2021 XDR Product Suite

CYBER LION

CyberLion's XDR Bundle gives companies the multi-layered protection that they need to stop threats, all monitored and backed by a 24x7x365 SOC and SIEM

Email Protection

PROTECTION FROM

- Phishing, Zero-Day Attack Phishing, 3rd Brand Impersonation
- VIP Impersonations
- Malicious Files
- Malicious Links
- Personal Device & Home Attacks
- Malicious Insider

KEY FEATURES

- Detects VIP spoofing, brand forgery, and other attacks used in business email compromise and phishing
- Provides user-friendly warnings in way of banners on malicious and suspicious email
- Sanitizes embedded links to help protect users from potentially malicious websites
- AI and computer vision models to catch evasion techniques
- Easy "Report to SOC Button" for human analysis
- Fast deployment built into CyberLion Dashboard

O365 Security Monitoring

PROTECTION FROM

- Malicious Admin Changes
- Unauthorized Delegate Access
- Failed or Unauthorized Access
- MFA Removed
- Foreign Login
- Impossible Login
- Suspicious Email Forward

KEY FEATURES

- Multi-tenancy dashboard
- SIEM correlation & SOC analysis
- Support for custom alerting and reports
- Visibility to login activity in CyberLion Dashboard
- Detects potential threats of suspicious activity in Office 365
- Supports industry & regulatory compliance requirements

Endpoint Protection

PROTECTION FROM

- Malware & Ransomware
- APT & Zero-Day Prevention
- Fileless Attacks
- Remote Worker Attacks
- Malicious Scripts
- Email Payloads

KEY FEATURES

- AI and behavioral-based
- Automated blocking
- Protection while offline
- Zero-day prevention
- Script and fileless malware detection
- Memory exploitation detection and prevention
- Easy deployment via CyberLion Dashboard
- Visibility to all managed endpoints in CyberLion Dashboard
- Low memory and CPU footprint

Network Security Monitoring

PROTECTION FROM

- Denial of Service (DoS) Attack
- Cross-Site Scripting
- SQL Injection
- FTP & Cloud Storage Exfiltration
- Command & Control Communication

KEY FEATURES

- Network intrusion detection
- SIEM analysis
- AI analytics engine
- Multi-tenancy dashboard
- Self-service reporting
- Physical or virtual appliance
- Supports key industry and regulatory compliance standards such as continuous monitoring and network monitoring

Log Security Monitoring

PROTECTION FROM

- Cloud Infrastructure Attacks
- Unauthorized Access
- Compromised User Credentials
- Anomalous Privilege Escalation
- Third-Party Violations
- Multi-Vector Attacks

KEY FEATURES

- Hundreds of supported integrations
- SIEM analysis
- AI analytics engine
- Multi-tenancy dashboard
- Self-service reporting
- Deployment of physical or virtual appliance for on-prem logs (like syslog)
- Supports key industry and regulatory compliance standards
- ROI - Merge data from existing security tools with multiple sources for greater visibility and re-use existing investment

www.cyberlion.cloud
info@cyberlion.cloud
704-800-5470