

IT Managed Security

Security Information Event Management

SIEM SERVICES

The triple threat against threats

EQ's fully managed SIEM service for healthcare and regulated organizations provides 24/7/365 real-time monitoring, alerting and analysis of technology assets in your organization. That's three layers of security to give your organization total peace of mind.

Security Information and Event Management (SIEM) systems more accurately identify unusual and potentially malicious activity from threats that include malware, phishing, viruses and spyware. Because organizations generate millions of log alerts every single day, the recognition and analysis of meaningful alerts in real-time is a complicated and resource consuming challenge. Security tools alone generate many false positive alerts and make finding legitimate threats even more difficult. EQ professionals skilled in web and cloud threat detection evaluate alerts to see which merit closer scrutiny, then gather context to determine severity and the potential courses of action.

With more organizations using Microsoft Office 365 than any other cloud application suite, the security challenges and threats are increasing for the administrative and security teams. The migration of critical and sensitive data to O365 cloud applications increase the security needs to monitor user authentications, data exfiltration/privacy, unauthorized access, and more. EQ has the expertise required to exceed your security objectives 24/7/365. We provide your business with the confidence, time and resources needed to keep up with strategic business demands.

Real-time visibility & actionable intelligence enables you to:

- Identify and protect your enterprise against persistent and evolving threats 24/7/365
- Achieve log monitoring compliance requirements for industry regulations such as PCI, DSS, GLBA, NERC, CIP, & HIPPA
- Gain unprecedented visibility into your organization's security posture through customizable dashboards & reports

Features:

- 24/7 real-time monitoring, alerting & analysis by certified security analysts
- Integrated business intelligence & analytics to make better business decisions
- Asset classification & reporting
- Threat intelligence
- Flexible & customizable reporting
- Easy integration with existing workflow products
- Pre-built security & compliance reports

EQ even goes to the dark side and beyond to protect you



Dark Web Monitoring

Security research has shown that 60% of passwords are reused, causing serious risk of account takeovers. To complement the managed SIEM service, EQ monitors the Dark Web for data attributed to you that could indicate an incident that requires action. We secure your accounts and data continuously scanning billions of records and files for hacked credentials. Teams are notified when passwords have been exposed so reset measures can be taken.

Additionally, should your organization become compromised, EQ can facilitate access to cyber forensics, legal and even public relations help to respond appropriately.



24/7 Breach Response

Clients have 24/7 access to report suspected incidents (from any source) and receive concierge service to connect to cyber forensics, legal and even public relations help to respond appropriately.



Cyber Insurance Coverage

We back up our Incident Response services with a cyber insurance policy to cover initial response costs with no deductible. This coverage is available in various amounts, and can be layered with existing policies to cover deductible or excluded costs, such as regulatory fines, penalties, or notification costs.



Equilibrium IT Solutions, Inc.

5559 North Elston Ave. | Chicago, IL 60630
www.EQinc.com | 773-205-0200 | 877-SUP-24X7

