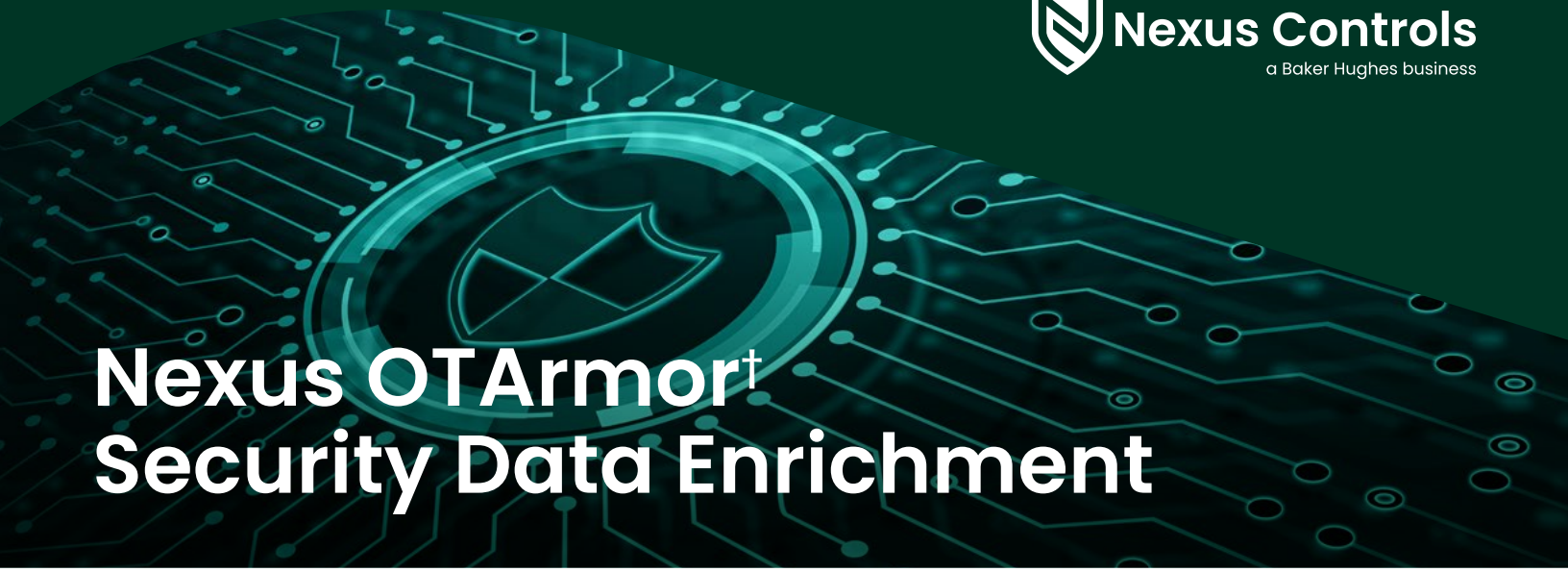
Nexus Controls
a Baker Hughes business



Nexus OTArmor†
Security Data Enrichment

Centralized log management with visibility operator dashboard

The Nexus **OTArmor** 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:

- The Nexus **OTArmor** is equipped with an OT purpose-built operator's dashboard designed by Nexus Controls 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:

