XPATTERNS SCANS AND SAFEGUARDS HEALTHCARE DATA

Situation Overview

One of the largest healthcare organizations in the U.S. needed to quickly deploy a national cyber solution that would enable them to protect their patients and their brand with a prediction, protection, detection and remediation platform. Their goal was to fuse their national network and cyber operations through a highly robust cyber security solution.

MAJOR HOSPITAL TURNS TO XPATTERNS FOR CYBER SECURITY

xPatterns provided a unified situational awareness platform that would deliver comprehensive security intelligence while providing real-time information to their newly-formed Security Operations Center. xPatterns was strategically configured to operate as a tier 0 analytic hub with universal spokes, helping them identify, prioritize and respond to modern security threats.

The data presented to xPatterns was:

1. PCAP
2. Wide Area Network Flow
3. User Reporting and Trouble Tickets
4. Active Directory Data
5. Firewall Activity
6. Microsoft Service Center Configuration Manager and Patch Management
7. ITSM/Service Management
8. Device & Facilities Data
9. Network Port Data
10. DHCP Management
11. External IP Space
12. Security Information and Event Management (SIEM) Data

xPatterns was designed to rapidly surface undetectable events, prioritize signatures and forecast unmatched and unmasked IP addresses. Once identified, the xPatterns platform directs insights in real-time to an SIEM tool for rapid payload inspection through its playback and transparency capabilities.

By “canalizing” the threat into a repeatable forensic capability, xPatterns now prioritizes and remediates events, whereas before, these events had gone undetected or were lost due to massive amounts of chaotic alerts.

Situational Outcome

xPatterns successfully deployed a massive tier 0 hub-spoke solution for this national healthcare organization with the ability to graduate a level of defense at a fraction of the cost. xPatterns enhanced existing point solutions, embraced and extended these appliances through an effective tier 0 integration methodology. This extended the end of life for these point solutions, while turning them into active sensors for the effective defense of their patients and their brand.

xPatterns for Cyber for this major healthcare organization yielded:

- Effective time management and rapid forensic analysis of significant threats, rather than an unsustainable laundry list of incidents needing to be reviewed.
- A fly-away team that was able to capture PCAP locally for analysis at the hub to prioritize a national rollout strategy, while reducing costs for a healthcare “extraprise” rollout.
- An effective threat intelligence team working deep in dark web, zone fields and social media to provide “left of bang” early warning and threat forecasting.
- The establishment of a global cyber dashboard that included:
  - Strong authentication and gradient trust model for privileged users and access policies
  - Unified critical vulnerability and patch management strategy
  - Effective scanning and indicators of compromise response strategy
  - Consistent measurement of performance or overall network effectiveness that analyzes availability, performance and quality in order to generate a cyber-scorecard grading optimal performance
  - Global high-value asset list that ensured proactive security practice and focused active and passive defense postures
  - Monthly privileged access reviews to reduce the impact of user error and insider threat
  - Daily above-the-proxy incident reviews for increased threat intelligence, situational awareness and policy review