NuSummit®
Cybersecurity

Customer Stories

Managed Detection & Response

cybersecurity.nusummit.com

Reducing cyber threats with Azure Sentinel SIEM and SOAR

The client is an online platform provider of financial products and services such as personal, unsecured, and instalment loans and credit cards. They connect borrowers with lenders to help them get the best deal possible.

Custom and built-in **rule-based alert decision**

Explored various log ingestion sources like firewall and Antivirus

Advanced **Machine Learning (ML)** for anomaly and algorithm-based alert detection

Framework for automated tracking and monitoring

AI-based threat intelligence for attack mitigation

LEADING ONLINE FINANCIAL SERVICE PROVIDER

Challenges

- Integrating SIEM and SOAR
- Swift receipt of real-time alerts
- Implementing advanced threat protection for endpoints
- Overseeing Azure Sentinel operations
- Identifying and addressing threats within the organization and finding opportunities for improvement
- Detecting and addressing suspicious activities within the environment
- Strengthening defense against potential threats to the organization
- Accelerating threat response with email integration

Solution

- Provided a Managed Detection and Response (MDR) environment to empower the customer's business growth with maximum cybersecurity
- Microsoft Azure is providing SIEM solution through the SAAS-based model in addition to SOAR platform to automate repetitive tasks
- Set up necessary connections and automated processes to match specific needs
- Provided continuous support through our Managed Detection and Response (MDR) service to ensure persistent cybersecurity

Outcome

- Implemented Azure Sentinel SIEM and SOAR
- Detected threats from Firewalls, Switches, and Windows servers
- Automated email-based incident response with Azure Sentinal playbook

Transforming enterprise cybersecurity with a universal SIEM solution

The client is a leading chair manufacturer in North America with a legacy of over 25 years. The enterprise is known for their innovation, unparalleled build-to-order solutions, with industry-leading 2-day delivery times, and a strong focus on value. The industry leader owns a group of brands with award-winning and best-selling products.

40% reduction in SIEM implementation time through device log compatibility

100% SIEM coverage for both on-premises and cloud infrastructure

Protection of IT infrastructure and applications

24x7 monitoring for capturing endpoint activities

LEADING CHAIR MANUFACTURER

Challenges

- Lack of proactive threat monitoring
- High risk of reputation loss from compromised data
- Absence of a well-defined incident handling framework
- Limited to no critical use-cases for threat detecting and response
- Absence of in-depth investigations
- Lack of centralized log management and correlation

Solution

- Implemented 24x7 event monitoring and incident response for safeguarding over 100 critical components of the IT infrastructure
- Established an in-depth incident handling process and procedures tailored to address high, medium, and low severity incidents proactively
- Designed and deployed customized dashboards and Standard Operating Procedures (SOPs) aligned with the client's specific investigative needs
- Monitored and managed the Endpoint Detection and Response (EDR) solution
- Monitored and troubleshot error log sources from various devices, ensuring uninterrupted security

Outcome

- Implementation, administration, and monitoring of all critical devices
- 24x7 alert monitoring and incident response
- Detailed documentation of information related to incidents using W6 Incident Investigation process
- 30% reduction in potential costs associated with cyber incidents using to proactive threat detection and response measures
- Reduction in attack surface through identification of hidden threats using smart correlation rules

