DIGITAL TEAMSIX

DATASHEET

SOC

Security Operations Center, around the clock

Experts defending your organization around the clock. Our US-based security operations center, built for critical infrastructure, monitors, detects and responds across endpoints, networks and cloud, with a dedicated analyst and threat hunter.

/01 What the SOC does

/01

US-based SOC

Analysts based in the United States, supporting critical infrastructure, including water and wastewater systems, 24/7.

/02

Around-the-clock monitoring

Endpoints, networks and cloud watched 24 hours a day, every day of the year.

/03

AI-enabled detection

Endpoint detection that correlates events with your topology, your sector's threats and user behavior.

/04

Automated root cause analysis

Detections combined with environment telemetry to find where an incident started.

/05

Response across your controls

Incident response through the security controls you already run, on premises and in the cloud.

/06

Cross-tool threat hunting

One view across tools, so hunters find what single products miss.

/07

Vulnerability management

Vulnerabilities tracked and patches pushed, with reporting on what is left.

/02 When we find something

01

Detect

An alert arrives enriched with threat intelligence for your sector.

02

Confirm

Your analyst investigates and rules out false positives.

03

Contain

We contain it through the controls you already run.

04

Call

You hear what happened, what we did, and what to do next.

AT A GLANCE

COVERAGE

US-based, 24 hours a day, every day of the year

YOUR TEAM

A dedicated, US-based analyst and threat hunter

WORKS WITH

The security tools you already run, from multiple vendors

SEES

Endpoints, networks and cloud, and with Culper-I, control systems

COMPLIANCE RESULT

Incident reporting and insurance requirements met

LEARN MORE

digitalteamsix.com
/platform/soc

/03 Questions about the SOC

Do we need to replace our firewall or endpoint tools?

Usually not. The SOC integrates with the controls you already own and recommends changes only where coverage is missing.

What happens when you find something?

Your analyst confirms it, contains it through your integrated controls, and contacts you with what happened and what to do next.

Will this help with cyber insurance?

Yes. Monitoring, reporting and insurer-aligned training are the controls carriers ask about most.

/04 A named analyst, not a ticket queue

Every client gets a dedicated, US-based analyst and threat hunter who learns your environment, your people and your risks, and explains what they find in plain language.

- A dedicated, US-based analyst and threat hunter
- Automatic overview reports on your cyber health
- Cyber risk analysis your leadership can act on
- Training tailored to industry, regulatory and insurance requirements

/05 Keep the tools you have

01 **No rip and replace**
The SOC integrates multiple vendors' technologies, so you keep your existing security stack.

02 **Sees the plant too**
Alerts from Culper-I go to analysts who understand control systems, so IT and OT incidents are handled together.

03 **Informed by your sector**
Threat intelligence filters noise and adds context to every alert before an analyst sees it.

Put a security team on watch tonight.

Start with an assessment of what you run today, and where monitoring would close the biggest gaps.

Request an assessment
digitalteamsix.com/platform/soc
973-339-0090
sales@digitalteamsix.com