



DETECT: 24/7

24 X 7 X 365

Cyber-threat monitoring
and response services

- Enhance your business's security posture
- Reduce the risk of a data breach (internal or external)
- Minimize downtime and loss stemming from security incidents
- Gain intelligence about the cyber-threats targeting your business
- Strengthen your business's continuity program
- Improve regulatory & industry compliance measures

NETWORK SECURITY THROUGH 24/7 CYBER-THREAT MONITORING AND RESPONSE

Let skilled security experts keep watch over the activity on your network. By applying cutting-edge **SIEM (Security Information and Event Management)** technology and established threat intelligence, suspicious activity and security incidents on your network can be identified and remediated as they occur.

Real-time log collection: As devices on your network generate logs and events, they are collected and transmitted to the cloud in real time for automated correlation.

Accurate Detection: Thousands of security correlation rules enable speedy evaluation of millions of network events to identify suspicious irregularities.

Human expertise: Every security event identified by the cloud-based, 24/7 cyber-threat detection engine is viewed and evaluated by a trained cyber-security expert.

Threat Intelligence: Detailed analysis of valid security alerts are initiated within a state-of-the-art Security Operations Center (SOC) – staffed 24x7x365.

Security Response: Threat mitigation and remediation procedures using industry best practices are provided either remotely or on-site to ensure continuity.

Status Reporting: Executive-level and in-depth technical reports provide a view of the number and type of threats your network is facing.



IMPORTANT FOR YOUR BUSINESS:

Cyber-threat monitoring and detection are the cornerstones of an effective IT security strategy. But collecting the right data, parsing and analyzing it into manageable and useful pieces of information is an extremely complex task.

Our 24/7 security service employs automated technology, paired with a staff of security experts, to reduce the risk and complexity of protecting your critical network systems.

PROTECT YOUR NETWORK FROM THESE THREATS AND MORE:

- Port scans, host scans, denied scans, sudden change of traffic between certain IPs or other anomalies in traffic.
- Network server/device and admin logon anomalies – authentication failures at all times and unusual IPs.
- Network access irregularities from VPN, wireless logons and domain controller.
- Account lockouts, password scans and unusual logon failures.
- Rogue endpoints, wireless access points.
- Botnets, mail viruses, worms, DDOS and other “day zero” malware identified by cross-correlating DNS, DHCP, web proxy logs and flow traffic.
- Abnormalities in web server and database access.

Our process combines cloud-based technology, highly-trained security experts and a security response team who take action on any incidents targeting your network.

CONTACT US TODAY TO SEE IF YOU ARE ELIGIBLE FOR OUR 30 DAY FREE TRIAL!