

Cybersecurity for state agencies, schools and colleges

Digital risk assessment and training that changes behavior

Find and fix your biggest digital risks, meet your insurer's requirements, and train every employee and staff member to spot an attack, with a team that works alongside your IT staff.

/01 Schools are a favorite target

82%

of K-12 schools experienced a cyber incident between July 2023 and December 2024.

K-12 DIVE, ON THE CENTER FOR INTERNET SECURITY REPORT, MAR 2025

+23%

ransomware attacks on schools, colleges and universities in the first half of 2025, year over year.

K-12 DIVE, ON THE CENTER FOR INTERNET SECURITY REPORT, MAR 2025

2 to 9 months

to recover after a cyberattack, with 3 days to 3 weeks of lost learning.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE, OCT 2022

/02 Digital risk assessment

Our experts work with your IT and operations teams to find the controls that are below standard and fix them in the right order, aligned with NIST.

01 Mitigate

Your security perimeter and infrastructure, regulatory and contractual obligations, and legacy and cloud technology.

02 Protect

Adaptive security assessments, policies pre-vetted against insurer requirements, and industry compliance modules.

03 Enforce

Incident response planning, consistent controls across old and new systems, and a maturity dashboard with periodic reporting.

AT A GLANCE

BUILT FOR

K-12 districts, colleges and universities, state agencies and education service agencies

CORE SERVICES

Digital risk assessment and security awareness training

ADD WHEN READY

MSSP++ managed IT and security, and 24/7 SOC monitoring

COMPLIANCE

Cyber insurance requirements, and CIPA, COPPA and FERPA considerations

LEARN MORE

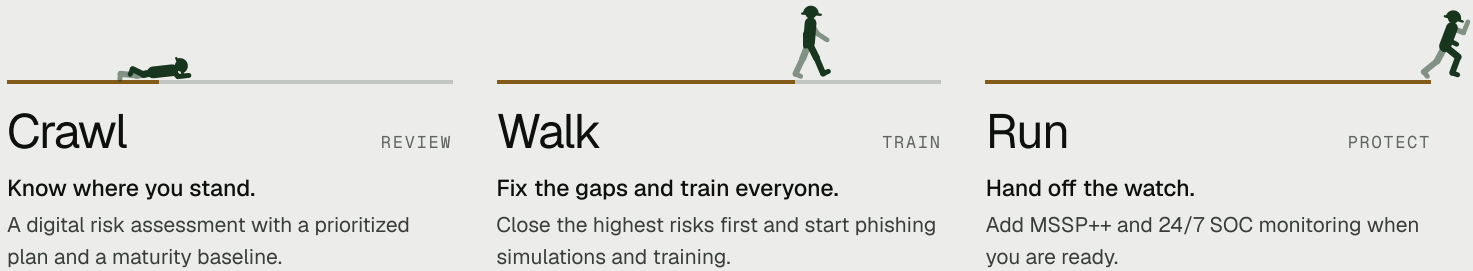
digitalteamsix.com/solutions/sled

/03 Security awareness training that changes behavior

Short, frequent lessons and realistic phishing tests, tailored to your policies, your regulators and your cyber insurance requirements.

- Phishing simulations modeled on real attacks, including spoofs of your own systems
- Dark web checks that show who needs to change a compromised password
- Short, adaptive modules plus compliance modules and your own policies
- Cyber risk ratings and reports your leadership can act on

/04 Three phases. In the right order.



/05 Built for how education works

WHAT WE FOCUS ON

School districts	CIPA, COPPA and FERPA considerations in policies and training, web filtering and activity monitoring for student safety, and training for teachers, staff and administrators.
Colleges and universities	Open networks segmented and monitored, research and student data protected, and training across faculty, staff and student workers.
State agencies	Controls aligned with NIST, cyber insurance readiness, and incident response plans with tabletop exercises.

/06 Questions schools and agencies ask

Will the assessment help with our cyber insurance renewal?

Yes. Policies and controls are pre-vetted against insurer requirements, which is often what qualifies you for broader coverage at a lower premium.

Does training work for staff who are not technical?

Yes. Lessons are short and frequent, and the phishing tests look like the email your staff actually receive.

Do you replace our IT team?

No. We work with your IT and operations teams and only take on what you want us to.

Find your biggest risks before an attacker does.

Request a digital risk assessment. An engineer will walk you through how it works and where we would start.

Request an assessment
digitalteamsix.com/solutions/sled
 973-339-0090
sales@digitalteamsix.com