eventus

eventussecurity.com

EVENTUS PLATFORM

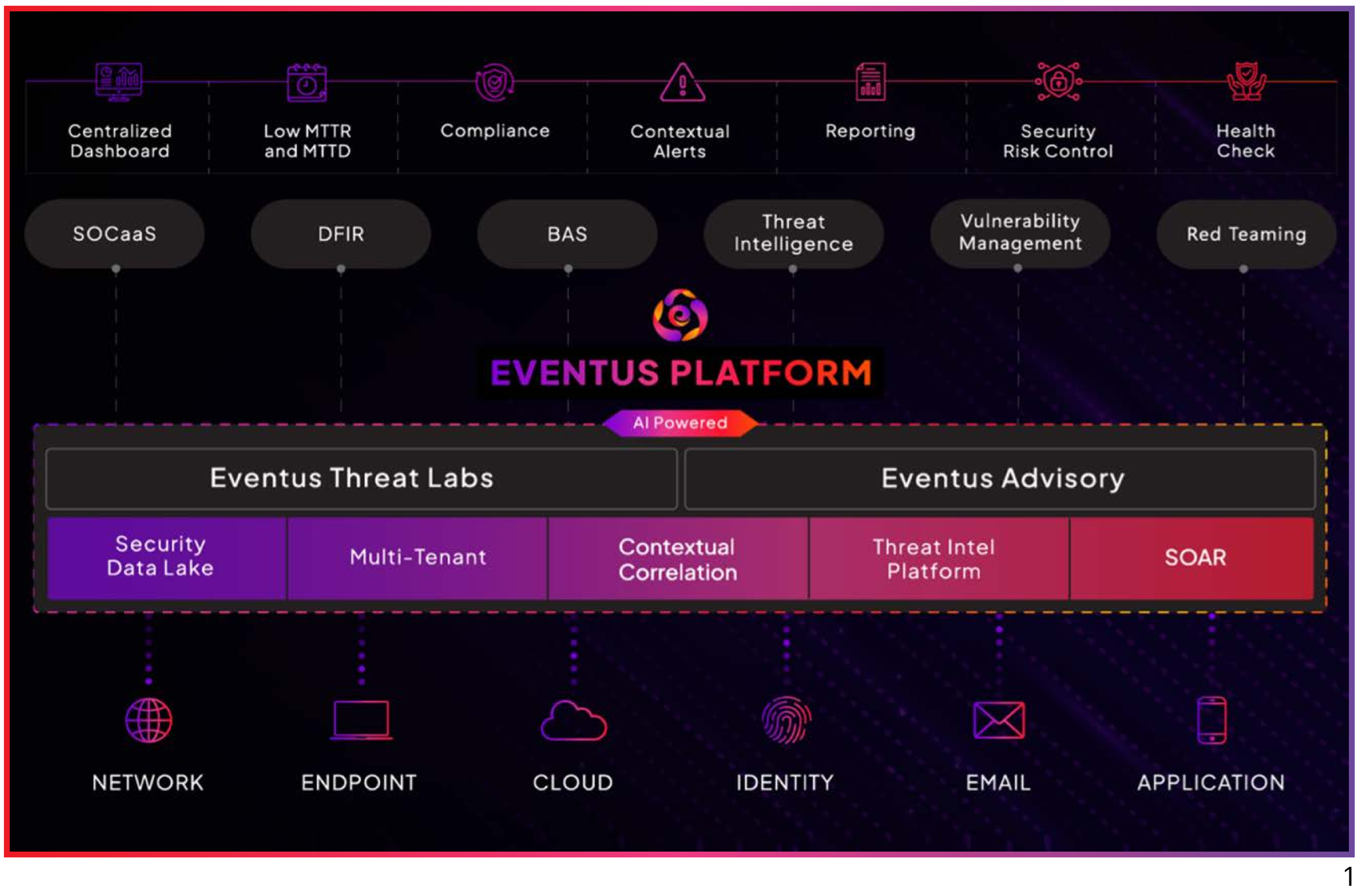
Unified Security, Unmatched Performance!

The Eventus Platform is a unified solution that delivers comprehensive managed security services. By integrating various functionalities and automation into a single robust system, it addresses security silos and reduces alert overload. This platform enables enterprises to manage, analyse, and respond to threats in near real-time.

Featuring a scalable microservice architecture, the Eventus Platform includes IAM, multi-level authentication, RBAC, AI-based playbooks, case management, and enhanced features like BAS, IR, VM, and real-time capabilities that ensures high security and compliance for our customers.