SOC management and device management services

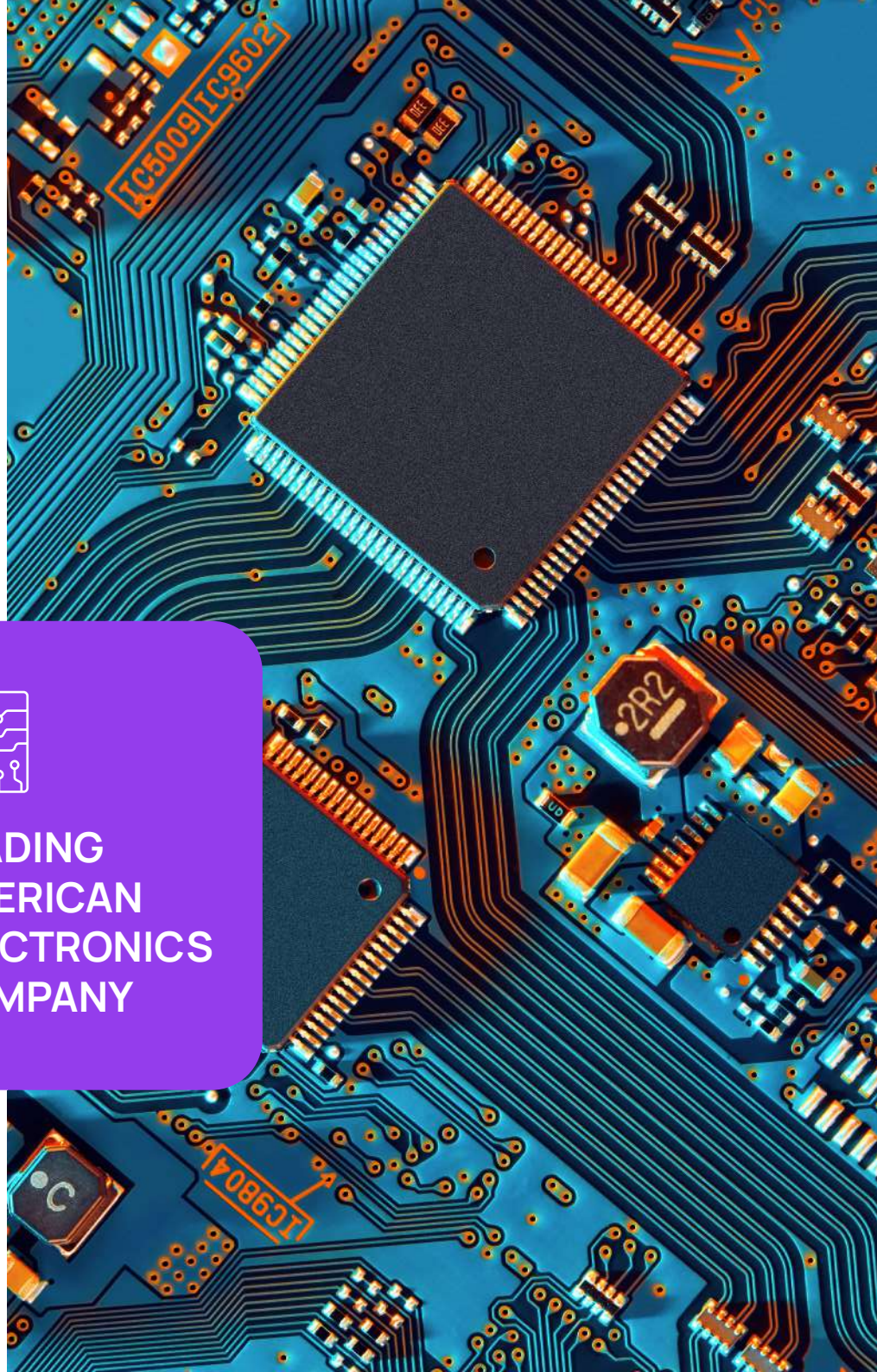
Leading American electronics company that develops, manufactures and supplies electronic components for a variety of industries including automotive, industrial, instrumentation, medical electronics, consumer equipment & portable electronics.

