GE VERNOVA

FACTSHEET

GE Vernova's Cybersecurity Platform - OTArmor

SECURITY DATA ENRICHMENT

CENTRALIZED LOG MANAGEMENT WITH VISIBILITY OPERATOR DASHBOARD

GE Vernova's cybersecurity platform security data enrichment solution includes a base platform for centralization of log collection, log retention and cybersecurity Incident response activities. The centralized log management solution collects logs and security related information from devices which support the ability to forward log data. Devices to log will include network switches, workstations, servers, controller(s), Network Intrusion Detection servers and firewalls. The log management solution provides a single, centralized, and real-time display of activity throughout the plant network to support event correlation and analysis.

UNIQUE FEATURES:

- GE Vernova's cybersecurity platform is equipped with an OT purpose-built operator's dashboard designed by GE Vernova to help with quick Threat analysis by operators.
- This centralized log management solution module is designed to forward logs to a centralized SOC (Security Operations Center) if required.

BENEFITS:

- Enables compliance with regulatory standards such as NERC CIP
- Alerts and reports log-based cybersecurity anomalies
- Decreases the dwell time for incident response
- Reduces security analyst fatigue

SECURITY DATA ENRICHMENT

Operator cyber security dashboard

Implements the following tools:

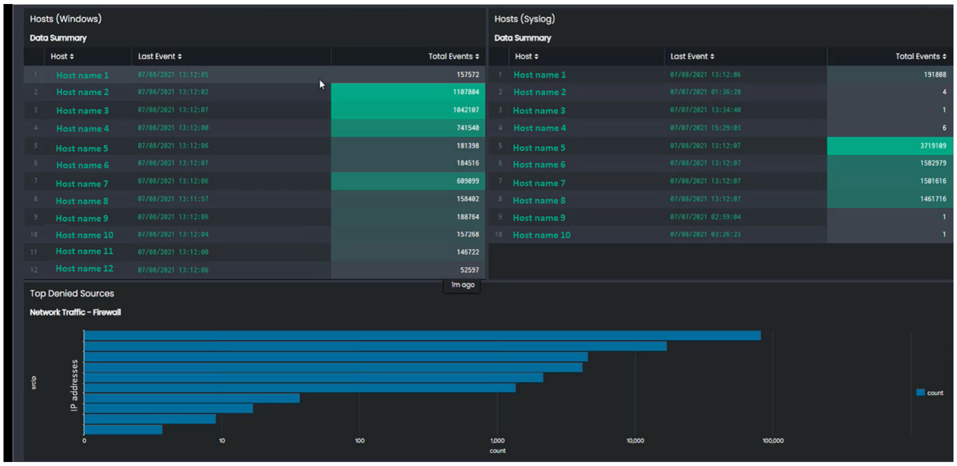
- Anomaly detection
- Compliance scoring
- Intrusion detection
- Change detection

Combining the above visual alerts with standard log collection for:

- Access control breaches (ex. wrong password, non-privileged access, etc.)
- Endpoint protection breaches (ex. Virus detection, application allow listing visual alert, block listed USB inserted, etc.)
- Disaster recovery system visual alerts (ex. system failed to backup)

GE Vernova's **industrial purposed** operator cybersecurity dashboards are designed to provide an interactive and easy user experience. The dashboards can be customized and help the plant security administrator to quickly run security checks by having the correlation of the **vendor agnostic** aggregated logs from the security modules listed above.

The causality designed within the dashboards will help running quick incident analysis and identifying whether a more complex expert analysis is required.



Hosts (Windows)

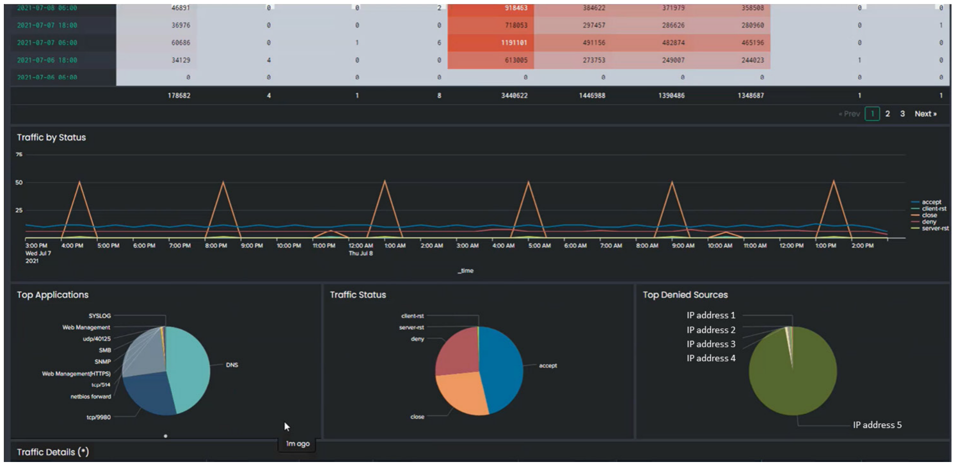
Data Summary

	Host ⇕	Last Event ⇕	Total Events ⇕
1	Host name 1	07/08/2021 13:12:05	157572
2	Host name 2	07/08/2021 13:12:02	1107804
3	Host name 3	07/08/2021 13:12:07	1042107
4	Host name 4	07/08/2021 13:12:00	741540
5	Host name 5	07/08/2021 13:12:06	181398
6	Host name 6	07/08/2021 13:12:07	184516
7	Host name 7	07/08/2021 13:12:06	609099
8	Host name 8	07/08/2021 13:11:57	158402
9	Host name 9	07/08/2021 13:12:06	188764
10	Host name 10	07/08/2021 13:12:04	157268
11	Host name 11	07/08/2021 13:12:00	146722
12	Host name 12	07/08/2021 13:12:06	52597

