Redpoint
CYBERSECURITY

USE CASE

HEALTHCARE vCISO

RISK/CHALLENGE:

A large healthcare organization was faced with impacts from a network security breach and the departure of their current CISO.

- Client required assistance with addressing remediation initiatives and managing the cyber security program.
- Redpoint Cyber's CISO worked in tandem with the client's leadership team, providing strategy, guidance and assisting with developing cyber and infrastructure requirements to mature the client's overall security posture.
- This included ensuring that all attack surfaces are covered, maintaining a risk register to track vulnerabilities, strategizing and developing the security program, ensuring alignment of security initiatives with IT and client objectives.

TOOLS & TECHNIQUES:

- Developed a Risk Register to track vulnerabilities, ensuring ownership and accountability.
- Implemented a formal policy management and governance process to define requirements, determined feasibility to implement, identify gaps/risks/exceptions and prioritization.
- Refined Identify & Access Management (IAM), Asset and Patch Management policies, Disaster Recovery and Incident Response processes.
- Developed a cyber/business security plan, ensuring IT project alignment (e.g., budgeted, prioritization, planning).
- Collaborated with IT to enhance patch, asset management processes and producing quality reporting.
- Defined requirements for the client's overall onboarding/off-boarding process, incorporating more comprehensive asset tracking and integration with respective HR, business and IT systems.

- Developed on updated policies around endpoint detection and response, Reduced false positives in the alerting process and created standardized baselines for all operating systems. Created approved application policies and data spill handling policies to reduce unauthorized access and movement of data outside of secure storage areas.
- Implemented intune to provide unified endpoint management of both corporate and BYOD equipment.
- Created remote user policies to monitor all VPN users and force routine endpoint check-ins to monitor endpoint health.

OUTCOMES:

- Successful remediation of HIPAA OCR audit findings pertaining to patch and asset management.
- Board and executive leadership approval of the cyber/business security plan, solidifying the clients cyber security roadmap.
- Cleaned up active directory policies, reduction of the number of privileged accounts, reducing risk profile.
- More efficient, repeatable patch management, reducing the percentage of out-of-date patched systems by 35%.
- A 45% reduction of known vulnerabilities, improving the client's overall maturity posture.