



Penta Sentinel

Next-Generation Security Monitoring

Overview

Penta Sentinel is a comprehensive Security Information Event Management (SIEM) solution crafted by Penta's cybersecurity experts using state-of-the-art technologies, customised for each of our clients and delivered as a managed service backed by a 24/7/365 Security Operations Centre and built-in regulatory compliance.

Penta Sentinel is part of Penta's IT Risk Solutions Portfolio, and an extension to Penta's managed private cloud and IaaS offerings, enabling businesses to stay alert and secure their operations from emerging threats. Hosted at Penta's data centres in Dubai and Geneva, Penta Sentinel combines best-in-class software with IT expertise that is trusted in running and maintaining IT infrastructures for some of the world's leading financial organisations.

Key Features



Data Collection

Penta Sentinel collects logs from across your entire IT infrastructure in a systematic way using a number of methods including network traffic monitoring, system event logs forwarding from servers, endpoints, applications, firewalls, anti-virus and anti-malware systems, in addition to dedicated agents configured to track specific types of flows, transactions, and interactions. Penta Sentinel also comes packed with its own network security monitoring, intrusion detection and intrusion prevention systems.



Correlation, Analysis and Alerts

Penta Sentinel aggregates and normalises all the data ingested and then parses and analyses this data to detect anomalies and suspicious activities that might signal real threats. Our Security Operations Centre (SOC) experts receive the alerts in real time, analyse the data aided by an advanced set of tools and methods, sifting through false positives and negatives to identify the real threats and respond in real time.



User Behaviour Analysis

Insider threats are a growing concern as they can have a greater impact and might take months or more to discover. That is why Penta Sentinel features user behaviour analysis, both manual and automated, designed to detect insider threats that may have been able to bypass firewalls, anti-virus and anti-malware tools.



Threat Intelligence

Apart from the anomaly-based threat detection, Penta Sentinel features signature-based threat intelligence that is enhanced by leveraging multiple sources of network-based and host-based intrusion detection systems, and multiple threat intelligence sources such as MITRE ATT&CK®, Snort, Zeek (Bro), and YARA.



Security Operation Center

Penta Sentinel's SOC is the central hub where all the data and insights are channeled and reviewed by our team of top cybersecurity experts who are monitoring and evaluating the events 24/7/365, and handling threat detection and response in real time. With Penta Sentinel you get your own outsourced SOC function, reducing the load on your internal teams and on your IT budgets.





Reporting

Penta Sentinel features automated reports that are reviewed and signed off by our cybersecurity experts, giving you full visibility over your security monitoring and the health of your IT infrastructure. Standard reports include elements such as user authentication, security events, risk reporting, email security, and network security. And with Penta Sentinel being a custom solution designed around your unique requirements, reporting can be expanded to include the metrics that matter to you.

