Industry

LEADING HEALTH SERVICES PROVIDER

26 Branches

CASE STUDY

This case study explains the successful implementation of LinkShadow intelligent NDR technology, Security Information and Event Management (SIEM) solution, and Security Operations Center (SOC) monitoring services across 25 hospitals under a leading Group of Hospitals. The deployment aimed to create a comprehensive cybersecurity ecosystem that proactively detects and mitigates advanced threats, enhances incident response capabilities, and fortifies the protection of sensitive healthcare data. Through a collaborative effort, the Customer significantly bolstered their security posture and ensured the continuity of critical healthcare operations.

OBJECTIVES

The key objectives of the iNDR with SIEM and SOC Monitoring Services deployment were as follows:

- Comprehensive Threat Detection: Implement an advanced XDR solution to detect and analyze threats across all attack vectors and endpoints.
- Centralized Security Management: Deploy a SIEM solution to collect, correlate, and analyze security event logs from all 25 hospitals in a centralized platform.
- Real-time Monitoring and Incident Response: Utilize SOC monitoring services to provide monitoring and rapid incident response to detect and neutralize potential threats promptly.
- Threat Intelligence Integration: Integrate threat intelligence feeds with the XDR and SIEM solutions to stay updated on emerging threats and attack patterns.
- Compliance and Reporting: Ensure compliance with healthcare industry regulations (e.g., HIPAA) and produce comprehensive reports for audits and assessments.
- Enhanced Incident Response: Establish well-defined incident response procedures, workflows, and escalation paths to ensure a swift and effective response to security incidents. Integration with a Security Operations Center (SOC) or managed security service provider enhances incident investigation and resolution.
- Incident Analysis and Reporting: Utilize the SIEM platform and monitoring services to conduct in-depth incident analysis, generating comprehensive reports for internal analysis, audits, and regulatory compliance requirements.

SOLUTION

- The cybersecurity team from the Customer collaborated with LinkShadow's experts to devise a comprehensive implementation plan, addressing the unique security needs and challenges faced by each hospital.
- The deployment of intelligent NDR and SIEM technologies took place in a phased manner, with tailored configurations for each hospital's network infrastructure and security ecosystem.
- It provided real-time monitoring of activities and detecting anomalies. Additionally, network traffic analysis was enabled to identify potential threats.
- The SIEM platform was integrated into the existing security architecture to gather and correlate security event logs from all hospitals. Customized correlation rules were defined to prioritize critical security events.
- LinkShadow's SOC monitoring services were engaged to provide round-the-clock monitoring of security events, leveraging the expertise of skilled analysts to detect and respond to incidents swiftly.
- IT and security staff at each hospital underwent training on the iNDR, SIEM, and SOC technologies, ensuring efficient utilization of the deployed solutions and seamless collaboration with the SOC team.

CONCLUSION

The successful implementation of iNDR with SIEM and SOC monitoring services from LinkShadow across 25 hospitals under the customer significantly enhanced their cybersecurity resilience. By adopting a proactive approach to threat detection, bolstering incident response capabilities, and ensuring compliance with industry regulations, the Hospitals demonstrated their commitment to safeguarding patient information and maintaining uninterrupted healthcare services. The collaboration with LinkShadow showcased the customer's dedication to staying ahead of evolving cyber threats and fortifying their position as a trusted healthcare provider.

BENEFITS

Advanced Threat Detection: AI Powered iNDR capabilities, combined with the SIEM correlation rules and SOC monitoring services, enabled the customer to detect and respond to advanced threats promptly, It uses machine learning algorithms to detect and correlate patterns indicative of advanced cyber threats.

Proactive Incident Response: With monitoring service by LinkShadow's SOC, potential security incidents were identified and mitigated proactively, reducing the impact of cyber threats on hospital operations.

Centralized Visibility and Reporting: The centralized SIEM platform provided real-time visibility into security events across all 25 hospitals, streamlining security operations and compliance reporting.

Compliance Assurance: The comprehensive security measures and reporting capabilities ensured that the customer-maintained compliance with healthcare industry regulations and internal security policies.

Resource Optimization: By automating routine security tasks, AI-powered SIEM frees up the hospital's IT and security staff from manual activities, allowing them to focus on strategic security initiatives, threat hunting, and incident response.