tekpon®

ANALYST REPORT · MARCH 2026

European SIEM Platforms 2026

Independent Comparison Report

A Tekpon Analyst Report evaluating Security Information and Event Management solutions for European enterprise and government buyers under DORA, NIS2 and the EU AI Act.

4	6	03/26
Vendors	**Criteria**	**March 2026**
Independently Evaluated	Weighted by EU Buyer Priorities	Published by Tekpon

Table of Contents

→ Executive Summary

→ Evaluation Framework

→ The Tekpon Quadrant

→ Vendor Profile: Nextgen Software — CYBERQUEST

→ Vendor Profile: Splunk Enterprise Security (Cisco)

→ Vendor Profile: Fortinet FortiSIEM

→ Vendor Profile: LogPoint

→ Head-to-Head Comparison Matrix

→ Recommendations by Buyer Profile

→ Frequently Asked Questions

→ Methodology

Executive Summary

Market Context

The global SIEM market reached an estimated USD 9.7 billion in 2025 and is projected to grow at a 14–17% CAGR through 2033. Much of this growth is driven by regulatory compliance pressure rather than pure security need — particularly in Europe, where three overlapping frameworks now demand audit-grade incident evidence within hours, not days.

Why This Report Exists

The 2025 Gartner Magic Quadrant for SIEM positions only US-headquartered vendors as Leaders. European-native vendors such as LogPoint and Nextgen Software fall outside Gartner's scope entirely, despite serving thousands of European enterprise and government customers. EU regulatory convergence — DORA, NIS2 and the EU AI Act — demands a new evaluation framework built around European buyer priorities: compliance automation, data sovereignty and total cost of ownership.

Methodology Reference

This report evaluates four SIEM platforms across six weighted criteria selected to reflect European enterprise and government buyer priorities. Assessments are based on publicly available documentation, vendor-provided specifications, published user reviews and regulatory requirement mapping. For full details, see tekpon.com/methodology/

Why a European SIEM Comparison Matters in 2026

The 2025 Gartner Magic Quadrant for SIEM positions Microsoft Sentinel, Splunk, Exabeam, Securonix and Google Chronicle as Leaders — all US-headquartered. Fortinet is classified as a Challenger. European-native vendors such as LogPoint and Nextgen Software fall outside Gartner's scope entirely, despite serving thousands of European enterprise and government customers.

The Gap

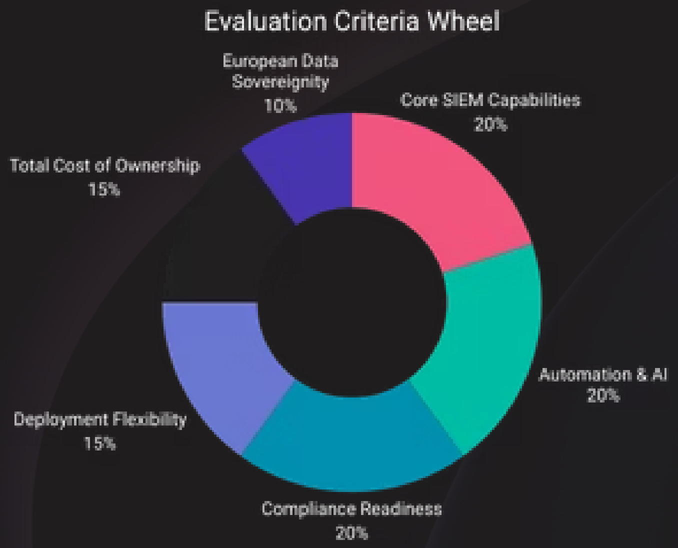
European procurement officers — particularly in defence, financial services and critical infrastructure — increasingly require **network security software** that meets EU data sovereignty requirements, maps natively to DORA and NIS2 reporting templates, and is developed under European jurisdiction. A comparison built around US-centric criteria misses these dimensions.

