opentext™

SERVICE OVERVIEW

OpenText SOC Modernization Services

Modernize and mature your security operations center to unlock its full potential and meet the demands of the modern digital landscape

Benefits

- Increase efficiency and reduce the time it takes to respond to security incidents
- Improve threat detection
- Save costs and free up security personnel by automating routine tasks
- Meet compliance requirements with a framework for incident response and reporting

With the proliferation of devices and applications, the attack surface for potential threats is expanding. Security operations center (SOC) personnel often face constant alerts, forcing them to react using disconnected point tools and manual processes. Cybersecurity threats are also becoming increasingly complex, sophisticated, and well-funded. The volume of data and network traffic that typical organizations deal with is tremendous, and new and unknown threats pose a significant challenge, as they may not be detected.

It is paramount to develop threat-detecting use cases that inspire confidence and can be adapted to reduce the response time, ensuring they are contextually relevant and effective. The necessity for analysis and investigation of large-volume alerts and threat-hunting is constant.

Overcoming these challenges requires a modern approach to SOC operations, including establishing SOC governance, investing in the right technologies, training staff, and developing the right process and procedures to "Identify, Protect, Detect, Respond, Recover" (see the NIST/CFS 2.0 Framework). Achieving this optimal state poses a formidable challenge for the SOC and leadership teams. The OpenText Cybersecurity Services is committed to assisting you in this endeavour.

Resources

Join the conversation

Strengthening Higher Education Institutions against evolving cyberthreats - OpenText Blogs ›

Learn more

OpenText Behavioral Signals ›

OpenText Enterprise Security Manager ›

OpenText Core Adversary Signals ›

OpenText Core Threat Detection and Response ›

Download

Security Assessment Services ›

Digital Forensic & Incident Response (DFIR) ›

Threat Hunting Service ›

Managed Security Services (MSSP) ›

These Professional Services packages are designed to modernize your SOC and improve your organization's overall security posture by leveraging the latest security technologies and best practices. Modern SOC services shift from a reactive to a proactive defence strategy, identifying potential threats before they can impact your organization. OpenText will deliver these services through our senior security operations experts, who understand how a SOC should or can work. Partner with a provider specializing in SOC operations and gain access to expert knowledge and skills that may not be available in house.

SOAR Primer

Accelerate your usage of SOAR to achieve mandatory EU regulations (e.g., NIS2, DORA) or international frameworks (i.e. NIST) and respond quickly to threat detection and remediation by providing multiple forms of automation. This service is ideal for existing OpenText Enterprise Security Manager customers who have not set up their "license-free" OpenText Enterprise Security Manager SOAR functionality or want to optimize its usage. In this 10-day workshop (2× 5 days Service Package), OpenText will optionally install SOAR and implement two key templated SOAR playbooks using input from staff members. Staff will gain enough knowledge to work independently in developing new playbooks.

SOC Mentoring

This offering can be used flexibly (i.e. several five-day Service Packages) and is designed to guide you in managing and enhancing your SOC cybersecurity posture. The goal is to empower you to manage your security operations effectively and confidently by providing a named mentor for one-on-one sessions to guide and share industry-wide insight. This is an excellent opportunity for SOC analysts, managers, and IT security directors, as it helps build capacity and capability. Customers will benefit from our SOC consultants' extensive experience and will gain insight to improve their skills for their day-to-day duties.

Threat Model & Use Case Workshop

This can be used flexibly (i.e. several five-day Service Packages). Broader than a simple use case review, this service is designed to equip you with the skills and knowledge to identify, assess, and mitigate potential security threats to your IT infrastructure. It involves providing hands-on experience to the team for developing and tuning use cases. This goes beyond a service to help you build capacity and capability.

Our Cybersecurity Services team is comprised of highly skilled and certified professionals with the expertise to handle a wide range of cybersecurity issues. OpenText invests in continuous training and development to ensure our team stays on the forefront of cybersecurity trends. As a world leader in cybersecurity, OpenText brings decades of consulting experience to helping our customers with NIS2 compliance. Our solutions can be tailored to meet your organization's needs and drive outstanding outcomes.

opentext™