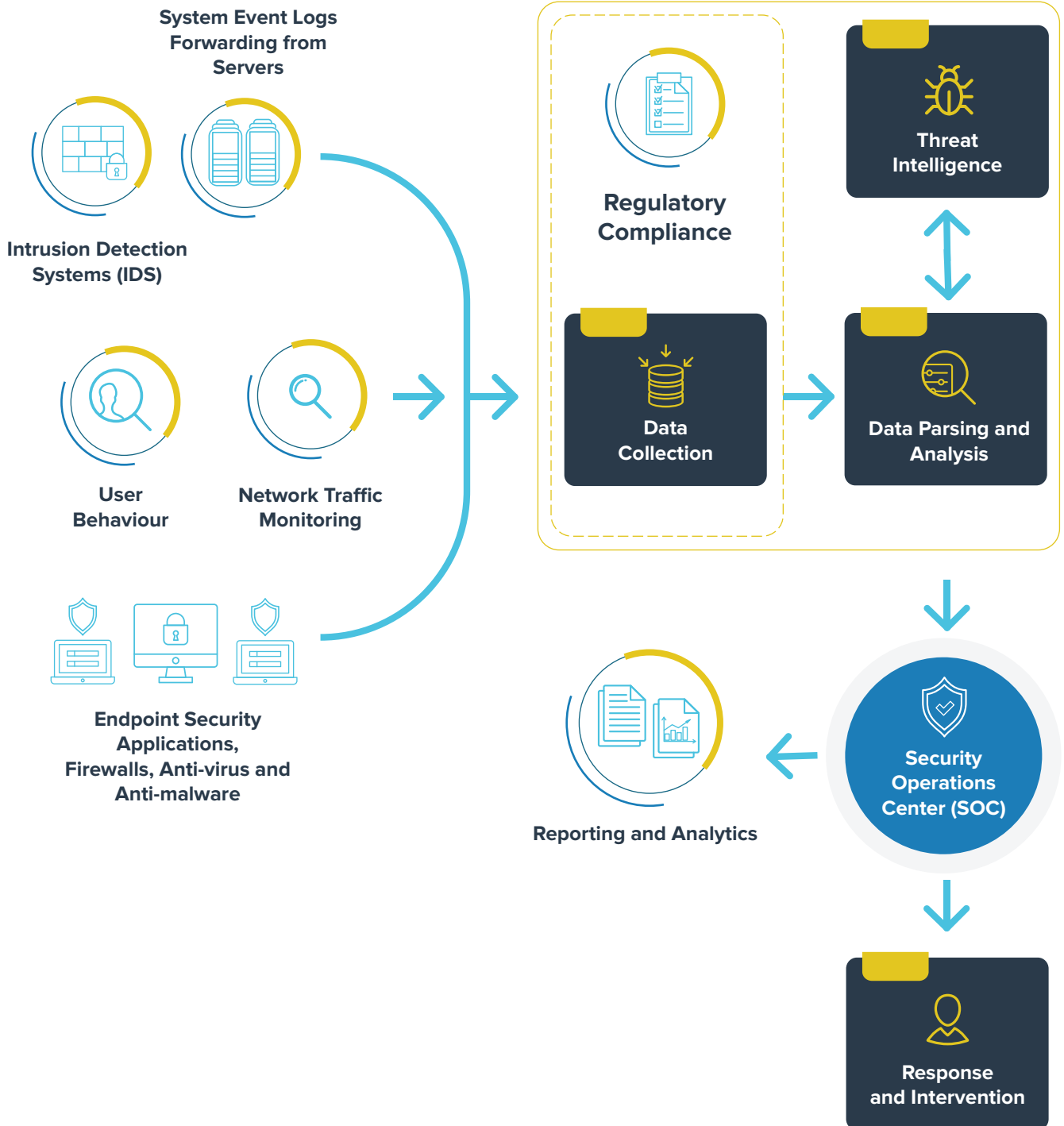


Regulatory Compliance

With Penta Sentinel being a hosted solution at Penta's data centres in Dubai and Geneva, regulatory compliance is built-in from day one for all the data captured and retained, thanks to Penta's compliance-ready infrastructure which supports SOX, HIPAA, PCI, SSAE, and GDPR.

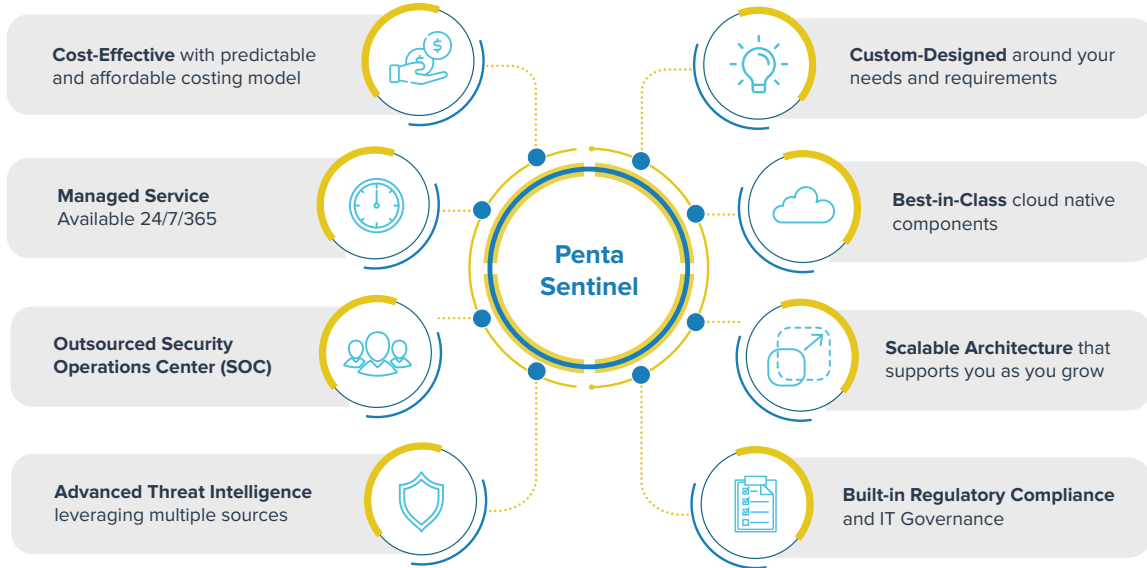
Additionally, Penta Sentinel supports your business to comply with the ISO/IEC 27001 standard for Information Security Management by enhancing controls such as Organisation of Information Security, Human Resource Security, Access Control, Information Security Incident Management, Business Continuity Management, and Compliance.