Tekpon's Approach

Tekpon's evaluation framework addresses this by weighting European regulatory readiness and data sovereignty alongside traditional SIEM capabilities. Our **methodology** is based on publicly available documentation, vendor-provided technical specifications, published user reviews, and regulatory requirement mapping.

Evaluation Framework

Each vendor is assessed across six weighted criteria reflecting European enterprise and government buyer priorities in 2026.



Criterion	What We Assess
Core SIEM Capabilities	Log collection, normalisation, correlation, alerting, dashboards
Automation & AI	SOAR integration, UEBA, AI-assisted investigation, playbook depth
Compliance Readiness	DORA templates, NIS2 mapping, GDPR alignment, EU AI Act, ISO 27001
Deployment Flexibility	On-prem, cloud, hybrid, OT/IT convergence, agentless monitoring
Total Cost of Ownership	Licensing transparency, scalability costs, integration overhead
European Data Sovereignty	EU-based development, data residency, jurisdictional control

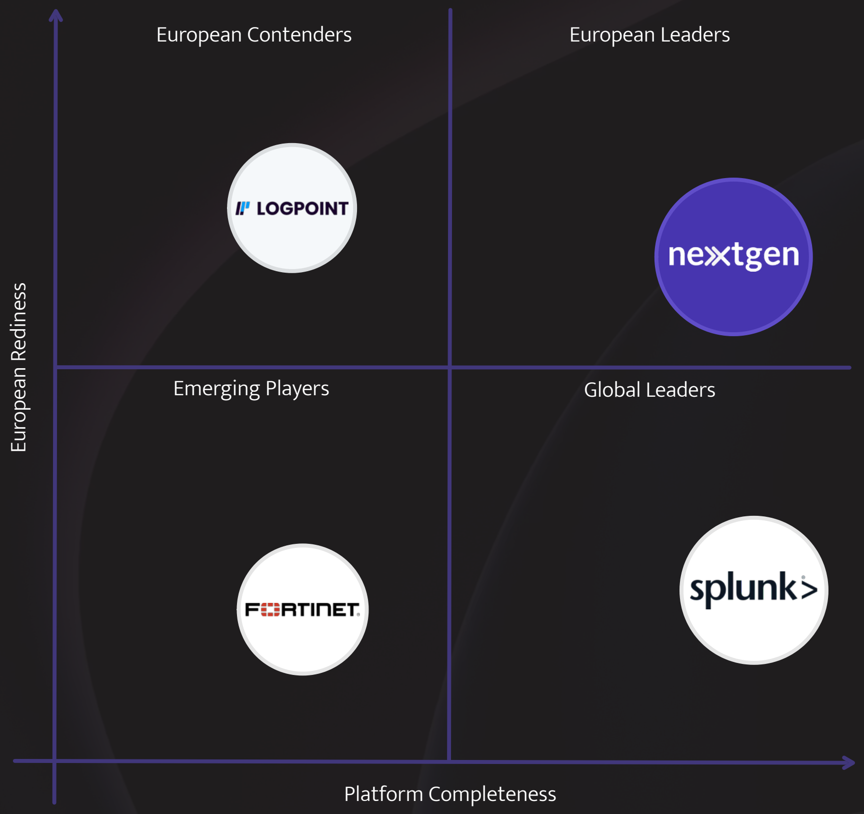
Scoring Scale

1–5 per criterion. 1 = significant gaps. 5 = market-leading.

Quadrant Axes

X-axis: Platform Completeness. Y-axis: European Readiness.

The Tekpon Quadrant: European SIEM Platforms 2026



US-Originated Platforms - Lead in raw platform capability and ecosystem breadth

European-Native Vendors - Outperform on regulatory readiness and deployment flexibility

Key Takeaway - No single vendor dominates both axes — buyers must weigh their priorities

Vendor Profile: Nextgen Software — CYBERQUEST

At a Glance

Headquarters: Bucharest, Romania

Founded: 2014

Focus: Unified SIEM + SOAR + UEBA + NDR

Nextgen Software's CYBERQUEST is a natively integrated security operations platform combining SIEM, SOAR, UEBA and network detection and response (NDR, via its NETALERT module) in a single architecture. Built entirely in-house by a European team, the platform targets enterprise SOC teams and government organisations that need compliance-ready workflows without multi-vendor integration overhead.