Automation of incident creation and improved response time

100% monitoring coverage using SIEM solution for on-prem and cloud infrastructure

70% effort reduction in detecting threat and related risks

LEADING AMERICAN ELECTRONICS COMPANY



Challenges

- SOAR implementation
- Monitoring on-prem SIEM and cloud devices
- Effective monitoring of all logs
- Identifying new threats
- Identifying suspicious activities within the environment
- Performing deep dive investigation on alerts and providing advanced recommendations and preventive measures

Solution

- CDC - Implemented and managed 24x7 SOC services for on-prem and cloud infrastructure using SIEM tool (1000 - EPS), servers – 150+
- Managed services to monitor NW/ Sec device and incident response
- Developed and monitored 70+ use cases as per MITRE ATT&CK Framework standards
- Automated incident notification using a playbook (SOAR) for immediate action on the incident
- Created of dashboard and workbooks for monitoring and tracking

Outcome

- Complete implementation, administration, and monitoring of all onboarded devices
- Continuous feedback and process improvement
- Adaptive learning for unknown threats
- Reduced false positive alerts through continuous use case monitoring
- Automated email notification playbook (SOAR) for incident notification
- Conducted multiple tabletop exercises to improve skills

Implementation and management of security solutions

The client is a USA-based world leader in subscription revenue management automation. Their automated platform enables easy price management, launch of new products, billing, and revenue collection. The platform allows quick measurement of customer activities for swift improvement in business management. They aim to centralize all customer knowledge into a collaborative platform.

Protection of critical applications

40% implementation and time reduction in SIEM

100% monitoring coverage using SIEM solution for on-prem and cloud infrastructure

Continuous monitoring to capture all endpoint activities

GLOBAL LEADER IN SUBSCRIPTION REVENUE MANAGEMENT

Challenges

- Proactive monitoring of all device logs
- Identifying new threats and suspicious activities within the environment
- Implementation of strong security measures on critical use cases
- To perform deep dive investigations required more visibility on the environment.
- Integration of critical devices and onboarding applications

Solution

- Implementation, administration, and monitoring of security solutions with Managed Security Services
- Monitoring the infrastructure using the SIEM tool (1500 - EPS), devices – 95+
- Creation of customized dashboards and SOP as per client requirements for investigation
- Proactively monitoring EDR and proxy solutions
- Continuously monitoring and performing troubleshooting on error log source devices

Outcome

- Implementation, administration, and monitoring of all the critical devices
- Reduced false positive alerts through continuous use case monitoring
- Used the W6 incident investigation process to cover all the detailed information related to the incident
- Improvement in SLA
- Removal of non-compliant devices from the environment through proactive monitoring of EDR and proxy solutions for non-reporting devices

Implementation and management of Azure Sentinel

The customer is a modern, hybrid consulting firm that builds custom AI applications for Fortune 500 and equivalent companies. Their well-rounded consulting model addresses gaps in conventional analytics service provider models and off-the-shelf products. They offer the collective advantages of customization of diverse problems.

