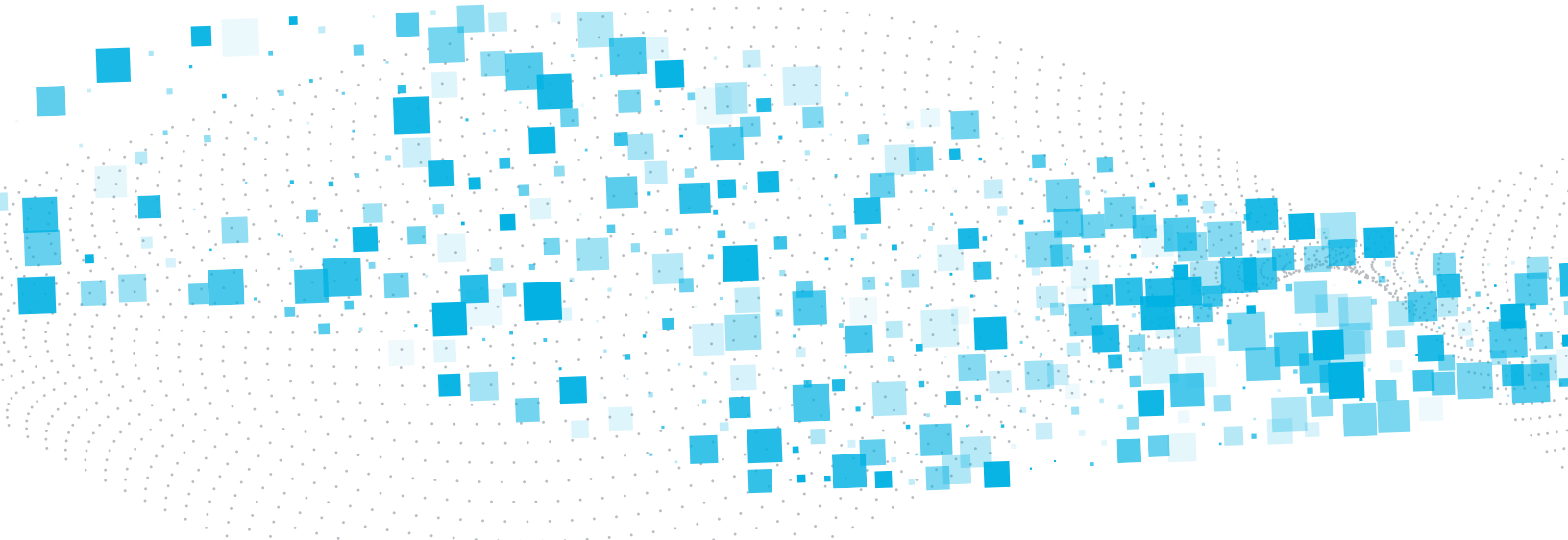
SOLUTION BRIEF

Supporting Cyber Protection Teams



On Oct. 24, 2016, U.S. Cyber Command (Cybercom) announced that all 133 of its Cyber Mission Force teams achieved initial operating capability. By the end of fiscal year 2018, the goal is for the Cyber Mission Force to grow to nearly 6,200 and for all 133 teams to be fully operational.

Cybercom's Cyber Mission Force teams align with the DoD Cyber Strategy's three primary missions: defend DoD networks and ensure data is secure; support joint military commander objectives; and, when directed, defend U.S. critical infrastructure.

As a recent live cyber exercise illustrated, the Cyber Protection Teams' (CPTs) first priorities are to validate the network map and to identify key terrain and critical assets. This process is made more difficult by the limited number of people with existing network knowledge. Using software as a force multiplier is the solution, so building and mastering a toolkit of proven, powerful cyber tools is one of the key measures of a fully operational CPT.

RedSeal: The Must Have Tool for CPTs

RedSeal understands and improves the resilience of every element, segment, and enclave of your network, enabling CPTs to carry out their missions. RedSeal works with your existing security stack and network infrastructure (including cloud and SDN) to automatically and continuously visualize a logical model of your "as-built" network.

RedSeal's network modeling and risk scoring platform is designed to enable CPTs to act with speed and efficiency. Visualizing end-to-end access—intended and unintended—between any two points of the network speeds incident investigation for CPTs. Visualizing detailed access

"We are overwhelmed with data and underwhelmed by information. RedSeal allows us to prioritize with actionable intelligence and stop playing whack-a-mole."

– DoD Customer

"We have to be lean and agile as we execute our programs. We cannot keep the United States safe into the future, especially in the rapidly changing domain of cyber, using a firehose approach. We have to have the precision of a microsurgeon. We can't just be good, we have to be great. And, we can't be great without partnerships."

– Adm. Michael S. Rogers, Cybercom

REDSEAL

and attack paths for individual devices in the context of exploitable vulnerabilities speeds decision making for cyber operators during a mission.

RedSeal builds its complete network model utilizing information that can be retrieved either dynamically or completely offline. The first is the Layer 2/3 configuration data from devices such as routers, firewalls, switches, VPN concentrators, and load balancers including public cloud and software-defined networks. Utilizing the most current configuration files, RedSeal builds a comprehensive network map showing every possible way in, out, and through the network and detailing all possible attack vectors. RedSeal performs a compliance check on every device against industry standards such as DISA STIGs and NIST guidelines. This proactive automation greatly reduces audit prep time (CCRI, others) and assists with speedy remediation.

The enemies of resilience are: incomplete information, lack of actionable intelligence and inability to act. The way forward is to integrate a complex ecosystem of cybersecurity tools across the technology stack, physical, virtual and cloud networks and data sources. RedSeal integrates into the user interfaces of proven tools like Tenable SecurityCenter, Rapid7's Insight VM, ForeScout's CounterACT, and industry-leading SIEMs from Splunk, IBM QRadar, and ArcSight. It works with Gigamon to detect live network traffic in your model. And, RedSeal includes sections of your network in AWS and Microsoft Azure, VMware NSX and Cisco ACI.

The RedSeal platform has been widely adopted by civilian, intelligence, and DoD agencies as well as commercial enterprises. With operational certifications such as NIAP EAL 2, DADMS, and ATOs from USMC and DISA, RedSeal was chosen as a component of the JRSS program, the security stack for the Joint Information Environment (JIE).

Key RedSeal Capabilities

- End to end network mappingand modeling
- Attack vector analysis
- Enclave/segmentationpolicy analysis
- Virtual penetration testing ofentire network
- Advanced threat scenariomodeling and simulation
- Incident investigation
- Vulnerability prioritization withnetwork context
- Layer 2 & 3 devicecompliance checking
- Works with existingsecurity products
- Unified network model,Including on-premise, SDN,cloud and hybrid datacenters
- Risk-based security auditand assessment

All CPTs require understanding and a model of the cyber terrain to discover, detect, analyze and mitigate threats and deliver resilience to the mission. RedSeal's network modeling and risk scoring platform enables enterprise networks to be resilient to cyber events and network interruptions.

RedSeal is the unique foundational platform to enable CPTs to achieve their missions.

To schedule a demo, or for more information, go to https://www.redseal.net/government/dod/

ABOUT REDSEAL (redseal.net)

RedSeal — through its cloud security solution and professional services — helps government agencies and Global 2000 companies measurably reduce their cyber risk and show where their resources are exposed to the internet.

Only RedSeal's award-winning cloud security solution can bring all network environments– public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on premises — into one comprehensive, dynamic visualization. RedSeal verifies that networks align with security best practices; validates network segmentation policies; and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk. The company is based in San Jose, California.

REDSEAL

+1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net