Key Strengths

CYBERQUEST's primary differentiator is architectural unity. Where competitors require separate modules or third-party integrations for SOAR and UEBA, Nextgen delivers these natively — including over 270 pre-built connectors and 1,200+ automated response actions. The CQ AI Assistant provides AI-powered investigation support, while the platform generates DORA and NIS2-compliant incident reports as a by-product of normal investigation workflows. The NETALERT NDR module offers agentless OT monitoring — critical for manufacturing and energy organisations under NIS2 that cannot deploy endpoint agents on industrial control systems.

Considerations

Nextgen's brand recognition in Western Europe (Nordics, DACH, Benelux) is still developing, though established in Romania, Southeast Europe and growing in Central Europe. The vendor ecosystem is smaller than Splunk's or Fortinet's, and third-party integration marketplace depth is more limited. Organisations requiring a very large partner network for implementation support may find fewer options compared to global vendors.

Criterion	Score (1–5)	Notes
Core SIEM	4.5	Full SIEM+SOAR+UEBA natively integrated; 400+ out-of-the-box detection scenarios
Automation & AI	4.5	Native SOAR with 1,200+ actions; CQ AI Assistant; Cyber Minds AI Personas
Compliance Readiness	5.0	DORA/NIS2 templates built in; automated compliance reporting; audit-trail-by-design
Deployment Flexibility	4.5	On-prem, hybrid; agentless OT via NETALERT; multi-tenancy for MSSPs
Total Cost of Ownership	4.5	Predictable modular licensing; no hardware lock-in; rapid onboarding
European Data Sovereignty	5.0	100% EU-developed; EU data residency; Romanian jurisdiction
Weighted Total	**4.65**	

Vendor Profile: Splunk Enterprise Security (Cisco)

At a Glance

Headquarters: San Francisco, USA (acquired by Cisco, 2024)

Focus: Data analytics platform with SIEM overlay

Splunk Enterprise has been a SIEM market leader for over a decade, named a Leader in Gartner's Magic Quadrant for eleven consecutive years. Its strength lies in massive scalability, a deep analytics engine, and one of the largest ecosystems of integrations and apps in the security industry. The 2024 Cisco acquisition brings additional network security telemetry but also introduces US corporate governance over European customer data.

Key Strengths

Unmatched ecosystem depth (2,400+ apps on Splunkbase), powerful SPL query language for advanced threat hunting, extensive community and training resources. Splunk SOAR (formerly Phantom) provides strong automation capabilities. The platform excels in large-scale data analytics beyond pure security use cases.

Considerations

TCO is the most common concern. Splunk's ingestion-based pricing model (approximately USD 1,800–2,500 per GB/day for annual licences) can escalate rapidly as data volumes grow. Implementation complexity typically requires specialised integrators and extended onboarding timelines. The Cisco acquisition raises data sovereignty questions for EU government customers — data may be subject to US legal jurisdiction (CLOUD Act). DORA and NIS2 compliance templates are not natively built in and require custom configuration or third-party overlays.

Criterion	Score (1–5)	Notes
Core SIEM	5.0	Industry-leading analytics engine; massive integration ecosystem
Automation & AI	4.5	Splunk SOAR strong but separate product; AI Assistant improving
Compliance Readiness	3.0	Powerful reporting but DORA/NIS2 templates require custom build
Deployment Flexibility	4.0	Cloud-first (Splunk Cloud); on-prem available; limited OT-native options
Total Cost of Ownership	2.5	High ingestion-based pricing; significant services overhead; lock-in risk
European Data Sovereignty	2.5	US-headquartered (now Cisco); CLOUD Act jurisdiction; EU data centres available
Weighted Total	**3.73**	

Vendor Profile: Fortinet FortiSIEM

At a Glance

Headquarters: Sunnyvale, USA

Focus: Network-security-first SIEM within the Fortinet Security Fabric

FortiSIEM is positioned as the SIEM component within Fortinet's broader Security Fabric — an integrated hardware and software ecosystem. Gartner classified Fortinet as a Challenger in its 2025 SIEM Magic Quadrant, recognising improving capabilities but noting gaps compared to Leaders. FortiSIEM is strongest when deployed alongside other Fortinet products (FortiGate, FortiAnalyzer, FortiEDR).

