PRODUCT SHEET

Advantal™

ADVANTAL SECURITY OPERATIONS PLATFORM

Integrated SIEM, SOAR, UEBA & Threat Intelligence

Unified detection, investigation, automation, response, and compliance operations for large-scale enterprise, cloud, and critical infrastructure environments.

Advantal Security Operations Platform is a modular, scalable, and integrated SIEM and SOAR platform designed for centralized security monitoring, investigation, response orchestration, compliance reporting, and long-term log governance. The platform combines high-speed log ingestion, real-time analytics, behavioral detection, case management, automation playbooks, threat intelligence, and forensic search in one security operations environment.

Built for hybrid and distributed environments, the platform supports collection and correlation of logs, events, alerts, and telemetry from network devices, servers, endpoints, databases, applications, cloud platforms, and security tools through agent-based, agentless, API-driven, and flow-based ingestion models.

WHY THIS MATTERS

Modern SOC operations require more than event visibility. Security teams need one controlled platform to ingest telemetry across infrastructure and cloud, detect threats in real time, investigate incidents with context, automate response actions, monitor SLA performance, and retain logs across searchable and archival storage tiers.

VALUE PILLARS

Unified SIEM and SOAR operations

One platform for log management, analytics, incident investigation, case handling, playbook-driven response, and continuous security operations.

Scalable data and detection architecture

Supports distributed ingestion, clustered deployment, horizontal growth in EPS capacity, and tiered storage planning for large operational environments.

Detection with context

Combines rule-based correlation, UEBA, threat intelligence enrichment, MITRE ATT&CK mapping, dashboards, and forensic search for faster triage and investigation.

Response with control

Enables case assignment, escalation workflows, automated containment actions, and third-party security tool orchestration through APIs and playbooks.

PLATFORM CAPABILITIES

Integrated SIEM + SOAR Architecture

The platform is designed as an integrated security operations environment with modular functional layers for collection, normalization, correlation, analytics, investigation, orchestration, response, reporting, and storage lifecycle management. It supports scalable deployment across primary and disaster recovery environments.

Log Collection and Ingestion Coverage

Supports centralized collection from heterogeneous sources including:

- network and security devices
- servers and operating systems
- endpoints
- databases
- enterprise applications
- cloud platforms
- identity systems
- virtualized and containerized infrastructure
- third-party security tools

Collection methods support both **agent-based and agentless log collection mechanisms.** Supported ingestion methods include **Syslog, SNMP, WMI, REST API, NetFlow, sFlow, and IPFIX,** along with vendor connectors and native integration methods where applicable.

Dashboards, Monitoring, and Compliance Reporting

Role-based dashboards provide customizable operational views for SOC analysts, incident managers, administrators, and leadership teams. The platform supports real-time monitoring, investigation panels, executive summaries, SLA views, and compliance-oriented reporting aligned to common frameworks such as ISO 27001, PCI-DSS, GDPR, and other organizational or regulatory reporting needs.

Centralized Retention and Search

Advantal supports centralized log retention with configurable storage tiers including hot, warm, and cold retention strategies. Retention periods are policy-driven and can be configured to support operational, regulatory, DC/DR, and archival requirements, including long-duration retention and searchable history.

SECURITY OPERATIONS, INCIDENT RESPONSE, AND AUTOMATION

Incident and Case Management

The platform includes built-in incident management and case management capabilities for triage, ownership, enrichment, assignment, escalation, investigation tracking, and closure governance. Cases can be linked to alerts, observables, assets, response history, threat intelligence, and actions executed during containment and remediation.

SOAR and Playbook Automation

Advantal includes **playbook-based automation for incident response (SOAR)** to support guided and automated workflows for alert enrichment, validation, containment, ticketing, escalation, and coordinated response across integrated tools. Graphical and logic-driven playbooks can trigger investigative steps and operational actions based on rule outcomes, severity, asset criticality, and threat context.

Automated Response Actions

The platform supports automated and operator-approved actions such as:

- block IP
- disable user
- isolate endpoint
- update firewall or security policy
- initiate ticket or case workflow
- notify response teams
- trigger enrichment or quarantine actions through integrated systems

Third-Party Security Tool Integration

Supports integration with firewalls, EDR, IPS, WAF, DLP, identity systems, ticketing systems, email systems, cloud services, and other external enterprise or security platforms through connectors, APIs, and orchestration workflows. Threat intelligence ingestion supports **STIX/TAXII and other open standards**. REST APIs support bidirectional integration with external systems.

