipelines (e.g., EDR, IAM, firewalls, cloud, and endpoint logs)• Restore fidelity through field extraction, parsing, and normalization• Tune detection logic to reduce false positives and enhance signal-to-noise ratio• Identify root causes of performance degradation and data loss• Optimize pipeline throughput using Cribl and native SIEM tuning tools• Provide same-day remote triage and short-notice surge support	<ul style="list-style-type: none">• Run the CYBRILL SIEM Health Check™ to assess coverage, content, correlation, and configuration• Map posture against Zero Trust architecture, EO 14028, and M-21-31 guidance• Simulate ransomware, phishing, and insider threat scenarios to expose detection gaps• Conduct purple teaming engagements and advanced detection evaluations• Deliver remediation plans to improve detection, correlation, and alerting outcomes	<ul style="list-style-type: none">• Deploy and optimize Splunk, Microsoft Sentinel, Elastic, Devo, and other SIEM tools across cloud and hybrid• Design and implement Zero Trust architectures aligned with EO 14028, OMB M-22-09, and CISA ZTMM guidance• Build DevSecOps-integrated logging pipelines and automation frameworks• Engineer secure multitenant architectures, RBAC policies, and access controls• Implement co-managed SOC models and provide transition support	<ul style="list-style-type: none">• Design and deliver “art of the possible” use cases that stretch SIEM capabilities beyond the standard playbook• Conduct proactive threat hunting and forensic investigations• Build advanced detection rules, correlation searches, and executive dashboards• Support RFPs, technical solutioning, and competitive evaluations of security tools• Integrate third-party tools and develop custom apps, alerts, and analytics• Bridge red and blue team insights into continuously improving detection logic
Trusted MSSP Surge Partner Trusted by top U.S. MSSPs for urgent delivery, overflow engineering, and SIEM performance recovery <ul style="list-style-type: none">• Deploy cleared engineers during client onboarding, migration, or incident escalation• Resolve data loss, alert fatigue, and correlation misconfigurations• Strengthen client retention by tuning underperforming SIEM environments• Deliver expert services under white-label or augmentation models• Act as a force multiplier with no channel conflict — accelerating MSSP performance			