CYBER PATROL

IT SECURITY THREAT MANAGEMENT AS A SERVICE

24x7 Monitoring, Threat Management and Quarterly Vulnerability Scans together in one simple service.

Safer data means safer business

In order to defend Australian business networks and devices against malicious threats, abnormal user behaviour and data breaches, Huon IT's Security Operations Centre (SOC) operates continuously 24 hours a day, 7 days a week, 365 days a year.

Our industry-best technology collects events and logs from your network devices and correlates them in our cloud-based Security Incident & Event Management (SIEM) infrastructure, including real time process checks against intelligent rules.

Any alerts detected are evaluated by our security experts, who create actionable incidents for swift remediation.

Did you know?

Most companies take **OVER SIX MONTHS** to detect data breaches giving cybercriminals plenty of time to conduct surveillance, steal data and spy upon victim companies to maximise damage.

(Ponemon Institute 2016)

Daily 24x7 monitoring
via our world class Security Incident & Event Management (SIEM) system.

Quarterly vulnerability scan & report
to identify any new potential weaknesses.

Expert analysis by real people
reviewing and validating issues, around the clock.

Licensed per device
for an affordable monthly fee.

Rapid response
to address any threats as they emerge.

Full incident remediation

OR

Escalation only levels of service available

Identify & address these (& more) threats:

- Port scans, host scans, denied scans, sudden change of traffic between certain IPs and 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 controllers
- Account lockouts, password scans and unusual logon failures
- Rogue endpoints, wireless access points
- Botnets, mail viruses, worms, DDOS and other "zero day" malware identified by cross-correlating DNS, DHCP, web proxy logs and flow traffic
- Abnormalities in web server and database access.

Quarterly Vulnerability Scans

In addition to day-to-day monitoring, once per quarter Huon IT's Security Team will run a vulnerability scan across your network to detect:

- Any new, unaddressed assets
- Un-credentialed vulnerability discovery
- System hardening and missing patches
- Threat auditing (to detect viruses, malware backdoors, host communicating with botnet infected systems, web services linking to malicious content)

These findings are assigned risk scores (Critical, High, Medium, Low & Info) and prioritised accordingly.

Compliance Benefits:

- Full log management: long term storage, archival & retrieval
- Raw log storage, archival and retrieval
- Event log correlation and threat intelligence
- Log and alert analysis
- 7-year log retention policy
- InfoSec incident report
- Executive summary and compliance report
- SOC2 certified

Prevention is ideal, but detection and quick response is essential.

Contact Huon IT today to speak with an expert to learn how Huon IT's Security Operations Centre can help protect your business.

SYDNEY – MELBOURNE
P: 1300 HUON IT (4866 48)
E: info@huonit.com.au
www.huonit.com.au

huonit