HOW DOES PENTA SENTINEL WORK?



WHY PENTA SENTINEL

THE PENTA MODEL FOR SIEM



PENTA SENTINEL VS COMPETITION

	Penta Sentinel	Traditional SIEM
Configuration & Design	✔ Rapid and easy deployment with a minimal footprint	✘ Lengthy, complex and costly implementation process
Threat Intelligence	✔ Access to several world class threat intelligence sources	✘ Access to fewer threat intelligence sources with higher undetected threat risk
Monitoring and Management	✔ Automatic monitoring based on signature and behavioural activity complemented by Penta SOC escalation and response team	✘ Requires a dedicated team of IT professionals often working shifts on a 24/7/365 basis
Reporting	✔ Comprehensive and simple to understand reporting. Available on a scheduled or ad-hoc basis for management and technical team	✘ Requires IT security technical skills to interpret reports and threats
Regulatory Compliance	✔ Built-in compliance and IT governance	✘ Lacking out-of-the-box compliance or available at additional cost
Hosting	✔ On-premise or on Penta's private cloud in data protected jurisdictions	✘ Usually on public clouds prone to data breach risks, or private clouds in non-protected jurisdictions
Pricing Model	✔ Transparent monthly price per IP address monitored.	✘ Multiple factors, often combining data sources and data volume, resulting in complex pricing
Overall Cost	✔ Affordable low entry-point at a fraction of legacy SIEM running costs	✘ High entry-point, unpredictable license and maintenance cost

THE PENTA VALUE PROPOSITION



IT Support

- ▶ Premium Service Desk
- ▶ Assigned Account Manager
- ▶ VIP & Critical Support



Security

- ▶ Bank Level Security
- ▶ 24/7 Monitoring
- ▶ Regular Penetration Tests



IT Governance

- ▶ Regulatory Compliance
- ▶ Yearly Audits
- ▶ Included at no extra cost



Technical Expertise

- ▶ Specialist Teams
- ▶ Bespoke Setups
- ▶ CTO as a Service



Innovation

- ▶ Latest Technology
- ▶ R&D Labs
- ▶ Business Transformation

Other Solutions in Penta's IT Risk Portfolio:

- ◆ IT Audits
- ◆ IT Governance
- ◆ IT Compliance
- ◆ Remote Monitoring and Management (RMM)
- ◆ IT Infrastructure Audits
- ◆ Penetration Testing
- ◆ IT Security Policy Development
- ◆ Cyber Security Awareness Training
- ◆ Cyber Insurance Support
- ◆ Microsoft 365 Security

Speak to one of our consultants today to learn more

Europe

Geneva, Switzerland

Rue Bémont 4
1204 Geneva
Switzerland

Email: sales@penta.ch
Telephone: +41 22 316 1000

Middle East

Dubai, United Arab Emirates

201B, North Tower, Emirates Financial Towers
Dubai International Financial Centre (DIFC)
PO Box 506600 – Dubai, United Arab Emirates

Email: sales@penta.ch
Telephone: +971 4 376 7100