Key Strengths

Competitive pricing (starting from approximately USD 2,000 annually for smaller deployments), particularly attractive for organisations already invested in the Fortinet hardware ecosystem. MITRE ATT&CK framework mapping is well-implemented. The perpetual licensing model with CAPEX option appeals to government procurement models that prefer one-time purchases.

Considerations

FortiSIEM's standalone value is limited — the platform performs best within Fortinet's proprietary ecosystem, creating significant vendor lock-in. Automation capabilities are primarily rule-based rather than AI-driven. UEBA and advanced analytics lag behind dedicated SIEM vendors. The licensing model based on events per second (EPS) can be difficult to predict as environments scale. Like Splunk, DORA/NIS2 compliance automation requires additional configuration. US headquarters raise the same data sovereignty concerns for EU government buyers.

Criterion	Score (1–5)	Notes
Core SIEM	3.5	Solid fundamentals; strongest within Fortinet ecosystem; limited standalone
Automation & AI	2.5	Rule-based automation; limited AI; SOAR basic compared to leaders
Compliance Readiness	2.5	MITRE mapping good; DORA/NIS2 templates not native; manual effort needed
Deployment Flexibility	3.5	On-prem strong; hardware-first design; limited agentless OT options
Total Cost of Ownership	3.5	Competitive entry pricing; hidden costs in ecosystem lock-in; EPS-based scaling
European Data Sovereignty	2.5	US-headquartered; data centres in EU available; CLOUD Act jurisdiction
Weighted Total	**3.00**	

Vendor Profile: LogPoint

At a Glance

Headquarters: Copenhagen, Denmark

Founded: European-native

Focus: European-native converged SIEM + SOAR + UEBA

Distribution: Primarily through Prianto

LogPoint is the other major European-native SIEM vendor, with strong adoption in the Nordics, DACH and Central Europe. The platform positions itself as a "converged SIEM" integrating SIEM, SOAR, UEBA and — more recently — NDR capabilities into a single solution. LogPoint has built its reputation on MSSP-friendly multi-tenancy and transparent node-based pricing.

Key Strengths

European-developed and headquartered (Denmark), making it a natural fit for EU data sovereignty requirements. Node-based licensing (rather than data-volume-based) offers predictable costs. Strong MSSP Director for managed security providers. Over 1,000 built-in detections and 80+ out-of-the-box playbooks. LogPoint explicitly markets "sovereign-ready" deployment options.

Considerations

LogPoint's feature set, while converged, is narrower than CYBERQUEST's or Splunk's — particularly in NDR maturity and AI-assisted investigation depth. The integration ecosystem has fewer pre-built connectors than Splunk or Nextgen. While popular in Nordics/DACH, market presence in Southern and Eastern Europe is thinner. DORA compliance templates are developing but not as mature as Nextgen's native implementation.

Criterion	Score (1–5)	Notes
Core SIEM	4.0	Solid converged platform; 1,000+ detections; good search and analytics
Automation & AI	3.5	Integrated SOAR with 80+ playbooks; UEBA included; AI less advanced
Compliance Readiness	4.0	Good EU regulatory awareness; sovereign-ready marketing; DORA templates developing
Deployment Flexibility	3.5	On-prem, hybrid, customer-managed cloud; NDR newer; limited OT depth
Total Cost of Ownership	4.0	Transparent node-based licensing; no volume penalties; full features included
European Data Sovereignty	5.0	Danish headquarters; EU jurisdiction; sovereign-ready positioning
Weighted Total	**3.93**	

