DATA SHEET

VERVE OT/ICS SIEM

Detect and rapidly respond to OT/ICS cyber threats

SUMMARY

Security Information and Event Management (SIEM) is a critical element in the detection of potential security threats.

The Verve SIEM was built for OT/ICS environments to include specific OT/ICS analysis and integrate with critical operating data such as device performance and DCS/ICS alarms to enable comprehensive response for security and reliability.

> WE DID A COMPLETE COMPETITIVE ANALYSIS AND CHOSE VERVE. IT HAS ALLOWED US TO DOUBLE OUR NIST CSF MATURITY IN 18 MONTHS.
>
> **- CYBER COMPLIANCE & SECURITY SPECIALIST**
> LARGE GENERATION & TRANSMISSION CO-OP

THE VERVE DIFFERENCE

Endpoint Focused

Verve is the only OT/ICS SIEM that goes directly to endpoints to gather log, syslog and performance data. This enables true host-level security and reliability analytics.

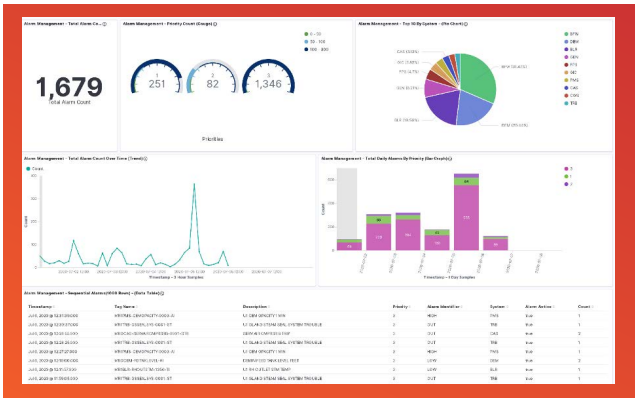
Integrated Response

Verve's integrated platform allows users to quickly pivot from real-time alert data to endpoint status (on items such as users, ports, software) AND enables immediate response through integrated actions.

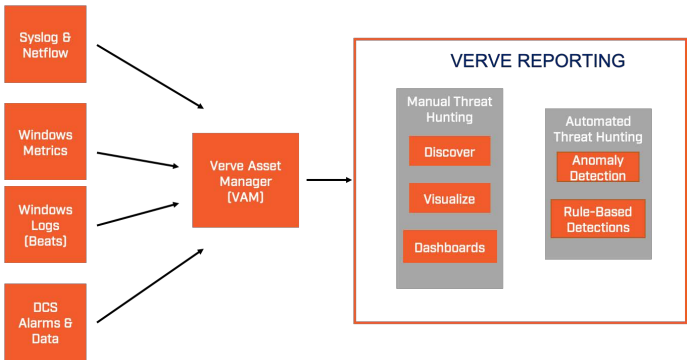
OT/ICS Process Data

Verve's SIEM is built specifically for OT/ICS environments, including the ability to bring ICS/DCS process alarm data into the same database and user interface to improve analysis and response.

VERVE



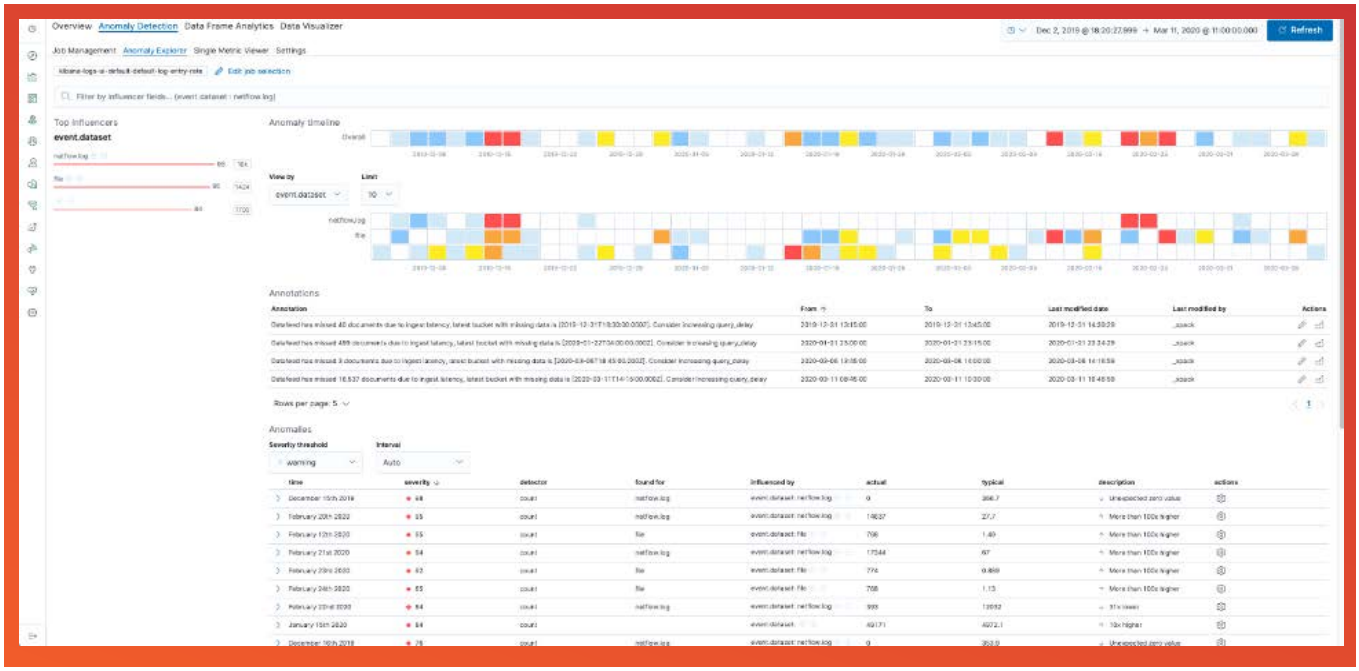
integrated DCS/ICS Alarm Data



Multiple Source Integration

FEATURES

- Ingest wide range of endpoint data: logs, syslog, Netflow, metrics
- Integrate DCS/ICS process alarm data for improved response
- Advanced machine learning engine to identify anomalous patterns
- Time analysis to track and reverse engineer incidents
- Built-in detections for MITRE ATT&CK, NERC CIP and others
- Improved analyst triage by all-in-one alert investigation with integrated asset inventory
- Integrated with response actions in Verve platform enables faster mean time to response



Pre-Built Detections