Red River

Red River’s K-12 Secure-EDU Security Posture Assessment Service:

Security Insights To Help K-12 Effectively Manage Risk

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, K-12 compliance awareness and effective security program budget management as cornerstones of our Secure-EDU programs. A key component of Secure-EDU offerings is our Posture Assessment Service (PAS), which is specifically designed to help our school districts 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 PAS services are designed around areas of specific focus beyond the typical vulnerability scan and network penetration assessment services. PAS security systems are designed to simplify the security process and work within your budget needs:

- All Secure-EDU PAS offerings are fixed price, so there is never a surprise or hidden cost.
- PAS 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.
- Red River PAS security services designed to target specific value and security deliverables.

K-12 PAS VALUE

The goal of the Secure-EDU PAS tool is to help our K-12 customers understand overall critical security vulnerabilities, gaps in compliance, areas of risk around student PII, K-12 specific threats and risks by mapping the current and desired level of operational security maturity using your District-specific exposures and K-12 best practices to generate a tailored risk management plan, security roadmap program and remediation strategy.

SECURE-EDU PAS COMPONENTS

The primary focus is to understand your K-12 District current cyber security framework and controls, network security infrastructure, student PII and critical data security controls, dark web digital footprint exposure, security operations and incident response capabilities. Every PAS engagement includes:

K-12 Security Framework Assessment & Review (Cyber, Infosec & Network Controls)

Red River Security will perform 1 of 3 actions in this area:

- Review your District K-12 security framework (policy & procedures)
- Leverage the NIST CSF framework, perform a gap analysis and recommendations
- Utilize the Center for Internet Security (CIS) framework, leverage a prioritized set of the CIS Top 20 Critical Security Controls to perform a gap analysis and recommendations

Published 10/15/2020

The results are recommendation practices that your K-12 organization can develop a streamlined and resource-effective cyber and information security program. Primary goals include identify and assess current safeguards and a program to communicate with key stakeholders regarding relevant risks and observations. In addition, Red River keeps a strong focus on student data assurance & related information privacy compliance requirements, gaps in coverages and Red River recommended best practices.

High risk areas of opportunity related to student PII and critical K-12 information assurance:

- 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

Secure-EDU PAS 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" and Groupsense First Recon Data Report, the goal of this phase is to mine the internet for detailed Information about your K-12 dark web presence and begin to understand the District Digital Risk Management exposures. 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 K-12 employee digital profiles
- Publicly available District data and information
- Publicly available network and technical information

K-12 District 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 *(Comprehensive service only)*

- 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

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
- Spear-Phishing Test

Security Operations Review

To ensure K-12 operational readiness, Red River will perform a high-level review of your organization's ability to monitor, respond and 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.

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 25 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.