Business Security through 24/7 Cyber-threat Monitoring and Response

Introducing 24 X 7 X 365 Cyber-threat monitoring and response services

- Enhance your company'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 continuity program
- Improve regulatory & industry compliance measures

No company wants to experience a data breach but it happens all the time. While larger companies can often weather the financial and PR storms associated with a breach, the average small business closes their doors within 6 months of a cyber-security incident[1]. What's worse is that a vast majority of breaches are active within the network for months or years before detection – the only thing missing in these cases was a security expert looking for the evidence of a compromise.[2]

Don't allow your business to be a victim of a cyber-hack!

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 business continuity.

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

www.ibsre.com (973)-575-4950

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.

Contact us today for a no-obligation quote on a 24/7 cyber-threat monitoring program.

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

What's involved in our 24/7 security service?

Collection: The process begins by collecting the most basic elements of cyber-threat monitoring: the event log (machine data) and configuration/performance (health check) data.

Correlation: This data is securely transmitted to the cloud, in real-time, where automated cyber-threat detection technology sorts through millions of events through a complex process called correlation.

Experience: The correlation rules used have been developed over nearly 15 years by world-leading security technologists and are constantly being updated and improved to ensure new threats are identified.

Intelligence: Discovered security alerts are escalated to a team of highly trained experts who perform a deep triage process by means of human inspection. This "eyes on" scrutiny definitively pinpoints security incidents which require attention to remediate.

Response: Finally, a response team member will act on the threat to neutralize or eliminate it - ensuring the risk to your business is reduced.

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.

1.U.S House Subcommittee on Health and Technology, March 2013.
2.Verizon Enterprise Services, 2012 Verizon Data Breach Investigations Report
3.Symantec Corporation, 2015 Internet Security Threat Report. April 2015.

www.ibsre.com
(973)-575-4950
99 Riverview Drive
Totowa NJ 07512