SOC CASE STUDY

Shielding Success: Unveiling 24x7servermanagement' Tailored SOC Triumph

EXPERTS IN

EXECUTIVE SUMMARY

Discover how 24x7servermanagement revolutionized security for a diverse organization offering Software Development and Infrastructure as a Service (IaaS) Hosting. By introducing a comprehensive Security Operations Centre (SOC), 24x7servermanagement empowered the client to surmount challenges posed by malware infections, phishing attacks, and unauthorized access. Explore how our customized SOC approach transformed threat detection, response, and overall cybersecurity, elevating both business protection and reputation.

THE CHALLENGE

The client, a dynamic entity bridging Software Development and IaaS Hosting, grappled with multifaceted challenges:

- Critical Security Risks: Combatting the looming dangers of malware infections, phishing attacks, and unauthorized access that posed substantial threats to the organization's integrity and reputation.
- Ecosystem Complexity: Managing security across a landscape encompassing cloud services, on-premises infrastructure, diverse applications, and software, proved a daunting task.
- Seamless VAPT: Ensuring robust Vulnerability Assessment and Penetration Testing (VAPT) while safeguarding operational workflows from disruptions.

OUR SOLUTIONS

24x7servermanagement devised a tailor-made SOC strategy, reshaping the organization's cybersecurity landscape:

AT A GLANCE

Challenges

- Multifaceted Security Risks
- Ecosystem Complexity
- Seamless VAPT
- 24x7 Monitoring Demand

Benefits

- Comprehensive Security
- Unified Protection
- Efficient VAPT
- Swift Threat Response

"Our expert team enabled us to navigate complex security challenges, from malware threats to phishing attacks, safeguarding our reputation and operations. We've achieved unparalleled peace of mind and efficiency in threat detection and response"

- Stellar K.

- SIEM Integration: Deploying a Security Information and Event Management (SIEM) system centralized security events and issues, streamlining security workflows and detecting vulnerabilities and threat intelligence.
- Wazuh is an agent-based SIEM solution using which the vulnerabilities are detected on the assets where the Wazuh agent is installed. Wazuh SIEM compares the incoming traffic with known threat indicators and improves the accuracy of threat detection.
- EDR Implementation: Bitdefender an EDR is used to continuously detect and respond to cyber threats for end-point devices. Through Bitdefender, we detect, monitor, and respond to cyber threats coming at endpoints. It provides visibility at an end-point level which helps to mitigate advanced threats.
- Seamless VAPT: OpenVAS is used to perform vulnerability assessment and management. Using OpenVAS we detect the vulnerabilities with up-to-date CVE records. Vulnerability assessment and Penetration is carried out to identify security gaps and mitigation. It enables the SOC to view potential threats, identify gaps in security, safeguard the business, and protect organization from malicious attacks.
- 24x7 Centralized Ticketing: Implementing a ticketing system for generating, tracking, and managing alerts and updates, enabling rapid and efficient SOC response.

TECHNOLOGY STACK

- SIEM Integration(Wazuh): Centralized analysis of security events with SIEM, enabling effective security workflows, vulnerability detection, and threat intelligence.
- EDR Empowerment(Bitdefender): Endpoint Detection and Response (EDR) solutions providing continuous threat monitoring, response, and visibility at the endpoint level.
- Comprehensive VAPT(OpenVAS): Robust Vulnerability Assessment and Penetration Testing (VAPT) to identify gaps in security, safeguard the organization, and mitigate advanced threats.
- Advanced Threat Intelligence: Leveraging cutting-edge threat intelligence to anticipate and mitigate emerging security risks.
- Security Orchestration and Automation: Implementing SOAR solutions to streamline and automate incident response, enhancing efficiency.
- 24x7 Agile Ticketing System: Centralized ticketing system for rapid alert generation, tracking, and management, expediting SOC response.

THE ADVANTAGES

- Enhanced Cybersecurity: A fortified security landscape combats malware, phishing, and unauthorized access risks, preserving both business integrity and reputation.
- Unified Ecosystem Protection: Seamless management of security across cloud services, on-premises infrastructure, applications, and software, mitigating complexities.
- VAPT Agility: Robust Vulnerability Assessment and Penetration Testing coexist with uninterrupted operational workflows, ensuring secure scalability.
- Advanced Threat Management: Cutting-edge threat intelligence anticipates and mitigates emerging security risks, bolstering proactive security.
- Efficient Incident Response: Security Orchestration and Automation streamlines and automates incident response, enhancing efficiency.
- Rapid Threat Response: Centralized SIEM, EDR, SOAR, and ticketing streamline threat detection, response, and mitigation, empowering SOC teams.

FOR MORE DETAILS, PLEASE CONTACT US

Our experts are ready to guide you through a transformative journey of comprehensive threat detection, response automation, and advanced cybersecurity.

CONTACT INFORMATION:

- Email: sales@24x7servermanagement.com
- Phone: +91-8484980596
- Website: www.24x7servermanagement.com

24x7 Server Management