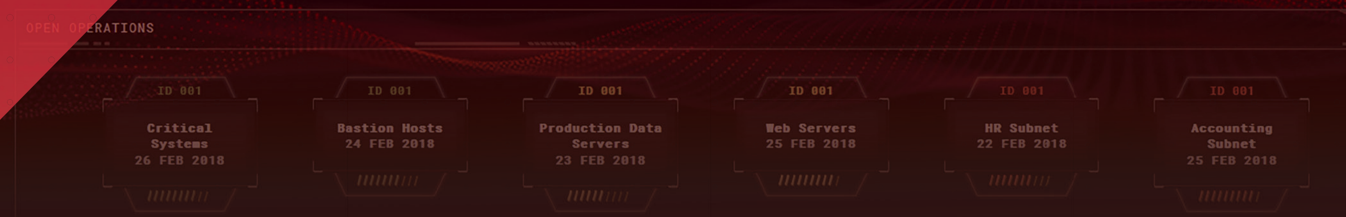

R9B HUNT
PROOF OF VALUE

Background and Description

root9B (R9B) understands how cyber attackers identify and target their victims and know that traditional passive solutions are ineffective against resourced and motivated adversaries. There are weekly reports of businesses and government entities falling victim to devastating cyberattacks. Your business depends on maintaining the trust and security of your network and the information vital to you and your clients. R9B provides proactive cybersecurity services which neutralize the threat and mitigate the risk of being the next headline.

R9B combines powerful tools to provide interactive, manned cyber defense executed proactively to search for malicious activity in your network. Our ORION platform provides a unique proactive, remote, and agentless HUNT capability to identify, stop, and remove adversaries who by-passed passive security technologies. HUNT operations are supported by client-specific, tailored Threat Intelligence (TI) which direct R9B operators to those areas of your network most critical to your business and assessed to be at greatest risk.

Proof of Value (POV) Scope

Prior to beginning operations, R9B and your team meet to agree upon the scope and duration of the POV. You indicate parameters within which you prefer we operate, particularly segments of your enterprise most critical to your business. We provide the following:

HUNT – Our operators integrate a deeper understanding of your cybersecurity architecture, perimeter defenses, and your client-specific TI to HUNT for indications of malware or exploitable vulnerabilities. We use our proprietary tools to include:

Adversary Pursuit Center (APC) – R9B's 24/7/365 remote computer network security operations center. R9B SOCs are located in Colorado Springs, CO, and San Antonio, TX. Both host a suite of services ensuring our ability to scale, react, and defend your networks.

ORION HUNT Platform – ORION quickly and accurately facilitates identification of unknown network intrusions. It provides cyber defense operators a comprehensive view of security risks to critical network segments.

- Agentless remote live memory analysis
- Designed for stealth
- Very light system and network resource footprint
- Designed to operate in diverse OS, system, virtualized, and distributed environments

ORKOS credential risk assessment – ORKOS identifies exposed risks focused on credential management while providing remediation recommendations.

- Advanced logic to analyze myriad conditions, privileges, and configurations which could potentially be used by an adversary to laterally move within a network
- Provides credential risk awareness to measure external adversary and insider threat vectors
- Cutting-edge visualization to identify and analyze credential risk likely paths of lateral movement pre and post incident
- Characterizes immediate risks, as well as higher-order effects.

THREAT INTELLIGENCE:

- Establish a baseline of threat exposure to identify likely adversaries, vectors, goals, and motives
- Develop threat profiles to identify motivation, sophistication, unique threat signatures, and recent or current tactics of the adversaries most likely to target your networks

Client-Provided Requirements

To successfully demonstrate the full benefit of our services during this POV, R9B requires:

System Admin or equivalent account privileges for the duration of the POV

- R9B HUNT engineers gather essential artifacts remotely and run specialized operations using our ORION platform
- None of the capabilities employed as part of HUNT operations cache credentials on the remote system
- We launch scans and collect information from a single point of entry facilitating operational logging, monitoring, and auditing
- At the end of the POV, we work with your technical representatives to ensure created accounts are deleted

VPN Access to in-scope POV Networks

- If we can reach all in-scope network segments via a single point of entry, only one set of credentials is necessary
- If network segments cannot be accessed through a single point of entry, we require access either through separate VPNs or the modification of existing network controls.

Deliverables

Upon completion of the HUNT POV R9B delivers:

- Executive Summary Report
- Findings report with detailed results of HUNT POV
- Initial ORKOS Credential Risk Assessment map and findings report
- A remotely provided executive technical out brief to discuss findings and recommended next steps

POV Benefits

As thought leaders in the field, R9B has brought about a true paradigm shift in defensive cybersecurity. We welcome the opportunity to demonstrate what our services can deliver in enhanced security to your organization. The direct and tangible benefits our HUNT services provide include:

- Prioritized and focused security efforts ensuring your most critical operations and information are protected first
- Identification of threat vectors specific to your organization allowing highly tailored support to defend against persistent and adaptive adversaries
- HUNT operations driven by business relevant threat intelligence
- HUNT services conducted remotely from our APCs provide a platform to execute effective proactive cyber defense
- Cybersecurity operations, products, and services designed, developed, and delivered by real world practitioners experienced in dealing with the adversaries targeting your enterprise

R9B

ROOT9B.COM

INFO@ROOT9B.COM