eventus

eventussecurity.com

SOC AS A SERVICE

Upgrade Your Security with our XDR Powered SOC!

To defend against today's advanced threat requires proactive monitoring and analyzing of large amount of data. Most of the organization have security tools generating lot of data but they lack capability making real sense or drive value from it, which needs automation to process it as it as quickly as possible.

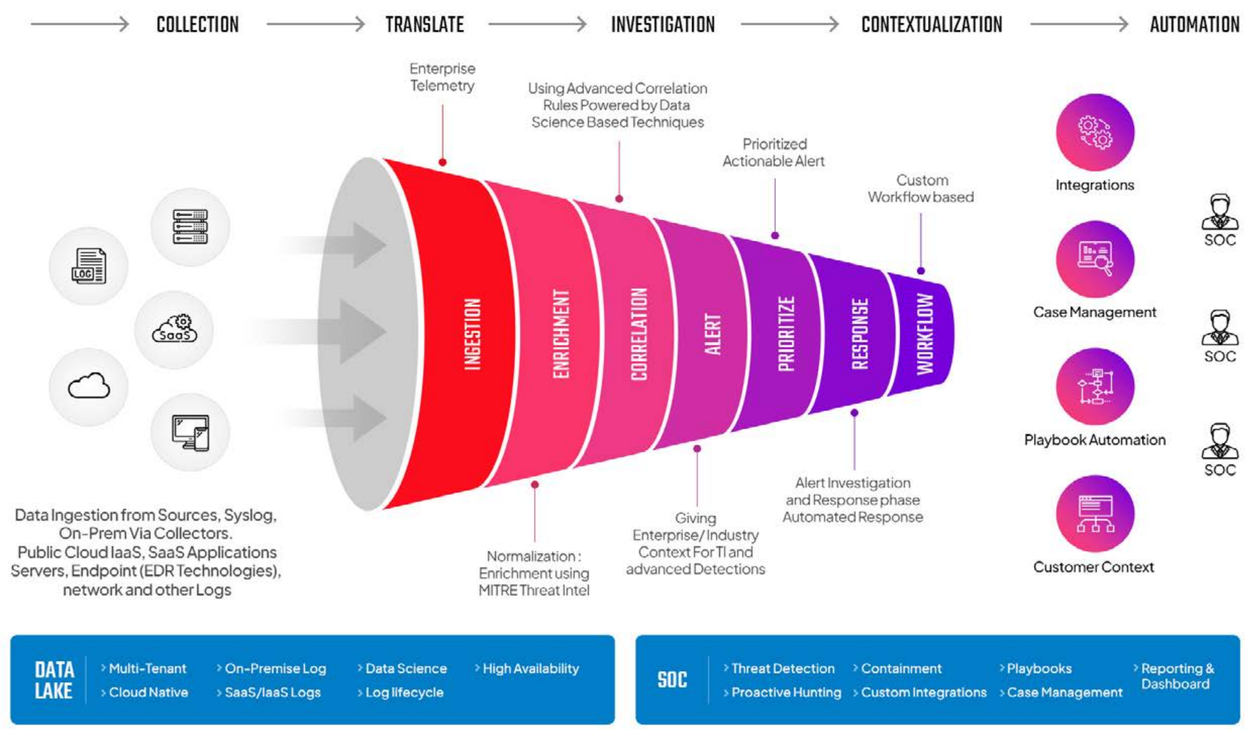
Eventus uses proprietary Security Operations Platform with Advanced Proactive Threat Hunting capabilities combined with 24/7 monitoring and response services to deliver threat detection and response capabilities. Platfrom uses automation driven playbooks for enrichment and response. Enables proactive threat detection using third party, community and proprietary threat intelligence

ADVANTAGES OF EVENTUS SOCAAS

1. Realtime Threat Detection and Response
2. Optimizing existing Products Detection capabilities
3. Cost Reduction and SecOps Manpower
4. Proactive Threat Hunting and Prevention
5. Global Threat Intel led Detection and Response Capabilites

KEY BENEFITS

- **Monitoring and Alert Management**
  Eventus SOCaaS platform excels in efficiently collecting, normalizing, enriching extensive telemetry data from various sources including endpoints, networks, etc. The data captured is further correlated using advanced data science-based technologies to ensure that only high-fidelity, actionable alerts are delivered to you.
- **Containment and Response**
  The SOCaaS team conducts in-depth investigations to identify the root cause, assess the impact, and determine appropriate remediation steps. Immediate response actions, such as containment, are taken based on Critical Asset and Approval workflows designed during the integration and onboarding. With our SecOps Platform, we automate process-oriented workflows, enabling faster and flawless execution of repetitive tasks.
- **Threat Intelligence and Research**
  Eventus Security leverages feeds from its Threat Research Lab to deliver contextual and proactive detection and response using various methods include IOC sweeping, MITRE ATT$CK TTP mapping, and other valuable global feeds.



