

# Unlock the full potential of your SIEM solution.

## CDW SIEM Professional Services



The average company can encounter anywhere from 10,000 to 200,000 security events in a given day<sup>1</sup>, making it easy to miss a potential security threat. Security teams are not only struggling to battle the onslaught of cyberattacks, but also manage the overwhelmingly large amounts of data across their IT landscape; and these same teams do so with a patchwork of tools, which can overcomplicate security operations, lead to missed critical alerts and, ultimately, expose organizations to security vulnerabilities and regulatory fines.

SIEM tools are vital to maintaining an effective and secure cybersecurity program, but finding the right option for your organization and its unique needs and environment can be a challenge. With CDW's SIEM Professional Services, organizations can build a comprehensive solution that empowers their security teams and strengthens their overall information security posture.

CDW SIEM Professional Services can help you achieve:



**Operational  
Efficiencies**



**Increased  
Performance**



**Reduced  
Risk**

### Finding the Right Solution

CDW delivers end-to-end SIEM services to improve the effectiveness of your security team, reduce the impact of security incidents and demonstrate compliance with regulatory mandates. Our partnership with the industry's most reputable technology providers enables us to seamlessly integrate the best SIEM solution into your cybersecurity strategy and derive the maximum value from your SIEM investment.

A strong SIEM solution plays a key role in identifying, investigating and responding to security threats in real-time. We work with today's leading SIEM solutions, including Cribl, Splunk, QRadar, Exabeam and Sumo Logic, to align your organization with the features and capabilities you'll need for long-term success.

Regardless of your existing security tools or where you are in your SIEM journey, CDW will help maximize your SIEM investment with integration and optimization services.

- **Assess:** CDW evaluates your SIEM environment to identify areas for improvements, helping you gain the insights you need to optimize your SIEM investment.
- **Design and Deploy:** CDW designs the optimal SIEM configuration for your organization based on your specific business goals and requirements and delivers a deployment roadmap to make integration and migration as simple as possible.
- **Extend:** Our team of experts provides long-term support of your SIEM solution by delivering managed services, expanding your deployment to integrate with new technologies and optimizing your SIEM tool to maximize your ROI and get the most out of your investment.

<sup>1</sup>Source: Cyber Security Nordic, "The average company encounters 200,000 security events every day. Is your organization prepared?" April 26, 2022.

CDW's full lifecycle of Services can support your organization no matter where you are on your journey



Design



Orchestrate



Manage



On-Premises



On-Journey



Cloud-Based

## CDW + SIEM SOLUTIONS

Our SIEM Professional Services help organizations mitigate cybersecurity risks and meet regulatory compliance standards due to our:

- **Trusted and Experienced Team:** Our team is composed of seasoned and CISSP-certified professionals, with a robust range of technical consulting and advisory skills and more than seven years of focused SIEM services experience.
- **Tailored SIEM Solutions:** We design a mature and optimal SIEM solution based on your unique cybersecurity business goals, and build a roadmap to deliver a successful and sustainable deployment.
- **Technology Partnerships:** Our partnership with the industry's leading SIEM technology providers enables us to deliver a comprehensive solution that fits your organization's needs.
- **Streamlined Compliance:** CDW provides the support you need to simplify compliance reporting and meet the changing demands of industry-specific compliance requirements and responsibilities, including GDPR, HIPAA and PCI-DSS.



## Services Overview

The following capabilities and services are available within our SIEM Professional Services:

Service	Available
Assess	
<b>System Health Check</b> <ul style="list-style-type: none"><li>Review your environment against recommended standard configuration and investigate your data ingestion to optimize your licensing consumption.</li></ul>	✓
<b>Data Optimization Assessment</b> <ul style="list-style-type: none"><li>Bring clarity to your data so you can improve your insights and outcomes. See the data you need to see, and nothing you don't.</li></ul>	✓
<b>Platform Upgrade Readiness Assessment</b> <ul style="list-style-type: none"><li>Prepare for critical upgrades or expansions.</li></ul>	✓
Design and Deploy	
<b>SIEM Deployment Architecture and Design</b> <ul style="list-style-type: none"><li>Design the optimal configuration for your organization and goals, and build a roadmap for successful and sustainable deployment.</li></ul>	✓
<b>Implementation Services</b> <ul style="list-style-type: none"><li>Implement a SIEM tool, integrate with high-priority data sources and technologies, and configure reporting to maximize your insights.</li></ul>	✓
<b>Migration Services</b> <ul style="list-style-type: none"><li>Move to the cloud or upgrade from an outdated log collection platform to a best-of-breed tool.</li></ul>	✓
Extend	
<b>Managed Support</b> <ul style="list-style-type: none"><li>From deployment and configuration to maintenance and upgrades, CDW delivers a wide range of managed SIEM services for leading providers.</li></ul>	✓
<b>New Technology/Data Ingestion</b> <ul style="list-style-type: none"><li>Expand your SIEM deployment to ingest new sources or integrate with new technologies.</li></ul>	✓
<b>Staff Augmentation</b> <ul style="list-style-type: none"><li>Supplement your team, or scale up to handle high demand, with a qualified, certified expert from CDW.</li></ul>	✓

## CUSTOMER SUCCESS STORY

**Organization:** Large financial company

**CHALLENGE:** With multiple terabytes of data spread between different backup sites, the customer required a solution that could maintain copies of operation data and allow them to back up data from a specific date in time to remote storage. The customer did not have existing backup capabilities in place; instead, they had an array of SIEM appliances across various data centers that were backing up data locally, which would take an extensive amount of time to recover in the event of a disaster.

**SOLUTION:** CDW implemented remote backup scripts on each of the customer's SIEM appliances, configuring them to back up data to a central offsite location. The scripts were also programmed to inspect the local appliance's file system to assess and automatically sync any data that required backup after a restart. The scripts were modular and simple to implement so the customer could apply them to new SIEM appliances in the future to keep it protected even as its infrastructure grows.

**RESULT:** With the new scripting solution in place, the customer was able to restore its SIEM data and now only retains the data necessary to meet its recovery point objectives, accelerating recovery times and saving storage space and complexity. The solution helped to provide the customer a hands-off approach to remote backups on their SIEM appliances, minimizing overall backup errors and freeing up resources for other important projects and tasks.

## SIEM Partners



**To learn more about CDW SIEM Professional Services, contact your account manager or call 800.800.4239.**

