



Network Security Monitoring Services

IAC SecureTech's **Network Security Monitoring** service serves as our client's principal bulwark and support in mitigating the risk of intrusion, while also providing improved reliability and availability of their networks and business processes. Unlike other security solutions, IAC SecureTech's Network Security Monitoring is designed to *support your business processes, not make your processes conform to our solution.*

IAC SecureTech's Network Security Monitoring is equivalent to a 24/7/365 network security monitoring staff and security help desk so our clients are able to reduce future need to hire security and network personnel. We report to our clients and provide alerts and advisories in order to support them against the multiplicity of network threats. While existing anti-virus may stop attacks through e-mail, many users bring both viruses and worms into the network on laptops and through downloading files. IAC Secure Tech's Network Security Monitoring mitigates network risk and improves systems availability.

MONITORING/INTRUSION DETECTION

IAC SecureTech monitors its clients alerts at a Central Monitoring Station and reports immediately to designated contacts. This 24/7/365 monitoring approach constantly updates and maintains your security layers as new threats develop. IAC SecureTech maintains all hardware as well as the underlying operating system — we won't be coming back again and again to charge for hardware and software upgrades.

INCIDENT RESPONSE & ACTION

In the event of an attack, virus or other security breach, IAC SecureTech acts as your incident response team in order to quickly mitigate any damage and ensure that any regulatory and legal vulnerabilities are contained and reported. Upon detection of a suspicious event, IAC SecureTech contacts the designated client contact and notifies them of all information that we know concerning the event, then advises on courses of action.

PATCH MANAGEMENT AND SYSTEM UPGRADES

The Network Security Monitoring Service includes support in maintaining infrastructure system upgrades and patches. Our team constantly evaluates real and potential threats which

may impact our client's networks. Based on our research and evaluation we notify our clients of patches and upgrades which must be implemented and the associated risks. The service process includes:

- Evaluation of vulnerabilities
- Identification of potential threats in the wild
- Analysis of patches released by vendors
- Strategy and distribution plan for patch/upgrade rollout.
- Support with automation of patch/upgrade rollout

NETWORK SECURITY MONITORING SCOPE

- 24/7/365 support of on-duty security technicians
- Network attacks (both internal and external)
- Spam and virus filtering
- Web application attacks
- DoS (Denial of Service) attempts
- Policy violations
- Worm/Trojan/Spyware activity
- Web content
- 24/7/365 Network and Server monitoring
- Bandwidth monitoring (notification if bandwidth drops or exceeds thresholds plus notification of what is causing the problem)
- Heartbeat (Up time)
- Server Events
- Hardening of critical servers
- Patch Management support (including time saving scripts)
- Network evaluation to identify systems not yet patched.
- Incident Response
- Assigned "handler" (single point of contact)
- Multilayered
- Customized Firewall Management & Security portal
- Incident Response
- Real-time Server Log Auditing and Archiving