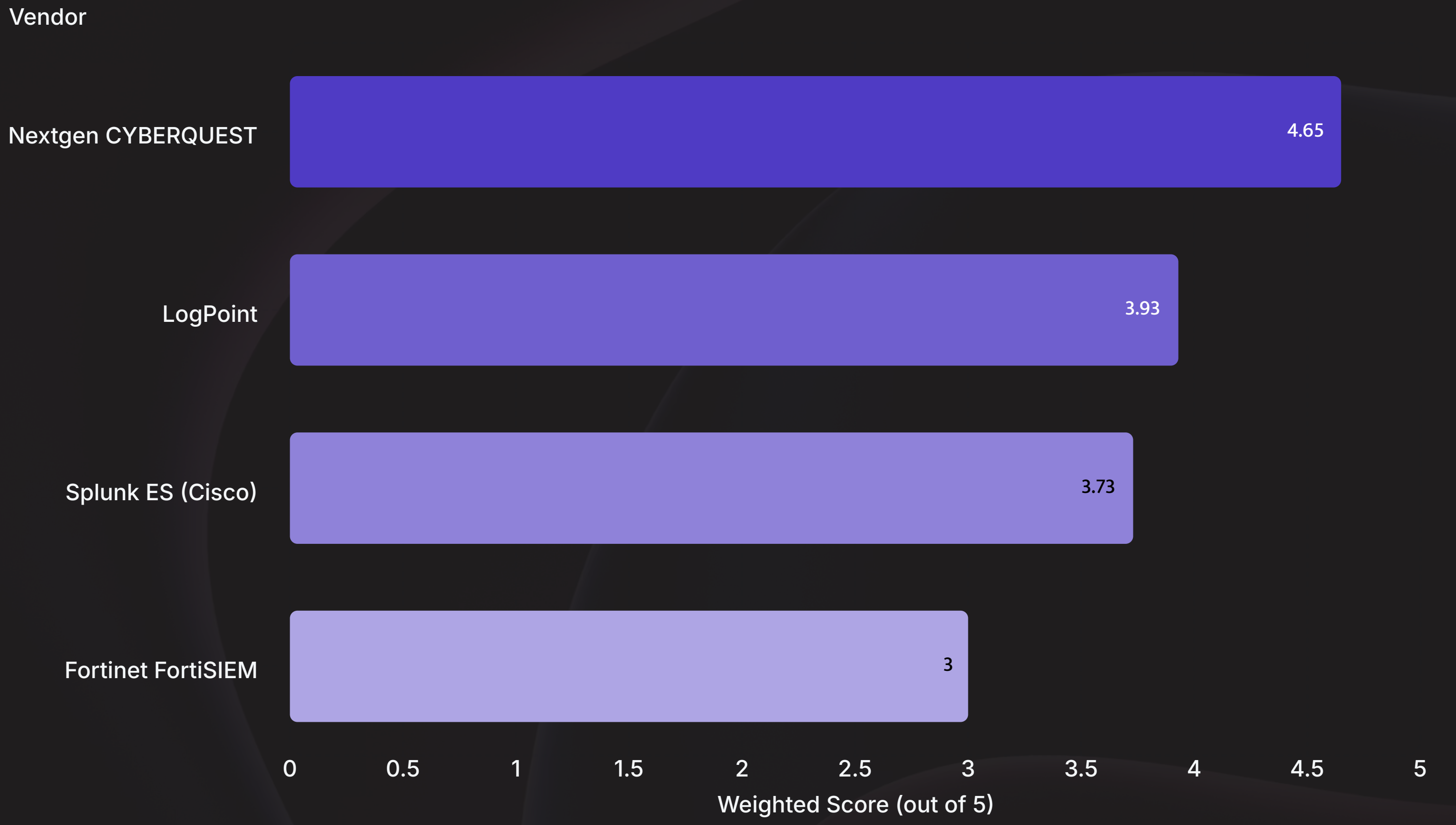
Head-to-Head Comparison Matrix

The following matrix maps each vendor against the core capabilities that European enterprise and government procurement teams typically evaluate. This table is designed to be used alongside specific technical requirements — such as those found in government SIEM procurement specifications — to identify which platform aligns best with a given use case.

