CYBERVIEW SECURITY ASSESSMENT:

Digital Security Beyond the Border

Red River

TECHNOLOGY DECISIONS AREN'T BLACK AND WHITE. **THINK RED.**

Red River Security Assessment Services

Red River has a strong security methodology that prioritizes risk management, industry awareness and threat intelligence as cornerstones of our security solution programs. A key component of our offerings is a suite of Security Assessment Services (SAS), which are specifically designed to help our customers prioritize security risks, gain additional insight into potential threats and keep pace with the evolving security threat landscape, both internal and external to the organization.

Red River's SAS services are designed around areas of specific focus beyond the typical vulnerability scan and network penetration assessment services. SAS value items include:

All SAS offerings are fixed price, so there is never a surprise or hidden cost.

SAS solutions are value-bundled with extra time, effort and security services scoped into each offering, producing robust results when compared to typical time-billed efforts.

Security services designed to target specific business value and security deliverables. This helps our customers utilize specific assessments to achieve the desired results.

Red River is continually updating our SAS program. We know threats are continually evolving and as a result Red River's assessment programs are continually adjusted to help our customers stay one step ahead and have all the information needed to keep their security programs in line with their risk management goals.

Published 09/25/2019

Cyberview SAS

One request that has been a common among CISO's and security managers, "Tell me what I don't know."

Red River has designed Cyberview to specifically answer that question. The digital footprint left by organizations in Cyberspace and within business-to-business partnerships is a powerful and growing threat. Information unknowingly left behind is collected, posted and sold on the Dark Web. Common examples of Dark Web threats include:

- Stolen employee credentials, including valid passwords
- Confidential company documents (corporate credit cards, financial sheets, payroll, HR info, etc.)
- Coordinated attacks & threats targeting your organization
- Exposed confidential information gained via social media
- Employee information obtained from phishing attacks
- Ransomware & malware variants that could directly affect your company

The focus is to expose Cyber & Dark Web vulnerabilities that could lead to the loss of sensitive data, introduce brand damage, and potentially lead to targeted cyberattacks from bad actors.

Cyberview Assessment Components

The goal of Cyberview is to review leading-edge attack vectors specific to cybersecurity and internet- facing connectivity. The focus is to expose Cyber & Dark Web vulnerabilities that could lead to the loss of sensitive data, introduce brand damage, and potentially lead to targeted cyberattacks from bad actors. Each Cyberview Assessment includes the following:

Published 09/30/2019

Private Asset Exposure Review

Red River will conduct comprehensive Dark Web information discovery specific to your organization's company name, primary company alias, related information assets and associated employee information.

- Extensive visibility into your organizational digital footprint and asset exposures, includes full forensic context plus enriched data to maximize fidelity.
- Searches for malicious activity, threat indicators to enterprises, illegal marketplace dealings, and more. Include Social Media, Paste Sites, Chans, Dark Nets (TOR, I2P, etc.), Forums, and Blogs.

Cyber Network Architecture Review

Red River will assess the cybernetwork (the boundary of your network, to include those systems that are accessible externally from your environment) for effectiveness, usage, reporting capabilities and recommended best practices in the following areas:

- Internet connection type & DDoS protection
- Cloud services being utilized
- DNS security
- Systems in place for identity, authentication & access management
- DLP capabilities
- App security samples (Internet apps, network security controls, vulnerability mgt process)
- UEBA / Anomaly detection
- Social engineering & phishing end user training program review
- Reporting & detection capabilities (SIEM / SOC capabilities)
- Network security setup & ability to react in case of event (People, Process & Technology)
- General Cyber security network profile & review

In addition, Red River security experts will interact with your IT/Security team to perform a technical assessment via system access in the areas depicted below (where applicable):

- End Point Detection & Response (EDR)
- Encryption use (in flight & at rest)
- Firewall use & set up (Layer 3-7; host, virtual or physical)
- IDS/IPS
- Email security
- Content filtering

Enhanced Vulnerability Scan & Penetration Testing (Optional)

As an additional service, this authenticated network scan consists of finding devices on the network by scanning a range of addresses.

Third-Party Vendor Security Review

Assesses the risk footprint and security posture of select third-party partners with sweeping assessment of business partner cyber risk and data exfiltration. Initial security metrics will report on the potential threats and risks of your organization's business partners, vendors, contractors and service providers, summary report includes supporting data.

Cyber Security App Scan

Report vulnerabilities found on select web applications or URLs and associated host names. The vulnerability scan will reference more than 100,000,000 verified attack vectors. The final report will include a summary of application layer vulnerabilities by asset and vulnerability class, as well as your overall application security profile based on the applications/ selected URLs.

Strategic Findings and Recommendations Report

Red River will deliver a findings and recommendations report, prioritized by severity, specific to the findings discovered during this Cyberview assessment. Final report will include areas of vulnerability, suggested areas of remediation, and specific recommendations (this is not just a list of scan results).

A unique value add, Red River offers an additional presentation: Our executive customer team will meet with your executive-level team to formally review our findings report and suggest remediation activities, prioritized based on criticality and potential impact to your organization.

Cyberview is specifically designed to help our customers **"understand what they don't know,"** gain a detailed understanding of their cybernetwork security capabilities and valuable insights into areas of emerging threats, and quickly acquire expertise at a fraction of the cost and time needed to do perform this as an organizational initiative.

For more information, please contact Red River at **security@redriver.com**

About Red River

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing more than 20 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions.

For more information please call 800.769.3060 or visit **redriver.com**

Follow us on Twitter: **@ThinkRed**

Red River

TECHNOLOGY DECISIONS AREN'T BLACK AND WHITE. THINK RED.