KONICA MINOLTA | All Covered
IT SERVICES FROM KONICA MINOLTA

SIEM & SOC SERVICES

A SECURITY STRATEGY IS FOUNDATIONAL TO BUSINESS GROWTH AND INNOVATION

For businesses to strive, they have to accept that security is part of the company culture, and needs to be ingrained in everything they do. With this in mind, the All Covered SIEM services are orchestrated from our national Security Operation Centers (SOC) and are staffed with seasoned cyber security analysts.

With the enormous footprint of the day-to-day SOC services we provide to our clients, our cyber security analysis team is versed on several attack patterns and strategies that are frequently present within the threat landscape.

We bring this wealth of knowledge and experience into our investigation and analysis of customer environments. This allows our team to quickly tune our SIEM services to predominantly hone in on the malicious activity companies regularly experience. Our team of experts allows companies of multiple sizes with varying services to quickly realize the value of an enhanced SIEM operation. This is not something that can be easily built or purchased as our services have grown and matured over time. Additionally, our experience and expertise will not only help you meet compliance regulations but it will also give you the visibility and peace of mind all organizations need when looking to stop a breach.

LOG SOURCES	ADVANCED PERSISTENT THREAT	INSIDER THREAT	SECURING THE CLOUD	CRITICAL DATA PROTECTION	INCIDENT RESPONSE	COMPLIANCE	RISK & VULNERABILITY MANAGEMENT
Firewall/Router	x		x	x	x	x	x
Intrusion Detection System/ Intrusion Protection System	x			x	x	x	x
Web Proxy	x	x	x	x			
VPN	x						
DNS	x	x					x
DHCP	x	x			x	x	
Mail Logs	x	x		x			
Data Loss Prevention	x	x		x			
Endpoint	x	x		x			x
Identity/Authentication	x	x	x		x	x	
Antivirus	x			x	x	x	x
Network Insights/NetFlow	x	x	x	x	x	x	x
Database Logs	x	x	x	x	x	x	
EDR	x				x	x	x
Cloud Infrastructure/Audit	x	x	x	x			
Office 365			x		x		

SIEM FEATURES AND BENEFITS:

- 24 x 7 x 365 SIEM support
- Level 1 alert triage to reduce false positives and patient zero eradication
- Reduced meantime to discovery
- Skilled security analysts for improved incident response
- Cognitive AI integration for advanced investigations
- UBA (User Behavioral Analytics)
- Insider Threat Monitoring
- Client External Attack Surface Monitoring
- Additional external vulnerability assessments (outside of our Vulnerability Scanning and Management programs)
- Integration into All Covered ITSM
- Over 120 open source threat feeds and 4 premium threat feeds
- Proprietary threat intel from deep and dark web
- Customized use cases available

EXAMPLE SIEM USE CASES:

- Cloud-first threats
- Detection of Crypto Miners
- Compromised instances
- Outgoing port scans and DoS
- Misuse of identity
- Brute force attack protection
- Ransomware protection
- Botnet and C2 protection
- Data exfiltration protection
- Phishing attack protection

For immediate assistance with your security needs please email SecuritySales@AllCovered.com

KONICA MINOLTA

KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.
100 Williams Drive, Ramsey, New Jersey 07446
CountOnKonicaMinolta.com

For complete information on Konica Minolta products and solutions, please visit: **CountOnKonicaMinolta.com**

© 2020 KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.

10/20-P