KEY BENEFITS

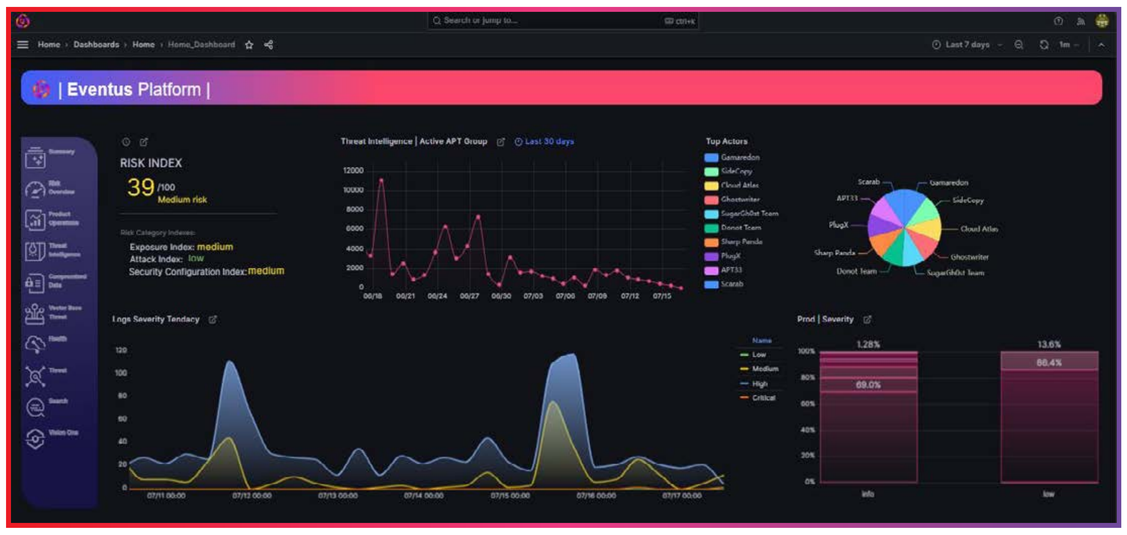
- Enhanced Security Posture
- Proactive Threat Mitigation
- Operational Efficiency
- Customizable Solutions
- Seamless integration with cloud and on-premises
- Compliance and Data Privacy
- Real-time threat intelligence and actionable insights
- Continuous Improvement
- Integrated IAM and robust RBAC



KEY FEATURES:

- **Security Data Lake:** *Centralized, Scalable, and Intelligent*

The Security Data Lake is part of the Eventus Platform, designed to manage vast amounts of security-related data. It centralizes storage, processing, and analysis of diverse data sources, including logs, events, and alerts, enhancing in-depth analysis and long-term trend identification for proactive threat detection and response. The platform ensures data isolation and encryption at all stages. Its powerful indexing and search functionalities enable quick access to historical data for forensic investigations and compliance reporting.



KEY HIGHLIGHTS

- Centralized Repository
- Scalable/Fail Proof/HA
- Advanced Indexing and Search
- Integration with AI and ML
- Data Encryption at all stages
- Long-term Trend Analysis
- Adhere to Local Compliance Practices

- **Contextual Correlation:** *Hyper-XDR for Unified Threat Detection & Response*

The Eventus Platform features advanced Hyper-XDR capabilities that enable sophisticated data correlation across multiple sources. By leveraging machine learning and AI, the platform identifies complex attack patterns and offers deep insights into potential threats. It supports robust on-prem log collection scalable to terabytes and seamless SaaS integration across multiple data centers. We use advanced aggregation and cross-vector correlation rules across identity, email, cloud, and campaign-based data, ensuring comprehensive threat detection and response.

Our platform is distinguished by contextual correlation and location-specific alerts, allowing the same alert to have different implications based on its origin, such as a LAN or a data centre server farm. For example, in a web application breach, Hyper-XDR correlates data from firewalls, endpoint detection systems, and network analysis tools to trigger automated responses like isolating endpoints and blocking malicious IPs.