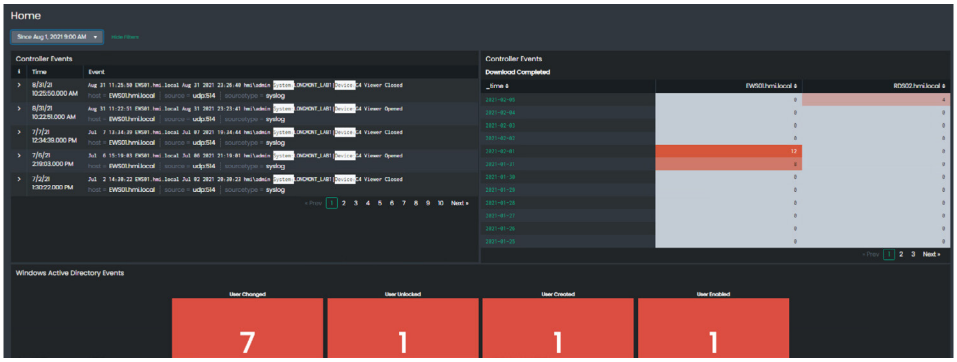
Hosts (Syslog)

Data Summary

	Host ⇕	Last Event ⇕	Total Events ⇕
1	Host name 1	07/08/2021 13:12:06	191808
2	Host name 2	07/07/2021 01:36:28	4
3	Host name 3	07/07/2021 13:34:40	1
4	Host name 4	07/07/2021 15:29:03	6
5	Host name 5	07/08/2021 13:12:07	3719109
6	Host name 6	07/08/2021 13:12:07	1582979
7	Host name 7	07/08/2021 13:12:07	1501616
8	Host name 8	07/08/2021 13:12:07	1461716
9	Host name 9	07/07/2021 02:59:04	1
10	Host name 10	07/08/2021 03:26:23	1



2021-07-08 06:00	46891	0	0	2	918463	384622	371979	358508	0	0
2021-07-07 18:00	36976	0	0	0	718053	297457	286626	280960	0	1
2021-07-07 06:00	60686	0	1	6	1191101	491156	482874	465196	0	0
2021-07-06 18:00	34129	4	0	0	613005	273753	249007	244023	1	0
2021-07-06 06:00	0	0	0	0	0	0	0	0	0	0
	178682	4	1	8	3440622	1446988	1390486	1348687	1	1



Home

Controller Events

i	Time	Event
>	8/31/21 10:25:50.000 AM	Aug 31 11:25:50 EWS01.hmi.local Aug 31 2021 23:26:40 hmi\admin System:LONGMONT_LAB1|Device:C4 Viewer Closed host = EWS01.hmi.local | source = udp:514 | sourcetype = syslog
>	8/31/21 10:22:51.000 AM	Aug 31 11:22:51 EWS01.hmi.local Aug 31 2021 23:23:41 hmi\admin System:LONGMONT_LAB1|Device:C4 Viewer Opened host = EWS01.hmi.local | source = udp:514 | sourcetype = syslog
>	7/7/21 12:34:39.000 PM	Jul 7 13:34:39 EWS01.hmi.local Jul 07 2021 19:34:44 hmi\admin System:LONGMONT_LAB1|Device:C4 Viewer Closed host = EWS01.hmi.local | source = udp:514 | sourcetype = syslog
>	7/6/21 2:19:03.000 PM	Jul 6 15:19:03 EWS01.hmi.local Jul 06 2021 21:19:01 hmi\admin System:LONGMONT_LAB1|Device:C4 Viewer Opened host = EWS01.hmi.local | source = udp:514 | sourcetype = syslog
>	7/2/21 1:30:22.000 PM	Jul 2 14:30:22 EWS01.hmi.local Jul 02 2021 20:30:23 hmi\admin System:LONGMONT_LAB1|Device:C4 Viewer Closed host = EWS01.hmi.local | source = udp:514 | sourcetype = syslog

Controller Events

Download Completed

_time ⇕	EWS01.hmi.local ⇕	RDS02.hmi.local ⇕
2021-02-05	0	4
2021-02-04	0	0
2021-02-03	0	0
2021-02-02	0	0
2021-02-01	12	0
2021-01-31	8	0
2021-01-30	0	0
2021-01-29	0	0
2021-01-28	0	0
2021-01-27	0	0
2021-01-26	0	0
2021-01-25	0	0

Windows Active Directory Events

User Changed	User Unlocked	User Created	User Enabled
7	1	1	1

KEY FEATURES

- Industrial purposed dashboards
- Visual alerts per severity for:
  - Anomaly detection
  - Endpoint protection breach
  - Policy compliance breach
  - Network intrusion detection
  - Change management
  - Backup & restore
- Security event logging
- Access management logging
- OT asset inventory
- Performance statistics
  - Network traffic
  - Sensor health status

GE VERNOVA

gevernova.com

Information contained in this document is indicative. No representation or warranty is given or should be relied on. Information provided is subject to change without notice.