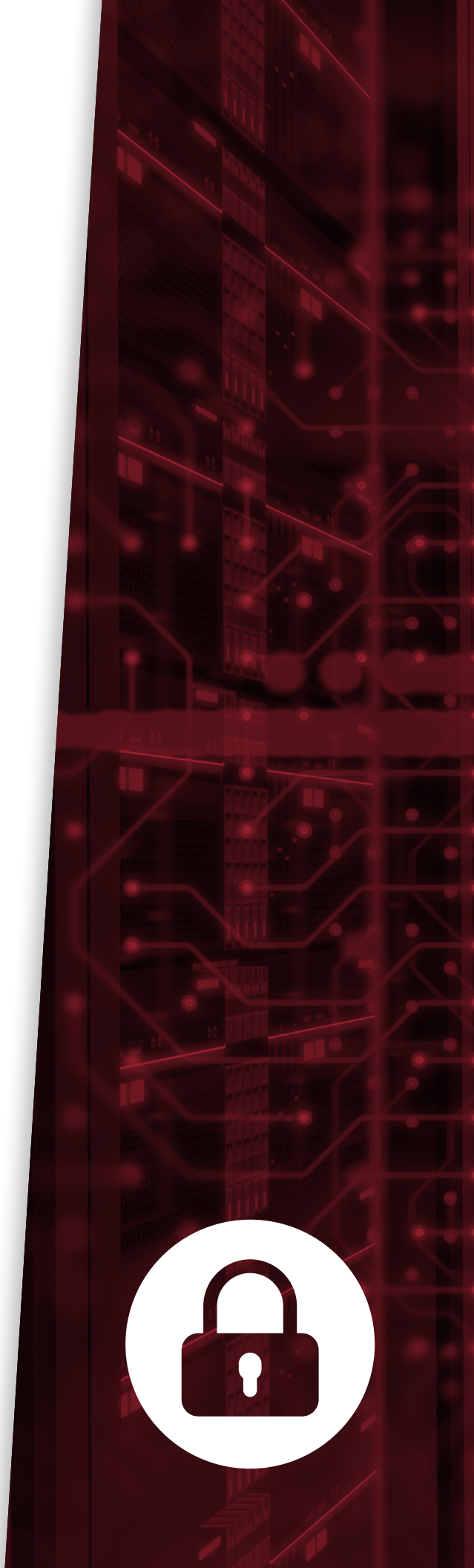
FOUNDATIONAL SECURITY ASSESSMENT:

The Critical Insights You Need To Effectively Manage Risk



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:

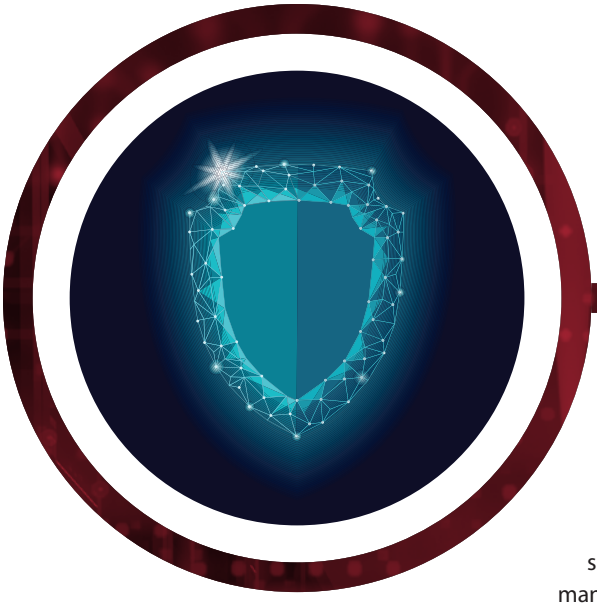
All SAS offerings are fixed price, so there is never a surprise or hidden cost.

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



Foundational Security SAS

Red River's Foundational SAS gives you baseline information and reporting to make informed security and risk assessments. The goal of this security service is to help our customers understand overall critical security vulnerabilities, threats and risks by mapping the current and desired level of operational security maturity using specific business and technical drivers to generate a tailored risk management plan and remediation strategy.

Foundational Security Assessment Components

The primary focus is to understand your organization's current security framework and controls, network security infrastructure, application security, security operations and incident response.

Every Foundational Security Assessment includes:

Security Framework Assessment & Review (Cyber, Infosec & Network Controls)

Red River Security will leverage the NIST CSF framework, a prioritized set of the "CIS Top 20 Critical Security Controls" and our Industry/Vertical-Specific Recommendation Practices to review your organizational information security program, identify and assess current safeguards, and communicate with key stakeholders regarding relevant risks and observations. In addition Red River keeps a strong focus on data assurance & related information privacy compliance requirements, gaps in coverages and Red River recommended best practices.

