CUSTOMER CASE STUDY

Hospital District Uses ThreatWatch Response & Remediation Capabilities to Detect Ransomware

The Breach

SUN-MON Security Team alerted that Ivanti App Control blocked unknown file execution attempts. No additional information could be provided.

TUES ThreatWatch RAR was used to triage the network and found active "Cobalt Strike" beachheads on three key servers. The attackers achieved FULL domain takeover and were caught actively staging more ransomware.

TUES ThreatWatch RAR support team sent the info to IR partner who reviewed the data and made initial response recommendations.

The Result

The root cause was discovered to be a medical doctor with overly-elated privileges that was breached on Sunday. The IR team recommended blocking IPs at firewalls, disabling doctor's account, and resetting admin accounts at the domain controller. ThreatWatch RAR removed ransomware from 1000s of systems, killed Cobalt Strike injections, and deleted shadow copy hiding places. After continuous monitoring, there was no new attacker activity seen.

Quick Facts

Level 1 Trauma Center and Magnet Hospital

Headquarters: Austin, Texas

Employees: 7000+

IT Budget: $1.7+ B

Existing Defenses

Network: ForcePoint Web Gateways, Cisco Firewalls

AV/Endpoint: Cisco AMP Endpoint Security, Defender, Ivanti App Control

Monitoring Service: Optiv Monitoring (Not ThreatWatch) with ThreatWatch Response & Remediation service