COMPLETE COMPUTERS

# Network Security through 24/7
## Cyber-Threat Monitoring and Response

**Introducing 24 X 7 X 365 Cyber-threat monitoring and response services from Complete Computers**

- 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 absorb these issues, the average small business closes their doors within 6 months of a cyber-security incident. What's worse, a vast majority of these breaches were active for months or years – and evidence of a compromise was there all along had a security expert been looking for it.

**Your business doesn't have to be a victim. There is a solution!**

Let skilled security experts keep watch over the activity on your network. By applying cutting-edge 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 minute but suspicious irregularities.

**Human expertise:** Every security event identified by Complete Computers 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 Security Operations Center (SOC)

**Security Response:** Complete Computers will provide threat
mitigation and remediation procedures using industry best practices either remotely or on-site to ensure business continuity.

**Status Reporting:** Complete Computers can offer a view of the number and type of threats your network is facing.

# The Complete Computers Security Operations Center

**Important for your business:**

Cyber-threat monitoring and detection are the cornerstones of an effective IT security strategy. Collecting the right data, parsing it and analyzing it into manageable and useful pieces of information is a tremendously complex task. Fortunately there is automated technology that makes the collection and normalization much easier, but the analysis is only effective when experienced and skilled security professionals are able to contribute their knowledge into the system.

***Call us today for a free quote on 24/7 cyber-threat monitoring.***
**(707) 400-6154**

Complete Computers has combined cloud based technology, highly-trained security experts and our security response team who will 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 is employed to sort through the millions of events through a complex process is called correlation.

**Experience:** The correlation rules used by Complete Computers have been developed and are constantly being updated and improved to ensure new threats are identified.

**Intelligence:** Discovered security alerts are escalated to a team of trained experts who perform a deep triage process by means of human inspection. This "eye's on" scrutiny definitively pinpoints security incidents which will require some kind of attention to remediate.

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

## Detects 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.

COMPLETE COMPUTERS