COMPANY NAME	CUSTOMER TYPE	LOCATION
Undisclosed	Healthcare	United States

Case Study

Microsoft

Leading HealthCare Insurance Provider Leverages SDG and Microsoft to Automate Security Operations and Reduce Costs

CHALLENGE

Limited personnel and high alert volumes overwhelmed the SOC, delaying responses and increasing costs.

SOLUTION

SDG enhanced Microsoft Sentinel with automation, playbooks, real-time remediation, and optimized alert triage.

RESULT

90% reduction in analyst hours, faster response times, cost savings, and full threat visibility—leveraging current Microsoft investment

SUMMARY

Our client, a leading healthcare insurance provider, needed to ensure round-the-clock SOC monitoring and threat response but faced a critical shortage of personnel, making continuous security coverage a challenge. With an overwhelmed team struggling to manage incidents, the client sought an efficient, cost-effective solution. SDG implemented an unmanned SOC powered by Microsoft Sentinel, leveraging automation to streamline security operations. This humanless SOC zeroed analyst workload in off business hours, improved incident response time, and optimized operational costs, allowing the security team to focus on complex threats while maintaining 24/7 security monitoring.

IN DEPTH: CHALLENGES

The client faced a persistent security coverage gap during off-business hours. Due to staffing constraints and high alert volume. Their Microsoft Sentinel-based SOC frequently failed to meet SLAs for incident triage after-hours. Analyst burnout, slow remediation times, and excessive managed service costs forced leadership to re-evaluate their operating model.

- Analysts spent 80+ hours/month triaging low-value alerts during evenings and weekends.
- 40% of events went unreviewed until the next business day.
- At least one vendor tool removed for duplicating effort with overlapping alert telemetry.
- Security operations cost $100K+ annually in after-hours labor alone.

SOLUTION

SDG enhanced the client's existing Microsoft Sentinel SOC by:

- Streamlining data ingestion to reduce false positives and ensure only relevant security events were visible in Sentinel.
- Reviewed and updated existing integrations for optimal functionality.
- Developed automated workflows for incident ticketing to expedite response times.
- Refined existing automation rules to enhance accuracy and effectiveness.
- Integrated external threat intelligence feeds to enhance Sentinel's detection capabilities.
- Improved SIEM analytic rules to provide better alerting and event correlation.
- Scheduled automated reports based on discussions with the client.
- Developed playbooks for Automated URL-based threats, endpoint isolation, and login anomaly detection, etc. for real-time remediation.
- Integrated third-party applications and systems for abnormal behavior detection and automated actions.
- Optimized alert triage, log ingestion, and data retention for improved efficiency.
- Enabled real-time monitoring dashboards for better SOC insights and reduced manual intervention.

By automating repetitive tasks and streamlining security workflows, SDG's humanless SOC allowed the client's security team to focus on critical threats during business hours while maintaining 24/7 coverage with unmanned operations during off-business hours.

RESULTS

After implementing SDG's automated, unmanned SOC, the client achieved:

- 90% reduction in required analyst hours, cutting analyst costs significantly.
- 10-second response time and 5-minute resolution, ensuring near-instant incident remediation.
- Lower operational costs, shifting from expensive manual operations to an automated $7/month model.
- Improved security efficiency, leveraging real-time monitoring and AI-driven remediation.
- 100% log visibility, eliminating blind spots and improving threat detection.

CONCLUSION

By partnering with SDG and Microsoft, the client successfully transitioned to a cost-efficient, fully automated security model, ensuring 24/7 protection with minimal human intervention. The integration of automation into their existing Microsoft Sentinel SOC reduced costs, improved response times, and enhanced security posture. As a result, the client's SOC team could dedicate its resources to proactive threat hunting, ensuring a more resilient, cost-effective security infrastructure.

ABOUT SDG

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

SDG
75 North Water Street
Norwalk, CT 06854
203.866.8886
sdgc.com

Contact Us: solutions@sdgc.com

© Copyright 2025. SDG Corporation. All rights reserved.