NSA PROTECTIVE DOMAIN NAME SYSTEM SERVICES

DRIVE DOWN RISK | PROTECT DOD INFORMATION

NSA’s Cybersecurity Collaboration Center provides no-cost Protective Domain Name System (PDNS) services, infused with NSA’s unique threat intel, to protect critical Department of Defense (DOD) information held on Defense Industrial Base (DIB) company systems.

DNS IS THE BACKBONE OF THE INTERNET.

Due to its pervasiveness, DNS queries are frequently hijacked to implant malware and gain initial access to sensitive systems. Small-to-medium sized DIB contractors are especially vulnerable to this technique. PDNS services reduce risk of compromise by seamlessly protecting users from connecting to known malicious websites.

NSA’S PDNS PILOT PROGRAM BLOCKED MORE THAN 16M DOMAIN RESOLUTIONS, including known nation-state spear-phishing, botnets and malware.

NSA is now scaling this service to qualifying contractors.

This service leverages Akamai GovShield architecture.

To learn more about qualifying for this service, email DIB_DEFENSE@cyber.nsa.gov

cybercenter.nsa.gov

@NSACyber
NSA VULNERABILITY SCANNING SERVICE

GAIN AN ADVERSARIAL VIEW OF YOUR NETWORK, FIND ISSUES BEFORE THEY DO.

NSA’s Cybersecurity Collaboration Center provides no-cost Vulnerability Scanning services to protect critical Department of Defense information held on Defense Industrial Base (DIB) company systems.

SUCCESS

NSA’s vulnerability scanning service has detected thousands of vulnerabilities on DIB networks and worked with network defenders to implement mitigations before they became compromises.

Vulnerability scanning is critical to protect DIB networks and sensitive data from compromise as unpatched services are often used by threat actors to gain initial access. NSA’s Vulnerability Scanning Service leverages commercial asset discovery and vulnerability assessment services, combined with in house analytic expertise, to discover vulnerabilities and provide mitigation guidance for internet-facing DIB assets.

To learn more about qualifying for this service, email DIB_DEFENSE@cyber.nsa.gov
NSA THREAT INTELLIGENCE COLLABORATION

NSA’s Cybersecurity Collaboration Center provides no-cost Threat Intelligence Collaboration services to protect critical Department of Defense information held on Defense Industrial Base (DIB) company systems.

STAY ONE STEP AHEAD OF THE ADVERSARY.

SUCCESS

NSA has helped harden over a billion endpoints around the world by sharing its unique insights into malicious nation-state and cyber-criminal activities with DIB network defenders.

Threat Intelligence Collaboration gives network defenders insight into Advanced Persistent Threat actor’s Tactics, Techniques, and Procedures. Through NSA’s Cybersecurity Collaboration Center, DIB partners collaborate with NSAs analysts via secure commercial collaboration platforms to increase timely threat intelligence exchange. Partners receive:

- Contextualized distribution of NSA cybersecurity advisories
- Prioritized sharing of indicators of compromise for DIB relevant Advanced Persistent Threat activity
- Collaboration with NSA analysts on findings and tailored mitigation guidance

To learn more about qualifying for this service, email DIB_DEFENSE@cyber.nsa.gov

cybercenter.nsa.gov @NSACyber