KEY DELIVERABLES

EVENTUS SOC AS A SERVICE

- Automation/Orchestration
- Out of Box Integrations
- Chained Playbooks
- Personalized Use Cases
- Security Consultation
- Guidance, Best practices, and Recommendations
- Health Checks
- Reporting on security incidents, threats
- Specialized onboarding

ADVANCE THREAT DETECTION

- 50+ In built Connectors and in- house Integration team
- 24/7 Security Alert Monitoring
- Realtime Threat Detection by analyzing ingested logs
- Continuous monitoring of networks, systems, and applications for security events and anomalies.
- Real-time monitoring of logs, alerts, and other security data sources.
- Identify malicious activities and indicators of compromise (IOCs)
- Native and 3rd Party Threat Intelligence
- Integrated Case Management
- Customized Threat Rules

XDR DRIVEN SOC

- Contain and Mitigate the impact.
- Follow incident response procedures conduct investigations, and work to remediate the incident while minimizing downtime and data loss.
- Handling security incidents.
  - Incident triage
  - Classification
  - Prioritization
  - Tracking,
  - Documentation
- Integration with Ticketing tool for custom approval and workflow

XDR DRIVEN SOC

- Network Telemetry
- 0365 Telemetry
- Endpoint Telemetry
- Cloud Telemetry

LOG MANAGEMENT & OPTIMIZATION

- Collect, Aggregate, and Analyze logs from various sources within organization’s
- environment.
- Provides historical analysis, visualizations and tiered data storage that optimizes
- performance.

  Provide Log Storage and retention for analysis and Threat Hunting
- Provides historical analysis, visualizations and tiered data storage that optimizes
- performance.

ACTIONABLE INTELLIGENCE

- Proactive threat hunting
- Adversary mapping
- Threat advisories
- MITRE ATT&CK Mapping
- Threat Indicators

KEY DELIVERABLES

EVENTUS SOC AS A SERVICE

- Automation/Orchestration
- Out of Box Integrations
- Chained Playbooks
- Personalized Use Cases
- Security Consultation
- Guidance, Best practices, and Recommendations
- Health Checks
- Reporting on security incidents, threats
- Specialized onboarding

ADVANCE THREAT DETECTION

- 50+ In built Connectors and in- house Integration team
- 24/7 Security Alert Monitoring
- Realtime Threat Detection by analyzing ingested logs
- Continuous monitoring of networks, systems, and applications for security events and anomalies.
- Real-time monitoring of logs, alerts, and other security data sources.
- Identify malicious activities and indicators of compromise (IOCs)
- Native and 3rd Party Threat Intelligence
- Integrated Case Management
- Customized Threat Rules

XDR DRIVEN SOC

- Contain and Mitigate the impact.
- Follow incident response procedures conduct investigations, and work to remediate the incident while minimizing downtime and data loss.
- Handling security incidents.
  - Incident triage
  - Classification
  - Prioritization
  - Tracking,
  - Documentation
- Integration with Ticketing tool for custom approval and workflow

XDR DRIVEN SOC

- Network Telemetry
- 0365 Telemetry
- Endpoint Telemetry
- Cloud Telemetry

LOG MANAGEMENT & OPTIMIZATION

- Collect, Aggregate, and Analyze logs from various sources within organization’s
- environment.
- Provides historical analysis, visualizations and tiered data storage that optimizes
- performance.
  Provide Log Storage and retention for analysis and Threat Hunting
- Provides historical analysis, visualizations and tiered data storage that optimizes
- performance.

ACTIONABLE INTELLIGENCE

- Proactive threat hunting
- Adversary mapping
- Threat advisories
- MITRE ATT&CK Mapping
- Threat Indicators

By partnering with an SOCaaS, organizations can leverage their expertise and resources to effectively operationalize XDR. SOCaaS alleviates the burden of managing and maintaining the XDR platform, allowing organizations to focus on their core business while ensuring comprehensive threat detection and response capabilities.

WHAT DO WE OFFER?

Contact us at

sales@eventussecurity.com

www.eventussecurity.com