MANAGED SIEM

Security

SERVICE DESCRIPTION

1. SERVICE ONBOARDING

REMOTE ACCESS SETUP	In order for CDW to manage the SIEM service, secure access will be set up and tested during the onboarding process. This typically consists of a site-to-site VPN tunnel from the data centre where the SIEM is provisioned to the CDW secure management network. This secure access is utilized by our Security Operations Centre (ASOC) to manage and monitor the service.
DEVICE LOGGING AND VERIFICATION	CDW will provide guidance on how to identify the right log sources to be monitored by the SIEM to ensure maximum security visibility. This includes reviewing the appropriate set of security controls, servers, applications and infrastructure to send event logs to the SIEM solution. Additionally, we will advise on the desired logging levels and events to be analyzed.
MONITORING SETUP	CDW will consult with you to enroll the right security use cases and set the appropriate alert levels to deliver the SIEM service. Additionally, we will perform false positive tuning during the onboarding phase to establish the alerting baseline, and will continue false positive tuning as part of regular service maintenance.
REPORT SETUP AND CONFIGURATION	Review, setup and configuration of technical security reporting. CDW MS will provide technical reports included in this service, along with the ability to add custom reports through our change management process. Sample Reports: ▪ Attack summary ▪ Summary of botnet (command and control) activity ▪ Top 10 peer to peer applications ▪ Infections/malware detected on systems
DOCUMENTATION	Throughout this project the CDW MS team will work closely with the client to document their network infrastructure and security zones. This documentation package includes network diagrams and limited asset information.

SERVICE DESCRIPTION

2. ONGOING SERVICE

SECURITY MONITORING AND ALERTING	CDW will continuously monitor the SIEM solution 24x7x365 to identify suspicious and malicious behaviour. Our dynamic alerting is driven by security use cases tailored for every environment, and enhanced through cyberthreat research provided by our penetration testing team and third party threat intelligence. All alerts are qualified and triaged by our advanced security operations centre personnel, and actioned based on criticality.
SECURITY EVENT MANAGEMENT AND RESPONSE	CDW will detect and respond to security incidents generated by your SIEM solution on a 24x7x365 basis. CDW will analyze and qualify the incident, and work with the customer to implement counter measures to contain the threat. Once the threat is contained, CDW will follow up with the customer to ensure the threat has been eradicated and that they have recovered full business functions. NOTE: CDW may offer additional services to eradicate the threat, and recover from the breach, such as server rebuilds and restore from backup services.
TUNING AND OPTIMIZATION	As security threats continue to evolve, so too does your SIEM policy and detection engine. CDW continuously tunes the SIEM platform to identify new attack patterns, and identify suspicious and malicious behaviour. CDW will also recommend new use cases to enhance security detection and continuously improve the service.
MONTHLY REPORTING AND SERVICE REVIEW	On a monthly basis CDW will provide detailed technical reporting. These reports contain valuable information on technical threats and can often reveal common trends and security areas for improvement.

For more information, contact your CDW account team at 800.972.3922 or visit CDW.ca/security