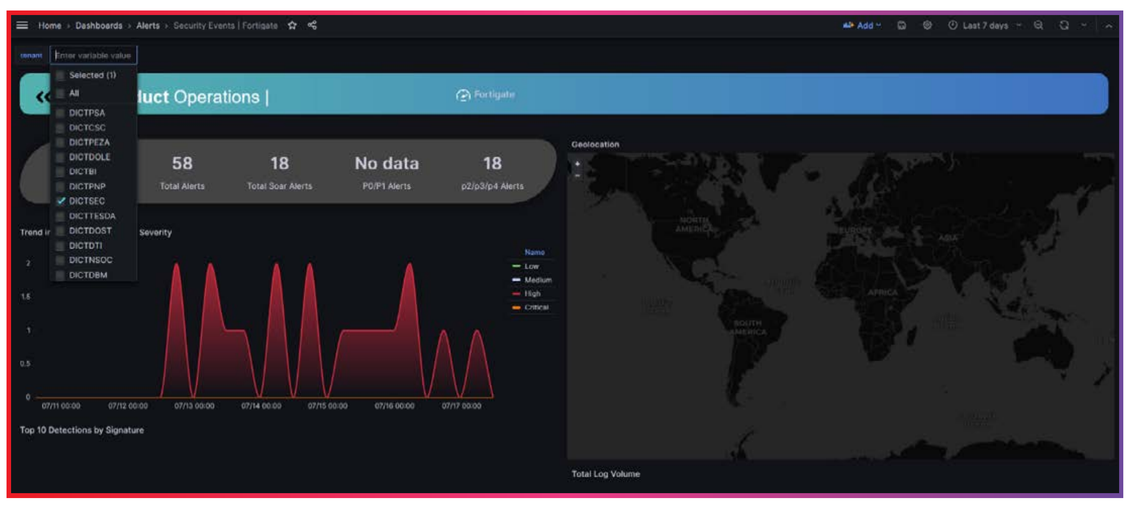
Rule Id	Rule Description	Rule Info			
112024	Spearphishing with malware download detected.	Rule ID : 119004 Description : File Download via PowerShell - Invoke-WebRequest Method Logtype : Endpoint Rule ID : 119011 Description : Shellcode execution via VBA Logtype : Endpoint	correlation	network	endpoint
112024	Spearphishing with malware download detected.	Rule ID : 119004 Description : File Download via PowerShell - Invoke-WebRequest Method Logtype : Endpoint Rule ID : 119011 Description : Shellcode execution via VBA Logtype : Endpoint	correlation	network	endpoint
112023	Ransomware Attack Detected.	Rule ID : 111513 Description : File size limit was exceeded Logtype : Network Rule ID : 119015 Description : Ransomware activity detected. Logtype : Endpoint	cross-correlation	network	endpoint
112023	Ransomware Attack Detected.	Rule ID : 111513 Description : File size limit was exceeded Logtype : Network Rule ID : 119015 Description : Ransomware activity detected. Logtype : Endpoint	cross-correlation	network	endpoint
112022	Credential Dumping : Unauthorized extraction of stored login credentials.	Rule ID : 111669 Description : Exceeded max AV memory Logtype : Network Rule ID : 119009 Description : Detects the DLL loading via UsoClient Logtype : Endpoint	cross-correlation	network	endpoint
112022	Credential Dumping : Unauthorized extraction of stored login credentials.	Rule ID : 111669 Description : Exceeded max AV memory Logtype : Network Rule ID : 119009 Description : Detects the DLL loading via UsoClient Logtype : Endpoint	cross-correlation	network	endpoint
112021	DLL injection: load malicious DLL into process.	Rule ID : 111636 Description : Infected file detected by the FortiGate unit and it passed Logtype : Network Rule ID : 119010 Description : Detects the DLL loading via UsoClient Logtype : Endpoint	cross-correlation	network	endpoint
112021	DLL injection: load malicious DLL into process.	Rule ID : 111636 Description : Infected file detected by the FortiGate unit and it passed Logtype : Network Rule ID : 119010 Description : Detects the DLL loading via UsoClient Logtype : Endpoint	cross-correlation	network	endpoint

KEY HIGHLIGHTS

- Advanced Hyper-XDR capabilities Machine learning and AI-driven data correlation
- Advanced aggregation, one-to-one, and cross-vector correlation rules
- Identity, email, cloud, and campaign-based data correlation
- Contextual correlation and location-specific alerts
- Unified detection and response system Automated threat mitigation

• **Multi-Tenant Support** *for Secure and Customized Management*

The Eventus Platform's multi-tenant support allows efficient management of multiple customers, providing each with a secure, isolated environment for their data and security operations. This architecture ensures data segregation, preventing cross-contamination and ensuring compliance with data privacy regulations. Key advantages include customized dashboards, reports, and alerting mechanisms tailored to each tenant. Robust RBAC enhances security by ensuring only authorized personnel access.



KEY HIGHLIGHTS

- Data Segregation
- Role-Based Access Control
- Scalability
- Enhanced Security
- Customized Dashboards and Reports
- Compliance with Data Privacy Regulations
- Centralized Management Interface
- Custom contextualization

• **Threat Intelligence and Labs:** *The Pillars of a Robust Cybersecurity Platform*

The Eventus Platform combines comprehensive threat intelligence with its Threat Labs division, providing a proven robust defence against cyber threats. This integrated approach ensures that organizations are always informed and prepared to address the latest security challenges, leveraging real-time data and The Eventus Platform combines comprehensive threat intelligence with its Threat Labs division, providing a proven robust defence against cyber threats. This integrated approach ensures that organizations are always informed and prepared to address the latest security challenges, leveraging real-time data and cutting-edge research for proactive threat management.

