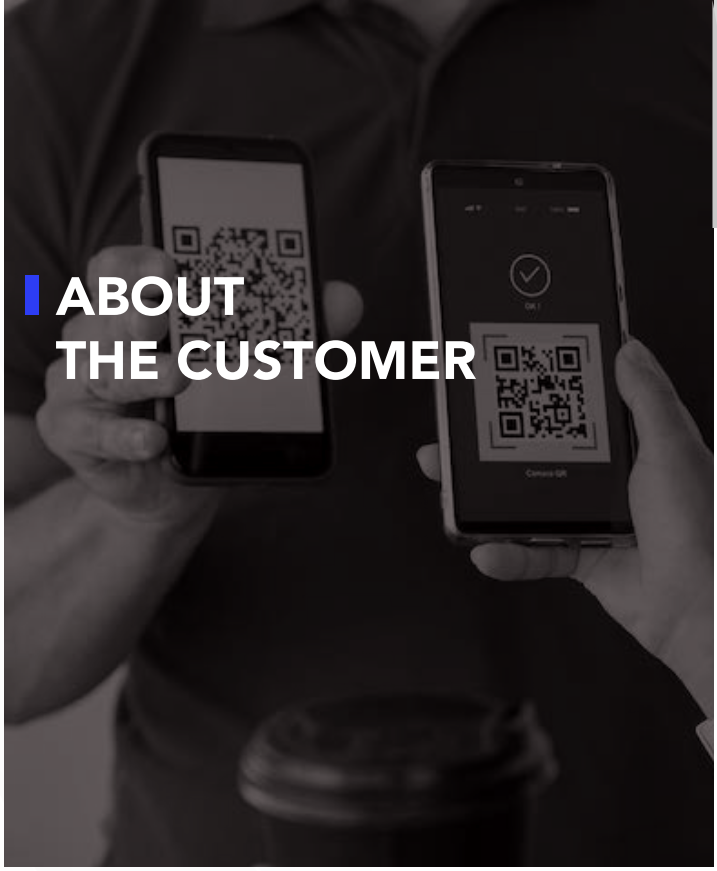
SISA

CUSTOMER SUCCESS STORY

SISA's cloud-based MXDR solution helps Paytia improve threat monitoring and incident response



ABOUT THE CUSTOMER

Paytia is a specialist payment service provider in the UK and USA, that allows businesses to take payment card details without putting their card data at risk over the phone. Through its ground-breaking Paytia Platform - a globally scalable cloud platform, it provides merchants of any size from entrepreneur to enterprise with a suite of highly secure phone-based card-payment solutions that can be set up in minutes.

THE CHALLENGE

Being a secure telephone payment product, Paytia's main goal is to enable businesses to give their customers the data protection they want and which regulations like PCI DSS and GDPR demand. This meant they needed to have a highly secure system while also being able to offer a flexible solution. However, they faced challenges on several fronts. To begin with, they required an effective event monitoring solution to detect internal and external threats. Secondly, as they were dealing with sensitive customer data, File Integrity Monitoring-based protection was essential. Thirdly, there was the need to monitor and secure all the cloud assets. Above all, they were looking for a flexible pricing model that could enable them to meet the dynamic needs of customers.

SOLUTION OFFERED BY SISA

Paytia was looking to partner with a Qualified Security Assessor (QSA) and approached SISA to help them secure their environment and enable compliance. The contract commenced with SISA first performing the PCI DSS certification audit and assisting the client in listing with VISA and Mastercard. In parallel, SISA also carried out ASV Scan and VAPT that covered architecture review, internal security assessments and validation. The client then expanded the scope of the contract to include SOC services for on-premises environment initially, and subsequently supporting AWS environment post-migration.

SISA proposed implementing 24/7 SOC Monitoring through its NextGen cloud-based ProACT Managed Extended Detection and Response (MXDR) solution. The solution included the implementation and refinement of 250+ Use Cases for improved threat detection through SISA's USECASE Factory and the deployment followed a 4-step process that encompassed:

Scoping	**Log sample collection**	**Server set-up, configuration and deployment**	**Network set-up**

SISA's MXDR solution allowed for manual and automated threat detection and incident response through real-time collection of logs and historical analysis of security events from a wide variety of contextual data sources. To make the whole process seamless and friction-free, all new deployments and upgrades were first tested on the client's UAT environment before being rolled out to their production environment. The other components of the solution included:

- **Integration of 60+ Threat Intel feeds into the platform for enhanced threat detection and enrichment**
- **Daily actionable Threat Advisories**
- **Standard Hypothesis based Threat Hunting**
- **Integration of Open Source Security Event Correlator (OSSEC) into SIEM to enable IPS/ IDS alerting for PCI DSS audit**
- **Deployment of in-house File Integrity Monitoring solution and its integration with SIEM**

SISA implemented volume-based pricing model to meet the client's dynamic needs for monitoring. The model offered the client greater flexibility in terms of addition/removal of log sources as against the asset count based model which requires a change request and approvals and takes longer time to be enforced.

BUSINESS IMPACT

SISA's solution enabled 24/7 monitoring of all critical cloud-based assets by the ProACT MXDR team. This included the monitoring of AWS Production environment and AWS Test environment, with SIEM servers hosted in both environments. Following SISA's implementation of the solution, the mean time to detect (MTTD) has been significantly reduced to <30 minutes. Through actionable IOCs and enhanced use cases, Paytia's client support team is equipped to take proactive actions and improve the security posture. SISA also provided necessary evidences and documents each year which helped them in their PCI DSS audits. Further, enhanced reporting through customizable dashboards and automated reports, enabled the client to significantly improve threat detection and response. Additionally, SISA conducted its flagship Forensic Learning Session (FLS) which helped Paytia improve its readiness for future forensic engagements.

If you would like to learn more about Paytia's secure phone-payment services, please visit www.paytia.com.

SISA

A forensics driven cybersecurity solutions company, trusted by organizations across the globe for securing their businesses with robust preventive, detective, and corrective security services and solutions.

Compliance

Payment Data Security

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance
- SWIFT

Strategy and Risk

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Cloud Security

Security Testing

Application Security

- Application Penetration Testing
- CREST/CERT-in Approved Security Testing
- API Security Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- PCI ASV Scan
- Phishing Simulation

Hardware and IoT Security Testing

- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing

Cyber Resilience

Managed Extended Detection and Response

- 24/7 Monitoring
- Breach and Attack Simulation
- Use-case Factory
- Superior Threat Detection

Digital Forensics and Incident Response

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation
- Ransomware Simulation

Data Security & Governance

Data Discovery and Classification - SISA Radar

- Card Data Discovery
- PII (Privacy) Discovery
- Data Classification
- Data Masking/Encryption

Data Security as a Service

SISA Training

Payment Data Security Implementation

- CPISI
- CPISI Advanced
- CPISI-D (Developers)

Certification Program in Cybersecurity for AI Awareness

- CSPAI

Cybersecurity Awareness

Forensic Learning Sessions for Senior Management

For more Information visit us at www.sisainfosec.com
OR
write to us at *contact@sisainfosec.com*

Follow us