Published
09/25/2019

High risk areas of opportunity related to information assurance include:

- Risk Assessment and Management
- Policies and Security Strategy
- Incident Response, Business Impact Analysis, Disaster Recovery
- Security Awareness
- Encryption of Data
- Vulnerability Management
- Access Management, Role Based, Change in Roles, Access Review
- Security Monitoring and Alerting

The Foundational Security Assessment will serve as a critical input in the development of an overall Strategic Security Framework and Roadmap.

Initial Dark Web Report & Spear Phishing Exposure Testing

Using a variety of "Open Source Intelligence Software Tools," Red River will mine the internet for detailed information about company infrastructure. Internet sources mined for data are considered open source intelligence (OSINT).

Examples of data derived from Red River's OSINT efforts will include:

- Publicly available employee digital profiles
- Publicly available Company data and information
- Publicly available network and technical

Red River will also perform spear phishing end-user testing on a select number of company-named employees to create a sample representation of your company level of security awareness and the impact associated with targeted malicious efforts.

Company Network Architecture Review

As the foundation, access and transport to all your organizational information, Red River will assess the entire network infrastructure for effectiveness, usage, reporting capabilities and recommended best practices in the following areas:

Internal Network Architectural Review, Assessment & Recommendations:

- General network security profile & review (LAN, Campus locations & WAN)
- DNS security (internal)
- Systems in place for identity, authentication & access management
- DLP capabilities
- UEBA / Anomaly detection
- Reporting & detection capabilities (SIEM / SOC capabilities)
- Network security setup & ability to react in case of event

External Network Architectural Review, Assessment & Recommendations:

- General Cyber security network profile & review
- Internet Service Provider review
- DDoS prevention capabilities
- DNS security (public facing)
- Network Firewalls
- Systems in place for identity, authentication & access management (public facing)
- DLP capabilities (ISP outbound)
- Cyber network security setup & ability to react in case of event

In addition, Red River security experts will interact with your IT/security team to perform a technical assessment of the internal network areas depicted below:

Internal Network:

- Endpoint detection & response (EDR)
- Encryption use (in flight & at rest)
- Firewall use & set up (Layer 3-7; host, virtual or physical)
- Internal network vulnerability scan

External Network:

- Firewall use & set up (Layer 3-7; host, virtual or physical)
- IDS/IPS
- Email security
- Content filtering
- Essential external vulnerability scan

Security Operations Review

To ensure operational readiness, Red River will perform a high-level review of your organization's ability to monitor, respond & mitigate security issues from the perspective of a typical Security Operations Center and related industry best practices. The goal of the review is to gauge general incident response readiness, testing and practice areas currently being employed, and the associated recommendations related to the customer's business size and industry vertical.

Third-Party Security Program Review

Third-party vendor security risk management is fast becoming a critical area to review and contain exposers and risks associated with your service and supplier network. Red River will assess the risk footprint and security posture of your organization's third-party program, including the initial assessment of business partner cyber risk and data exfiltration. Security metrics include the potential threats and risks associated with key business partners, vendors, contractors and service providers across multiple categories.

Application Security and DevSecOps Program Review

The importance of application and DevOps security cannot be overstated. Red River will perform a software security process review to identify and understand the vulnerabilities that can be exploited in the code your organization leverages. In addition, your business may leverage software and code from a variety of sources, including both internally developed code, outsourced development and purchased third-party software. Red River review process supports your secure development lifecycle, security incident response capabilities and internal bug bounty efforts.

Code Review

As part of the discovery-based application security process, Red River conducts a sample code review of a select application of the customer's choosing. The assessment will review up to 500,000 lines of code as part of this app sec review process. Red River will also review your security toolset and process automation of security test (SAST, DAST, plus TBD as appropriate).

DevSecOps

While many organizations are just now beginning to utilize DevOps and CI/CD application methods, we feel it is never to early to begin the security foundation review process to better enable this fast-moving application development methodology. As part of the Foundational Security program, Red River will either review or discuss potential plans for your company's DevSecOps program, overall security process and implementation. Red River will inspect and provide recommendations on your company's software development principles, collaboration, communication, and automation as it relates to securing the DevOps process.

Final Report & Recommendations Presentation

It is one thing to perform the security discovery work, it is another thing altogether to present the results in a manner that is equally beneficial to the security engineers as it is at the executive level.

Red River prides itself on the quality of the discovery and findings report – how the information is presented and how it will be used going forward. The final report will include areas of vulnerability, suggested areas of remediation and recommendations specific to your organization and security controls supporting critical business processes.

As a unique value-add, Red River will assemble our Executive customer team (Account Executive, Technology & Services Leadership) to meet with your Senior Management or Board-level team to formally review our findings report and suggest remediation activities, prioritized based on criticality and potential impact to your organization.

The outcome of this conversation serves to assist with identifying additional initiatives and action plans with the potential to have Red River help with people, process & technology recommendations and supporting activities, based on your company's timeframe and priorities.

The time is now to ensure your organization's security framework and practices are optimized for managing risk. Red River's Security Assessment Services is here to help. 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**