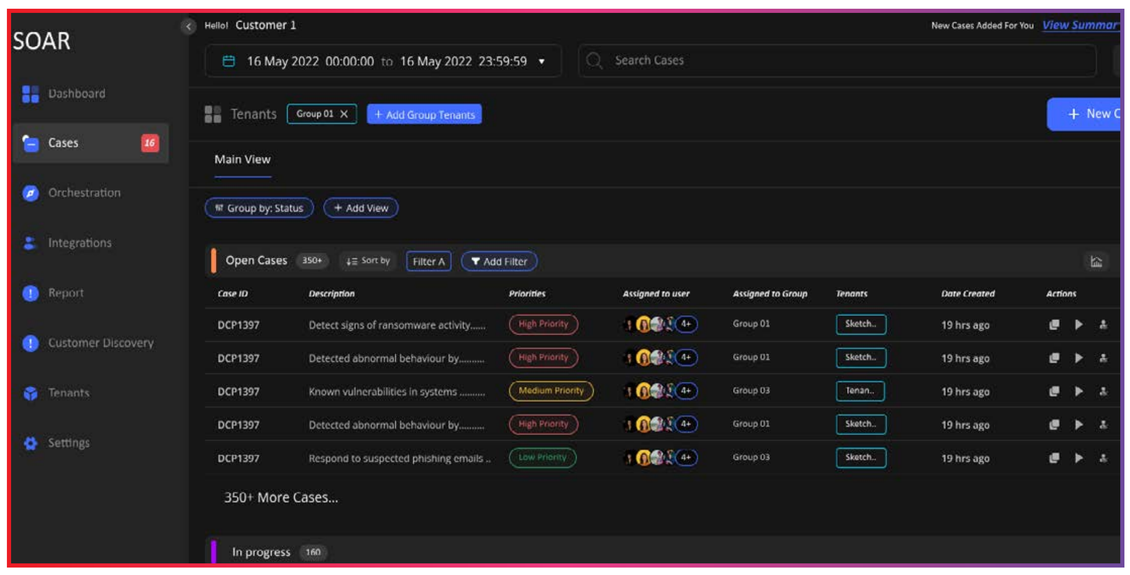
By combining the strengths of real-time threat intelligence and continuous threat research, the Eventus Platform ensures a comprehensive, proactive, and adaptive approach to cybersecurity, keeping organizations ahead of evolving threats.

KEY HIGHLIGHTS

- Real-Time Threat Insights
- Proactive Detection and Mitigation
- Advanced Threat Research
- Custom Rule Development
- Threat Actor-Based Visualization
- Threat Campaign-Based Visualization
- Automated Data Enrichment
- Collaboration with Global Intelligence Feeds
- Actionable Intelligence

• **SOAR:** *Transforming Security Operations Automation & Intelligence*

Eventus Platform SOAR (Security Orchestration, Automation, and Response) is a holistic solution for incident management, automation, and response, designed to enhance the efficiency and effectiveness of Security Operations Centres (SOCs). Leveraging advanced AI/ML algorithms, it provides real-time threat detection and response capabilities, integrating seamlessly with existing enterprise systems. SOAR reduces manual intervention, minimizes alert fatigue, and enables faster resolution of security incidents through automation and robust case management. Its scalable architecture supports multi-tenancy, ensuring secure and customized environments for different customers.



KEY HIGHLIGHTS

- Versatile Playbooks
- Multi-Tenancy
- Role-Based Visualization
- Curated Threat Intelligence
- Case Management
- Advanced Analytics and Reporting
- Custom Integrations with robust APIs
- AI/ML-Powered Insights
- Reduced Alert Fatigue

• **AI-Powered/Augmented Security** *for Predictive Threat Detection and Response*

Eventus Platform Utilises AI-driven analytics as the platform processes vast amounts of security data in near real-time, identifying patterns and anomalies that indicate potential threats. This precision and speed surpass traditional methods. With large language models (LLMs) and advanced ML algorithms, the platform continuously learns and adapts to evolving threats.

A key advantage is predictive analytics, which analyses historical data to anticipate potential security incidents before they occur. This proactive approach helps mitigate threats and reduce overall risk. For example, the platform can detect subtle signs of an impending ransomware attack by correlating seemingly unrelated events, providing timely alerts and enabling pre-emptive measures.

Contact us at

sales@eventussecurity.com

www.eventussecurity.com