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.

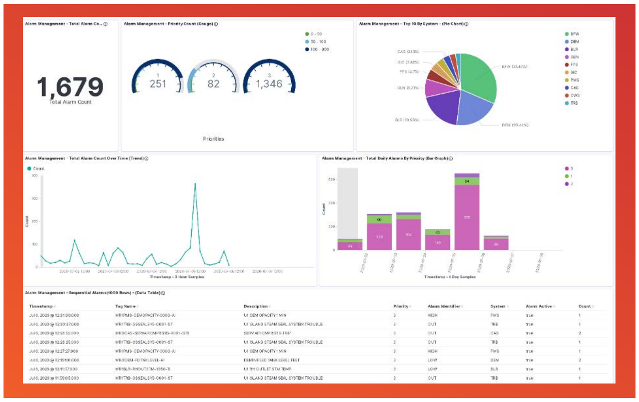
Integrated Response

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.

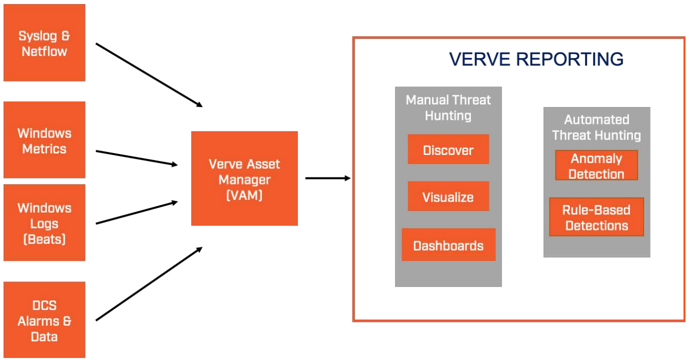
OT/ICS Process Data

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
A ROCKWELL AUTOMATION COMPANY



integrated DCS/ICS Alarm Data


Syslog & Netflow

Windows Metrics

Windows Logs (Beats)

DCS Alarms & Data

Verve Asset Manager (VAM)

VERVE REPORTING

Manual Threat Hunting

Discover

Visualize

Dashboards

Automated Threat Hunting

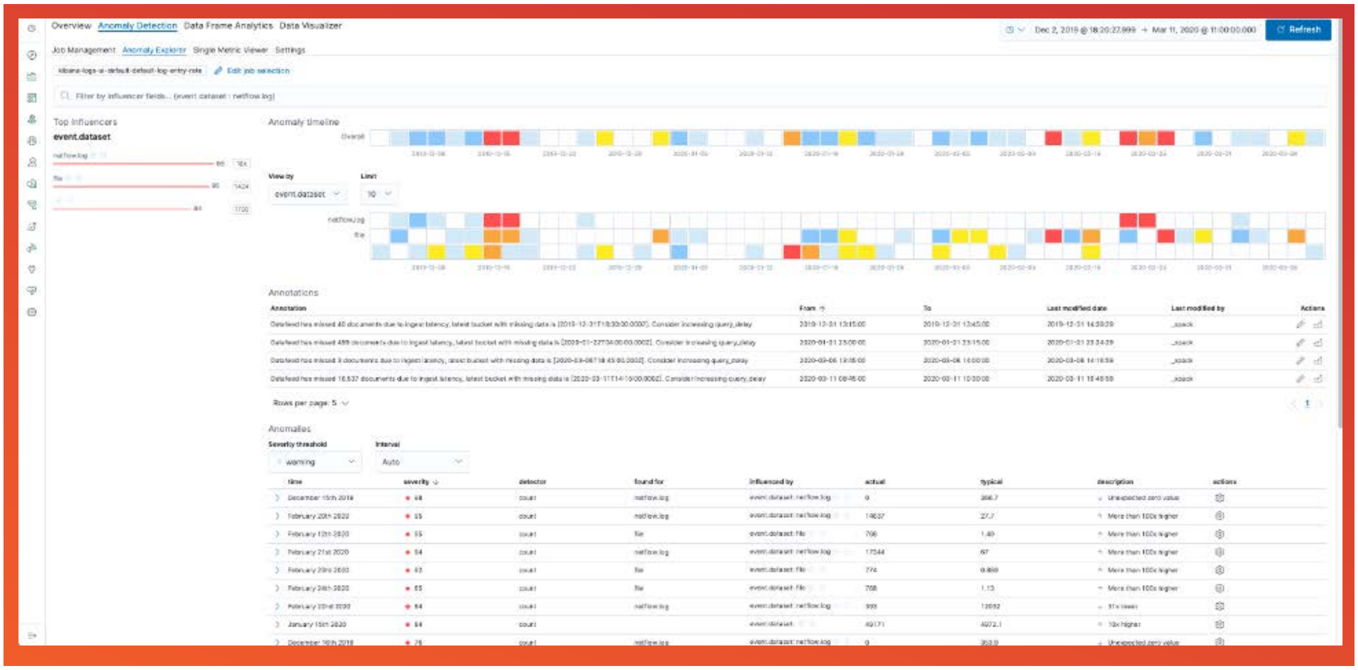
Anomaly Detection

Rule-Based Detections

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



Dec 2, 2019 @ 18:20:22.999 → Mar 11, 2020 @ 11:00:00.000

View by: event.dataset

Limit: 10

Annotations

Annotation	From	To	Last modified date	Last modified by	Actions
Datafeed has missed 40 documents due to ingest latency, latest bucket with missing data is [2019-12-31T18:30:00.000Z]. Consider increasing query_delay	2019-12-31 13:15:00	2019-12-31 13:45:00	2019-12-31 14:30:29	_xpack	
Datafeed has missed 499 documents due to ingest latency, latest bucket with missing data is [2020-01-22T04:00:00.000Z]. Consider increasing query_delay	2020-01-21 23:00:00	2020-01-21 23:15:00	2020-01-21 23:24:29	_xpack	
Datafeed has missed 3 documents due to ingest latency, latest bucket with missing data is [2020-03-06T18:45:00.000Z]. Consider increasing query_delay	2020-03-06 13:15:00	2020-03-06 14:00:00	2020-03-06 14:18:59	_xpack	
Datafeed has missed 18,537 documents due to ingest latency, latest bucket with missing data is [2020-03-11T14:15:00.000Z]. Consider increasing query_delay	2020-03-11 08:45:00	2020-03-11 10:30:00	2020-03-11 10:48:59	_xpack	

Rows per page: 5

Anomalies

Severity threshold: warning

Interval: Auto

time	severity	detector	found for	influenced by	actual	typical	description	actions
December 15th 2019	68	count	netflow.log	event.dataset: netflow.log	0	366.7	Unexpected zero value	
February 20th 2020	55	count	netflow.log	event.dataset: netflow.log	14637	27.7	More than 100x higher	
February 12th 2020	55	count	file	event.dataset: file	706	1.40	More than 100x higher	
February 21st 2020	54	count	netflow.log	event.dataset: netflow.log	17344	67	More than 100x higher	
February 23rd 2020	52	count	file	event.dataset: file	774	0.869	More than 100x higher	
February 24th 2020	55	count	file	event.dataset: file	768	1.13	More than 100x higher	
February 22nd 2020	54	count	netflow.log	event.dataset: netflow.log	993	13092	31x lower	
January 15th 2020	54	count		event.dataset:	49171	4072.1	10x higher	
December 16th 2019	76	count	netflow.log	event.dataset: netflow.log	0	353.9	Unexpected zero value	

Pre-Built Detections

To learn more, visit us at www.VerveIndustrial.com or contact us at info@verveindustrial.com