Sterling Brooks Lead Security Engineer

Falls Church, VA · sterling.brooks@gmail.com · +1 703-555-0152 · linkedin.com/in/sterlingbrooks

PROFILE SUMMARY

- **Lead Security Engineer** with **12 years** of experience securing **defense and federal networks** at a **Fortune 500 defense contractor** and a **federal IT services firm**, specializing in **CUI enclaves, smart-card identity and network segmentation**.
- Hands-on with **Microsoft Entra ID** and **CyberArk** for identity, **Palo Alto Networks** for segmentation, **Splunk** for detection, **Tenable.sc** for scanning, Thales Luna HSMs for PKI, and **PowerShell** and **Python** for automation.
- Deep expertise in **security architecture for regulated enclaves**, **PIV and CAC authentication**, **deny-by-default segmentation** and **FIPS-validated encryption**, building each control to **NIST SP 800-171** and **CMMC Level 2**.
- Works with **program security**, **IT operations**, the **SOC** and the **ISSM office**, and sits on the **security architecture review board** that approves changes to controlled environments.
- Leads a **team of 6 security engineers**, runs their hiring loops and on-call rotation, and holds the **CISSP** and an active **Secret clearance**.

TECHNICAL SKILLS

Identity & SSO:	Microsoft Entra ID, Active Directory, CyberArk, PIV and CAC smart cards, Conditional Access, SAML 2.0
Vulnerability Scanning:	Tenable.sc (ACAS), Tenable Nessus, CVSS, CISA KEV, DISA STIG Viewer
Endpoint & MDM:	Microsoft Defender for Endpoint, Microsoft Intune, Group Policy, DISA STIGs, BitLocker
Firewalls & ZTNA:	Palo Alto Networks, Panorama, Cisco ISE, 802.1X, network segmentation
SIEM & Detection:	Splunk Enterprise Security, Microsoft Sentinel, MITRE ATT&CK, SPL, KQL
Cloud & Secrets:	Microsoft Azure Government, Thales Luna HSM, Microsoft AD CS, HashiCorp Vault
Languages, Automation & Frameworks:	PowerShell, Python, Ansible, NIST SP 800-171, CMMC Level 2, NIST SP 800-53

EDUCATION

George Mason University — M.S. in Cyber Security Engineering — Fairfax, VA · Sep 2012 to May 2014

ISC2 — CISSP — Fairfax, VA · Jun 2017

WORK EXPERIENCE

Northrop Grumman — Lead Security Engineer — Falls Church, VA · May 2021 to Present

- Lead a team of 6 security engineers and review about **25 system designs a quarter** on the security architecture review board before any change reaches a CUI enclave.
- Moved **4,200 enclave users** from passwords to PIV and CAC smart-card login with Microsoft Entra ID certificate-based authentication, and put 1,350 admin accounts behind CyberArk just-in-time access.
- Split a flat enclave network into 11 segments on **Palo Alto Networks** firewalls with deny-by-default rules, cutting the systems a standard workstation can reach from **2,600 to 140**.
- Moved the internal certificate authority onto FIPS-validated hardware security modules and reissued **8,000 device and server certificates** over 5 months with no outages.
- Brought enclave logs into **Splunk** and wrote **120 detections** mapped to MITRE ATT&CK with the SOC, covering the audit logging controls in NIST SP 800-171.

General Dynamics Information Technology — Senior Security Engineer — Fairfax, VA · Jul 2014 to Apr 2021

- Ran **Tenable.sc** (ACAS) scanning for 8,500 endpoints on 2 civilian agency contracts, and cut the open critical backlog from **580 to 74**.
- Applied DISA STIGs to 2,200 Windows and RHEL servers with Group Policy and Ansible, raising STIG compliance scores from **68% to 95%**.
- Wrote **PowerShell** and Python scripts that build the monthly POA&M report straight from scan data, cutting the work from **5 days to 1** on each contract.