Capability	Nextgen CYBERQUEST	Splunk ES (Cisco)	Fortinet FortiSIEM	LogPoint
Architecture	Unified SIEM+SOAR+UEBA+NDR	SIEM + separate SOAR (Phantom)	SIEM within Security Fabric	Converged SIEM+SOAR+UEBA
Native SOAR	Yes (1,200+ actions)	Separate product (Splunk SOAR)	Basic, rule-based	Yes (80+ playbooks)
UEBA	Natively integrated	Add-on module	Limited	Natively integrated
NDR / Network Detection	NETALERT (agentless)	Via Cisco ecosystem	Via FortiNDR (separate)	Recently added
AI-Assisted Investigation	CQ AI Assistant + Cyber Minds	Splunk AI Assistant	Limited	Developing
Pre-built Connectors	270+	2,400+ (Splunkbase)	Ecosystem-dependent	500+
Out-of-box Detections	400+ scenarios	1,400+ (Community + ES)	700+ rules	1,000+ detections
DORA Compliance Templates	Native, automated	Custom configuration	Custom configuration	Developing
NIS2 Mapping	Built-in	Requires overlay	Requires overlay	Available
OT/ICS Monitoring	Agentless via NETALERT	Via Cisco OT Security	Via Fortinet OT products	Limited
Multi-Tenancy (MSSP)	Yes, horizontal/vertical	Yes (complex setup)	Within Fortinet ecosystem	Yes (MSSP Director)
Licensing Model	Modular, predictable	Ingestion-based (GB/day)	EPS-based or subscription	Node-based
Data Sovereignty	EU (Romania)	US (Cisco) + EU DCs	US + EU DCs	EU (Denmark)
Gartner MQ 2025	Not evaluated	Leader (11th year)	Challenger	Not evaluated
Tekpon Quadrant Position	European Leader	Global Leader	Global Challenger	European Contender

Vendor Weighted Score Summary

Vendors are scored on a 1–5 scale across six weighted criteria. The chart below reflects overall positioning on the Tekpon Quadrant.



Recommendations by Buyer Profile

Government and Defence Buyers

Government procurement — particularly in defence and critical infrastructure — prioritises data sovereignty, on-premises deployment and compliance automation. The Cyber Defence Command specification from Romania's Ministry of National Defence, for example, requires a SIEM capable of on-premises deployment, multi-source log correlation, real-time analytics with Threat Intelligence integration and role-based access control (RBAC) with dataset-level granularity. European-native vendors score highest here, with **Nextgen CYBERQUEST** offering the strongest alignment between native compliance automation and EU jurisdictional control, followed by **LogPoint** for Nordics- and DACH-focused procurement.

Nextgen CYBERQUEST — European Leader

Strongest alignment between native compliance automation and EU jurisdictional control. Recommended for defence, critical infrastructure and government buyers requiring on-premises deployment, DORA/NIS2 automation and full EU data sovereignty.

Financial Services (DORA-Regulated)

Banks, insurers and investment firms under DORA must submit initial incident reports within hours, backed by digitally signed forensic evidence. The platform must generate compliance artefacts as a by-product of investigation — not as a separate manual process. **Nextgen CYBERQUEST** and **LogPoint** both address this, with Nextgen offering deeper automation of the evidence chain. Splunk provides the most powerful raw analytics but requires significant custom work for DORA-specific reporting.

LogPoint — European Contender

Recommended for Nordics- and DACH-focused procurement. Danish headquarters, sovereign-ready positioning and transparent node-based licensing make it a strong fit for regulated European enterprises.

