What Cyber Responsibilities Does RoboShadow Cover?

Cyber Heal AutoFix Vulnerabilities

- Update over 7000+ Applications via WinGet
- Uninstall unwanted or insecure applications
- Manually update via MSIs / EXEs
- Change Cyber Benchmark configuration
- Patch Windows Updates automatically
- Enable Firewall and Anti-Ransomware
- Integrated fully with your PSA system

External Scanner :

- Scan external IP addresses for issues
- Scan websites for vulnerabilities
- Reconcile with Shodan (Hacker search engine)
- Scan for insecure SSL certificates
- Discover additional domains

RoboGuard:

- Continuously scan internal & external networks alongside your devices
- Real-time alerts via email or automated tickets log in your PSA or Servicedesk for vulnerabilities found
- Daily digest reports of new items detected across the attack surface

Intune Integration : Roll Out via Intune in One Click

- One-Click sync with Intune data.
- One-Click rollout the RoboShadow agent via Intune on all your devices.
- Receive Intune coverage reports and analyse risky sign-in data.

Device Vulnerabilities:

- Identify and remediate vulnerabilities
- Ensure laptops are encrypted with BitLocker
- Ensure AV is updated and enabled
- Ensure the operating system is updated

Antivirus Management :

- Verify AV is enabled and protecting
- Verify AV is updated with latest signatures
- Discover actionable defender alerts
- Report on Defender firewall
- Report on Defender anti-ransomware

OS Update Oversight :

- Identify and apply all critical OS and security updates
- Determine if a system reboot is required to complete updates
- Identify available driver updates for installation

Device Encryption : Is Your Estate Correctly Encrypted?

- Detect laptops lacking full-disk encryption.
- Identify open or insecure network folder shares
- Detect usage of unencrypted USB storage devices

RoboGuard: Continuous Vulnerability Scanning

- Continuously scan internal & external networks alongside your devices
- Real-time alerts via email or automated tickets log in your PSA or Servicedesk for vulnerabilities
- Daily digest reports of new items detected across the attack surface

365 MFA Sync: Keep on top of Multi Factor Authentication

- Identify user accounts without Multi-Factor Authentication (MFA) enabled
- Detect inactive or redundant user accounts eligible for deactivation
- Audit and monitor Microsoft 365 global administrator accounts
- Identify external guest users with access to Microsoft 365 resources

Windows Defender Sync : Pull in Golden Vulnerability Data from Defender

- Centrally managing device vulnerabilities from Defender and Microsoft 365
- Logging PSA or Servicedesk tickets based on your Microsoft Defender data
- Making real use of your investment into 365 Business Premium by including Tier-1 Defender vulnerability data

Cyber Benchmarks: Centrally Keep Tabs on Your Security Benchmarks

- Audit system for unsecure or deprecated protocol configurations (e.g., SMB1, TLS settings)
- Identify unauthorised or anomalous local administrator accounts across systems.
- Password policy audit

PSA / Ticket Integration: Actionable Insights Through Ticketing

- Alert you of any new vulnerabilities directly into your Servicedesk or PSA system
- Reduce noise by ensuring only relevant alerts are sent into your ticketing system
- Provide actionable insights and track accountability over updates through tickets

Compliance Exports: How do you Prove your Cyber Posture to the World ?

RoboShadow has a compliance engine built within the platform, allowing you to export evidence data for a whole host of cyber governance frameworks including but not limited to:

- Cyber Essentials (UK)
- Essential 8 (Australia)
- NIST (US)
- SOC 2 (Worldwide)
- ISO 27001 (Worldwide)
- HIPPA (US)

Advanced Cyber Reporting: Getting neat Cybersecurity Reports

- Generate board-level management summary
- Provide device-level vulnerability reports
- Deliver prioritised risk insights with action remediation plan

AI Pen Test: In the Middle of a Vulnerability Assessment and a Penetration Test

- Define the scope and toolset used to conduct the assessment
- Management overview and overall scoring.
- Vulnerability and exploit information discovered during the test
- Actionable next steps and strategy suggestions

Book A Demo Today!

Email us at hello@roboshadow.com