

CUSTOMER SUCCESS STORY

Driving Peak Performance: How PayU Leveraged SISA ProACT MXDR to Dominate Big Billion Sales

About PayU

PayU is a leading online payment service provider operating across 50+ high-growth markets. The company processes approximately 10 million payments daily through over 400 payment methods and PCI-certified platforms, globally. The company operates in three primary business sectors – payments, credit, and PayTech – generating over \$60 billion in annualized volumes.

Business Requirement: Seamless operations during peak sales

As a leading digital payments processor, PayU plays a critical role in facilitating seamless transactions for thousands of merchants, especially during high-traffic events like the Big Billion Sale. During such sale periods, the availability of business applications is absolutely critical, as even minimal downtime can lead to significant revenue loss and a damaged reputation. Recognizing the dynamic and evolving nature of their business and to ensure the business is not getting impacted by cyber risks, PayU needed a flexible partner capable of scaling up threat detection and response.

With surges in web traffic during such events, security plays a critical role not only in protecting sensitive data but also in ensuring the continuous availability and optimal functionality of services. Any disruption could ripple through the ecosystem, affecting merchants and customers alike, making the stakes incredibly high.

The Solution

ProACT MXDR provides PayU with around-the-clock monitoring and access to SISA's dedicated cybersecurity experts, offering more than just automated alerts. The platform integrates advanced analytics with hands-on threat management, ensuring that critical issues are addressed before they escalate. ProACT MXDR's transparency allows PayU to clearly see the threats being addressed, while its automated scaling capabilities ensure that transaction spikes are handled effortlessly.

How ProACT MXDR delivered business value

 **24x7 Monitoring and Threat Detection:** ProACT MXDR continuously scans PayU's environment, providing enhanced visibility across cloud platforms and networks. Any anomalies are flagged immediately, ensuring real-time detection and response to potential threats.

 **Auto-Scaling for High EPS:** By integrating with AWS, ProACT MXDR dynamically scales during periods of high EPS, preventing system slowdowns or outages during critical sale events.

 **Dedicated Security Experts:** During peak sales, PayU benefits from SISA's rapid response team, which operates 24x7 to address any threats or compliance needs immediately, minimizing downtime risks.

 **Rapid Merchant Onboarding:** ProACT MXDR accelerates merchant onboarding by embedding baseline security measures into the process, ensuring new partners meet compliance requirements without delaying operations.

 **Data Localization and High Availability:** ProACT MXDR supports data localization to meet regulatory demands, while ensuring high availability through redundancy and failover systems, safeguarding data integrity at all times.

Benefits

ProACT MXDR has proven instrumental in enabling PayU to scale its operations without compromising security or performance. The solution's ability to unify existing security investments, streamline compliance, and provide ongoing monitoring has delivered measurable business outcomes. .

ProACT MXDR delivered—

**Seamless Peak Period Management:**

Successfully managed two Big Billion Sale events in 2023 and 2024 with no operational disruptions, ensuring consistent revenue streams during critical periods.



Accelerated Growth and ROI: Year-on-year business growth has surged, driven by improved security, flexibility, and scalability, while optimized operations and reduced downtime have delivered a strong return on investment.



Enhanced Security Posture: By integrating diverse security tools and providing continuous oversight, ProACT MXDR ensures PayU remains ahead of potential threats, contributing to a stronger overall defense framework.



Superior Threat Detection: Enhanced detection capabilities have allowed PayU to identify and mitigate potential risks proactively, reducing vulnerabilities and safeguarding their operations against cyber threats.



Seamless Compliance: ProACT MXDR simplifies audits and regulatory processes, ensuring PayU meets industry standards effortlessly while building trust and confidence among partners.

With ProACT MXDR, PayU gains more than just a security platform—it secures their growth, allowing them to focus on expanding their merchant network and scaling operations confidently during peak sale periods. The proactive defense mechanisms provided by ProACT MXDR ensure that PayU stays ahead of potential threats, reinforcing trust and ensuring seamless digital payment experiences for their customers.

Ensuring uninterrupted operations during critical business periods like Big Billion Sales is essential for PayU. With SISA as our cybersecurity partner, their ProACT MXDR solution has successfully safeguarded our business from cyber threats for two consecutive years during these high-stakes periods. The ProACT MXDR platform's scalability for peak traffic during festive sales, combined with 24/7 monitoring, proactive threat hunting, customized dashboards, and tailored threat intelligence, has enabled us to maintain a strong security posture. Additionally, their dedicated war room provided quick support for addressing potential threats with immediate action. SISA's expertise and commitment have been instrumental in ensuring business continuity during our most critical times.

Shrikant Malikarjun Ware

Lead SOC Engineer, PayU

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

Compliance	Security Testing	Cyber Defense	Data Protection & Governance	Trainings & Certifications	Leading Tech Security
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 • HITRUST Unified Audits Managed Compliance	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 • Firewall Rule Review • PCI ASV Scan Phishing Simulation Red Teaming Exercise • Layer Security Testing	Managed Extended Detection and Response Solution - SISA ProACT • 24x7 Monitoring • UEBA • Threat Intel • Advanced Threat Hunting • Breach & Attack Simulation • SOAR • Use-case Factory 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 Discovery and Classification • PCI/PII/PHI Data Discovery • Data Classification in Endpoint (Windows, Linux) • Data Classification in O365, Metadata • Dynamic Masking, Redact, Truncation • Integration to DRM, DLP, SIEM Data Privacy Professional Services • Assessments (Unified Privacy Maturity, DPIA, 3rd Party Risk) • Data Inventory, Mapping and Process flow, RoPA • Data Privacy Framework - Policy, Notice, SoPs • Consent and Notice Management framework • Data Breach and Management • Principal management • Privacy by Design implementation guide • Define Data Retention Guidelines and processes • Technical/Organization measures • Privacy Training/Awareness	Payment Data Security Training and ANSI Accredited Certification • CPISI (2 Day Program) • CPISI (3 Day Program) • CPISI- Advanced (3 Day Program) • CPISI-D (Developers) • CPISI Hybrid (4 Weeks) Certification Program in Cybersecurity for AI – CSPAI • CSPAI • CSPAI - Developers Forensic Briefing Sessions for Senior Management	AI PRISM • AI PRISM LLM Vulnerability Scanner Solution • AI Risk Management and Governance Solution Framework • AI Compliance and Governance Consulting Service Hardware and IoT Security Testing • Firmware Security Testing • Hardware/Embedded Security Testing • IoT Network Security Testing • IoT/Embedded Application and Management Layer Security Testing • MPOC/ PCI PTS Quantum Security • Quantum Cryptographic Consulting • Quantum Security Risk Assessment • Quantum Security Standards Compliance

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

Follow us