Recommendations by Buyer Profile

Manufacturing and Energy (NIS2-Regulated)

NIS2 expansion brought manufacturing into the regulated perimeter for the first time in 2025. These environments require OT/IT convergence — monitoring industrial control systems without deploying intrusive endpoint agents. **Nextgen CYBERQUEST** with NETALERT stands out here, offering agentless OT monitoring natively integrated into the SIEM workflow. Fortinet offers OT capabilities through its broader ecosystem but requires multiple products. Splunk addresses OT through the Cisco acquisition but integration is still maturing.

Nextgen CYBERQUEST — OT/NIS2 Leader

Agentless OT monitoring via NETALERT natively integrated into the SIEM workflow. Recommended for manufacturing and energy organisations under NIS2 that cannot deploy endpoint agents on industrial control systems.

Managed Security Service Providers (MSSPs)

MSSPs need multi-tenancy, horizontal scalability and competitive unit economics. **LogPoint** with its MSSP Director and node-based pricing is purpose-built for this segment. **Nextgen CYBERQUEST** offers strong multi-tenancy with lower TCO. Splunk is powerful but overhead makes it less optimal for smaller MSSPs.

Splunk Enterprise Security — Global Leader

Best suited for large enterprises with existing Splunk investments, advanced threat hunting requirements and the resources to manage ingestion-based costs and custom compliance configuration.

Fortinet FortiSIEM — Global Challenger

Most appropriate for organisations already deeply invested in the Fortinet Security Fabric ecosystem, where the SIEM functions as one component of a broader integrated security architecture.

Frequently Asked Questions

1

Q: What is a SIEM platform and why do European organisations need one?

A: A Security Information and Event Management (SIEM) platform collects, normalises and correlates security logs and events from across an organisation's IT infrastructure. In Europe, SIEM platforms are increasingly essential not just for threat detection but for meeting regulatory requirements under DORA, NIS2 and the EU AI Act, which demand auditable evidence of cybersecurity monitoring and incident response.

2

Q: How does DORA affect SIEM requirements for financial institutions?

A: The Digital Operational Resilience Act (DORA), in force since January 2025, requires financial institutions to submit incident reports within hours, backed by forensic-grade evidence. This means SIEM platforms must generate digitally signed, time-stamped logs and automated compliance reports — not just security alerts. Platforms with native DORA templates significantly reduce the manual effort required.

3

Q: What is the difference between a European and US-based SIEM for procurement?

A: European-native SIEM vendors (headquartered and developed within the EU) offer jurisdictional advantages: customer data remains under EU law, insulated from extraterritorial legislation like the US CLOUD Act. For government and critical infrastructure procurement, this can be a decisive factor in vendor selection.

4

Q: How does NIS2 change SIEM requirements for manufacturing companies?

A: NIS2, transposed into national law across Europe in 2024–2025, expanded the regulatory perimeter to include manufacturing as a regulated sector. This means manufacturing companies must now implement security monitoring, incident reporting and board-level accountability for cybersecurity — requirements that typically necessitate a SIEM platform with OT/IT convergence capabilities and automated compliance workflows.

5

Q: Can smaller European SIEM vendors compete with Gartner Magic Quadrant Leaders?

Yes, particularly in regulated European markets. Gartner's evaluation criteria emphasise global scale, ecosystem breadth and cloud adoption — dimensions where US hyperscalers naturally lead. European vendors like Nextgen Software and LogPoint compete on different axes: native EU compliance automation, data sovereignty, transparent pricing and architectural efficiency for mid-market and government buyers. For these buyer profiles, European vendors often deliver better outcomes at lower total cost.

Methodology

This comparison was prepared by Tekpon's editorial team based on the following sources:

- publicly available vendor documentation and technical specifications
- published pricing information and licensing guides
- regulatory framework analysis (DORA, NIS2, EU AI Act)
- vendor-provided product materials and demonstrations
- published user reviews on G2, Gartner Peer Insights and Capterra
- the Nextgen 2025/2026 Cybersecurity Trends Report for market data

Tekpon is an independent software review platform. Vendor inclusion in this report does not imply endorsement, and all assessments reflect Tekpon's editorial judgement based on the criteria described above. For full details on how Tekpon evaluates software, see our methodology page.