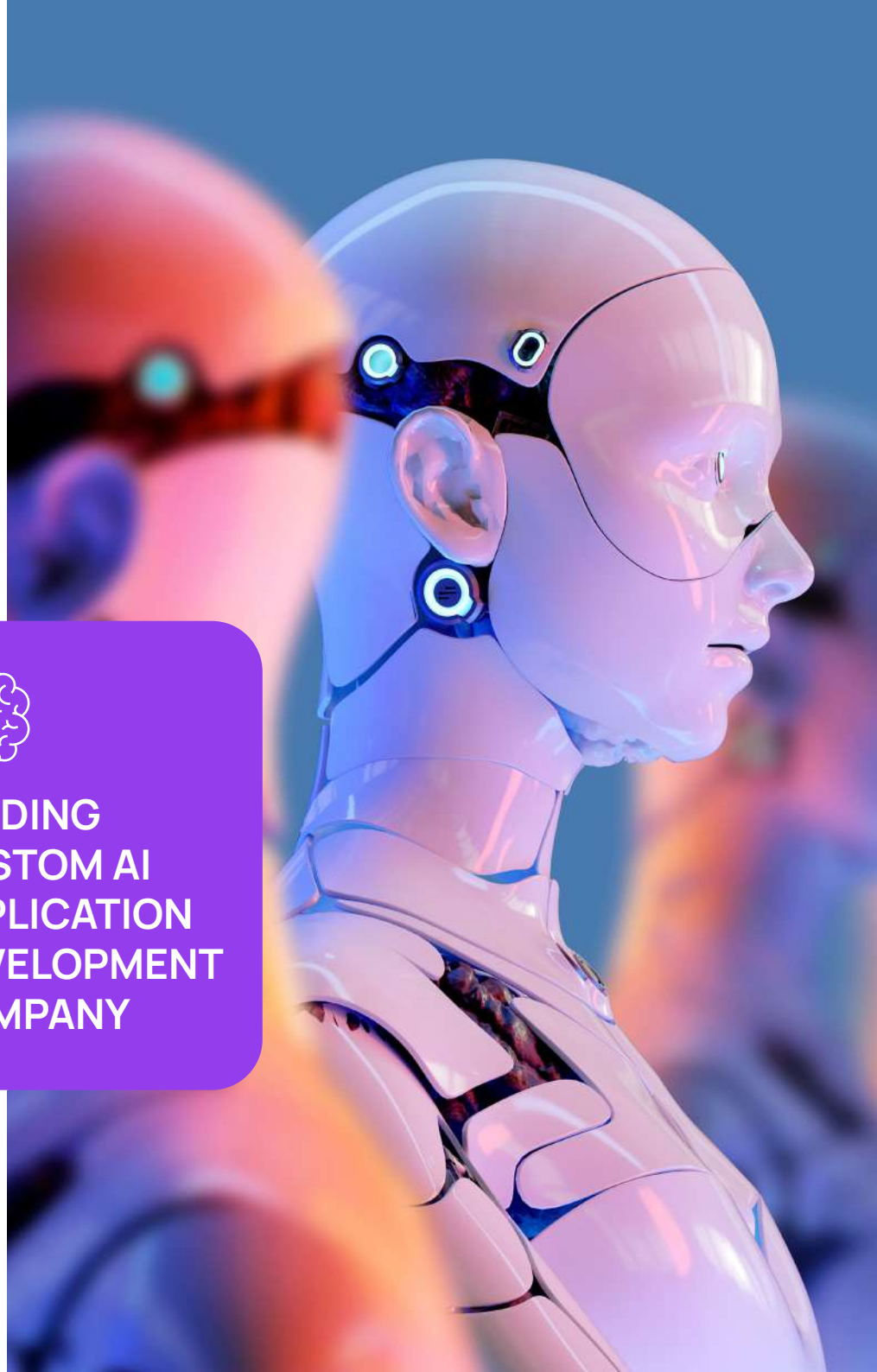
Created **200+** custom rules for alert detection

Leveraged Machine Learning (ML) to correlate events of two different log sources

Rule-based alert decision

Continuous monitoring to capture all endpoint activities

LEADING CUSTOM AI APPLICATION DEVELOPMENT COMPANY



Challenges

- Identify threats in the organization and ways to improve
- Identify suspicious activities within the ecosystem
- Perform process improvement for preventive measures
- Integrate their wide range of devices, like servers, network devices, security tools, and other Microsoft products available into Azure Sentinel
- Track the security alerts that get generated from the log sources
- Set up and manage the operations of Azure Sentinel

Solution

- Delivered an MDR environment to scale the business with maximum cyber assurance. Microsoft is providing SIEM solutions through the SAAS-based model in addition to SOAR platform to automate a lot of repetitive tasks
- Created all the connections from various log sources to Azure Sentinel and ingested the data into Sentinel
- 24*7 monitoring of Azure Sentinel to detect and alert if any incident occurs
- Provided continuous support in the monitoring phase, and in adding new use cases and fine-tuning old ones

Outcome

- Successful implementation of Azure Sentinel
- Threat detection from various data sources like Firewalls, Azure AD , Windows servers, etc.
- Incident response automation using Azure Sentinel

Improving security with Azure Sentinel SIEM and SOAR

The customer is a leading global provider of managed services, business process management, and advanced technology solutions for organizations aiming for improved operational efficiency, flexibility, and cost reduction. Their offerings encompass network access control, mobile security, data analytics, business process mangement, and consulting.