Identity, Access, and Role Governance

The platform supports **RBAC with granular role definitions**, enabling role-based control over data visibility, dashboards, configuration, response actions, and administration. It supports integration with **AD/LDAP and MFA systems** for enterprise authentication and controlled access.

ARCHITECTURE, SCALE, STORAGE, AND SECURITY

High Availability and Scalability

The platform supports high availability and clustering for resilient security operations. Collection, analytics, storage, and application tiers can be scaled horizontally to support growth in ingestion rate, data volume, and processing demand. The architecture is suited for environments requiring minimum **20,000 EPS with ability to scale up to 40,000 EPS** through scale-out design.

Storage and Retention Model

The solution can be architected with **500 TB of storage for logging purpose (Hot 100 TB / Warm 200 TB / Cold 200 TB)** based on the required deployment sizing and retention model. It supports minimum **1-year searchable log retention + 5-year archive**, with policy-driven lifecycle movement between indexed, nearline, and archival tiers.

Centralized Monitoring and Correlation

The platform is designed to integrate infrastructure, network, security, cloud, and application logs into a single SIEM environment for centralized monitoring, analytics, alerting, investigation, and correlation across DC and DR operations.

Forensic Search and Threat Visibility

Indexed and retained event data supports forensic search across historical logs, alerts, entities, and incidents. Search workflows support deep investigation, cross-source pivoting, and structured analysis of events across dual-stack and distributed environments.

Cloud, Multi-Tenant, and Network Readiness

Supports monitoring and integration across **AWS, Azure, GCP, and private cloud deployments**. The platform also supports **multi-tenancy for DC/DR environments** and segregated operational views where required. It is designed for both **IPv4 and IPv6 environments.**

Data Protection and Cryptographic Controls

The platform supports encryption for data in transit and at rest, including secure transport using **TLS 1.2/1.3** and storage protection using **AES-256** or equivalent deployment-aligned controls. Cryptographic implementation can be aligned to **FIPS 140-2/140-3 validated cryptographic modules or equivalent** and supports security architectures requiring cryptographic controls aligned with **ISO/IEC 19790** expectations.

THREAT INTELLIGENCE, REPORTING, ASSET VISIBILITY, AND SUPPORT

Threat Intelligence and ATT&CK Mapping

The platform ingests and processes external and internal threat intelligence feeds for enrichment, prioritization, and automated response workflows. Detection and incident views can be aligned to the **MITRE ATT&CK framework** for analyst context, reporting clarity, and security operations mapping.

Alerting, Reporting, and SLA Visibility

Supports alerting and reporting through **Email, SMS, and Webhooks.** Dashboards and reports can be configured for operational visibility, incident metrics, compliance views, and management reporting. The platform also provides **dashboard for SLA** monitoring of **incident response**, including workload tracking, response timing, escalation visibility, and measurable SOC performance indicators such as MTTD and MTTR.

Asset Discovery and Monitoring

The solution supports **automatic discovery/grouping of devices and applications with predefined monitoring templates collecting performance metrics** including CPU, memory, disk, interfaces, processes, and related infrastructure indicators. This enables broader asset context for security operations, prioritization, and investigation workflows.

OEM Support and Service Continuity

Advantal provides minimum **5 years OEM support with defined SLA (response, resolution, updates)** as part of long-term deployment support, platform maintenance, product updates, and operational continuity planning.

Advantal™

WHY ADVANTAL

Security operations focused

Built to unify SIEM, SOAR, UEBA, threat intelligence, incident handling, and operational governance in one platform.

Designed for large-scale environments

Structured for high-ingestion deployments, DC/DR readiness, multi-year retention, and controlled growth from day one.

Open and integration-ready

Supports security ecosystem interoperability across enterprise, cloud, identity, and operational tooling.

Compliance and response aligned

Combines visibility, reporting, workflow, and response automation in a form suited for regulated and always-on operational environments.

CONTACT FOR SUPPORT

Corporate Office
Unit No. 527 and 528, 5th Floor, Vipul Trade Centre, Sector 48, Sohna Road, Gurugram, Haryana – 122018, India

Development Center
17-A, Electronic Complex, Pardesipura, Indore - 452010, Madhya Pradesh

For Sales Assistance
sales@advantal.net

kartikay.shukla@advantal.net
+91-9971161261

www.advantaltechnologies.com