CYBERCLAN™

Managed Security Services

Cyber threats never sleep—neither do we. Protect your organization 24/7 with our security operations center.

The Challenge

In today's fast-evolving threat landscape, partnering with a managed security services provider reduces the exposure your organization faces with escalating cybersecurity risks, stretched resources, and a reactive IT strategy.

Cybercriminals are relentless and operate around the clock. Let CyberClan watch over your organization and assets so you can focus on your business operations.

Our Solution

At CyberClan, we empower your security posture with our state-of-the-art Security Operations Center (SOC), providing 24/7 monitoring, swift threat detection, and expert response tailored to your needs. Our technology-agnostic framework offers unparalleled flexibility, while our globally managed detection and response services ensure your protection is unwavering, day and night.

Backed by industry-leading certifications—including CISSP, GCFA, GCFE, and GCIH—our experienced specialists are equipped to respond to critical threats in under 15 minutes. With CyberClan, you can rest assured knowing that your business is firmly safeguarded against evolving cyber threats.

Endpoint Detection and Response (EDR): Stay ahead of threats by continuously monitoring all endpoint activity and analyzing data in real-time while containing and quarantining potential dangers. Experience a reduction in alert fatigue by over 90%, with critical events escalated as necessary.

Threat Intelligence, Monitoring, and Hunting: Our proactive approach combines cutting-edge artificial intelligence with expert human oversight, allowing us to devise the best offensive strategies, uncover hidden intruders, and identify vulnerabilities and Indicators of Compromise (IOCs).

Security Information and Event Management (SIEM): Gain a holistic view of your entire hybrid enterprise—from on-premise to cloud—as we identify threats and automate responses, dramatically reducing downtime and accelerating threat response times.

24/7/365 Monitoring and Reporting: Our security framework aligns with leading standards, including NIST, CIS, ISO, and SOC2, ensuring you receive the highest level of protection.

User and Entity Behavior Analytics (UEBA): We provide detailed analytics to distinguish normal from abnormal activity, enabling targeted detection of IOCs.

Advanced Email Security: Protect your organization from sophisticated attacks that bypass conventional security measures with our automated, cloud-based email security solutions.

Continuous Vulnerability Management: Our Continuous Vulnerability Management service leverages advanced tools to provide in-depth visibility into the entire attack surface, identifying overlooked and unmanaged assets that pose potential risks.

Our global team of experts monitors activity across your systems, swiftly investigating any signs of malicious behavior. This proactive vigilance allows for prompt containment and detailed reporting, keeping you informed at every step.

Our Framework

Establish Protections: Identify the most effective security measures to ensure your investments yield maximum value.

Develop and Implement: Conduct thorough assessments to understand your environment, recommending customized safeguards based on your budget and risk profile.

Analyze and Respond: With deep knowledge of your systems, our SOC analysts differentiate normal behavior from anomalies, enabling rapid responses.

Take Action: Beyond automated responses from EDR tools, our SOC team actively investigates critical threats, alerting you within 15 minutes of detection.

Identify and Alert: Detect threat actor behaviors and create actionable alerts to mitigate compromised data, significantly shortening the time between identification and containment.

Customized Rules for Business Needs: These guidelines cater to your unique challenges and goals, providing relevant recommendations. By addressing your industry and operations, these tailored strategies create a framework for driving success and innovation.

Benefits

- Minimize overall system downtime.
- Leverage our extensive experience in recovery.
- Align with industry best practices.
- Enhance your internal IT teams with our resources.
- Gain insights and recommendations from our experts and CERT resources to fortify your security posture for the future.
- Minimize the requirement for client intervention by isolating all low priority incidents before they become an issue.

CYBERCLAN™

Incident Hotline
US/CA 1 800 762 3290
UK 0800 368 8731
AU 61 1800 413 128
response@cyberclan.com

General Inquiries
US/CA 1 855 685 5785
UK 0800 048 7360
info@cyberclan.com