Explored various log ingestion sources like firewalls and Windows server

Advanced machine learning for anomaly and algorithm-based alert detection

Rule-based alert decision for investigations with minimal false alarms

Framework for automated tracking and monitoring

LEADING TELECOMMUNICATION SOLUTION PROVIDER

Challenges

- Integrating diverse devices with Microsoft Sentinel
- Monitoring security alerts originating from various log sources
- Detecting threats within the organization and suggesting enhancements
- Spotting suspicious activities within the ecosystem
- Enhancing processes for preventive security measures

Solution

- Implemented a managed detection and response system for clients to boost their business growth while ensuring top-notch cybersecurity
- Utilized Microsoft's SIEM solutions via a SAAS-based model and SOAR platform to streamline and automate routine tasks
- Established essential connections and automated processes as required to enhance efficiency
- Offered ongoing support as part of our Managed Detection and Response (MDR) service, ensuring constant cybersecurity vigilance

Outcome

- Successful deployment of Microsoft Sentinel
- Effective threat detection across a wide range of data sources including Firewalls, Switches, Windows servers, etc.
- Optimized incident response through automation

Securing OT environment with security assessment

The client is a leading cement manufacturing company operating multiple manufacturing plants worldwide and boasting an installed capacity of 100 million tons per annum.

Complete view of the security posture through a **patented traffic analysis technology**

In-depth review of the OT network architecture

OT firewall review report with advisory on identified issues

LEADING CEMENT MANUFACTURER

Challenges

- Evaluating the existing security status of OT devices, infrastructure, and processes without disrupting plant operations
- Developing an effective OT security program to safeguard devices, infrastructure, and processes

Solution

- Leveraged IEC 62443/ISA 99 standards to conduct security assessments
- Identified security vulnerabilities within OT devices and the infrastructure like misconfigurations in the OT network and a lack of security policies and procedures
- Strengthened OT device and infrastructure security by promptly remediating identified vulnerabilities

Outcome

- A complete view of the security posture through a patented traffic analysis technology available on the OT security management platform
- Insights into identified risks, gaps, and recommendations for improvements through an in-depth review of the OT network architecture
- Report on the OT firewall review, complete with advisory on identified misconfigurations, overly configured rules, and access issues, along with recommendations for improvements

Success stories

Leading SaaS provider for subscription management

Managed Security Operations

Incident response, EDR and Firewall Management, yearly SOC maturity assessment and vulnerability management, cloud security management, UEBA, and SIEM engineering

---

World's second largest stock exchange

24*7 Security SOC operations

End-to-end management for all Cybersecurity solutions like Microsoft Defender Suite, N/W security solutions, etc.

Multi-channel digital and physical market-place

Managed Security Operations

Firewall management, EDR solution management, SIEM engineering including log sources integrations, use case finetuning, and automation

---

Managed security operations for American food processing and packing company

Consumption-based security

Protection of people, operations, systems on-premise and on the cloud, Cloud-based SIEM –Microsoft Sentinel, SOAR, UEBA, and endpoint devices management

Success stories

Leading B2B e-commerce marketplace

24*7 Managed Security Services

Setting up and managing security operations covering five countries.
Managing endpoint devices, cloud security management

Leading telecom Provider

Managed Security

24x7 SIEM monitoring and SOC Engineering, management of security systems, proactive hunting, and continuous security posture improvement

---

Smart city initiative in Asia

Threat Hunting

Manual and automated threat-hunting services using threat intelligence platforms.
Security device management and remediation services

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services. Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information,
visit us at **cybersecurity.nusummit.com** or
write to us at **cybersales@nusummit.com**

Cupertino I Dallas I Jersey City I Ottawa I Riyadh I Dubai
Mumbai I New Delhi I Bangalore