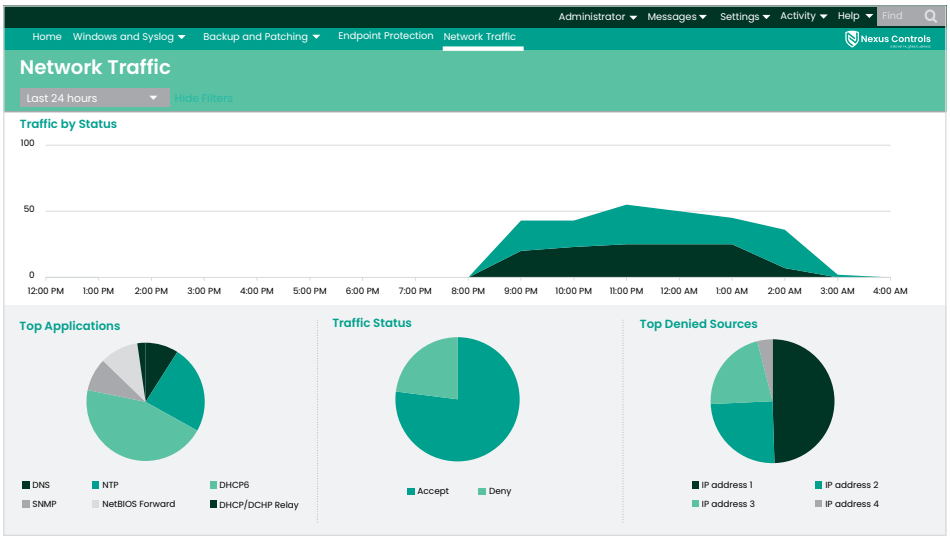
- Access control breaches (ex. wrong password, non-privileged access, etc.)
- Endpoint protection breaches (ex. Virus detection, application allow listing visual alert, block listed USB inserted, etc.)
- Disaster recovery system visual alerts (ex. system failed to backup)

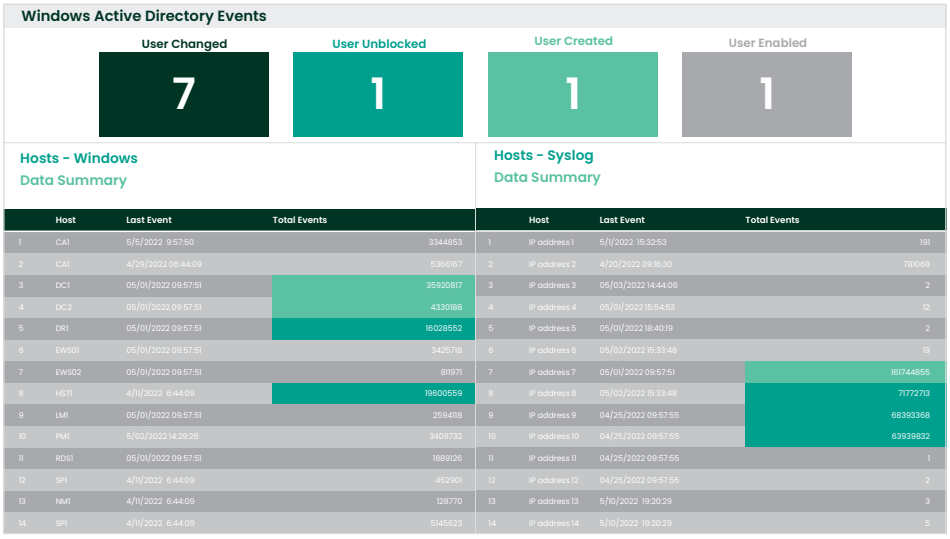
The Nexus Controls **industrial purposed** "Operator Cybersecurity Dashboards" are designed to provide an interactive and easy UX. The dashboards can be customized and help the plant security administrator to quickly run security checks by having the correlation of the **vendor agnostic** aggregated 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.

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





	Host	Last Event	Total Events
1	CA1	5/5/2022 9:57:50	3344853
2	CA1	4/29/2022 06:44:09	5366167
3	DC1	05/01/2022 09:57:51	35920817
4	DC2	05/01/2022 09:57:51	4330188
5	DR1	05/01/2022 09:57:51	16028552
6	EWS01	05/01/2022 09:57:51	3425718
7	EWS02	05/01/2022 09:57:51	811971
8	HST1	4/11/2022 6:44:09	19600559
9	LM1	05/01/2022 09:57:51	2594118
10	PM1	5/02/2022 14:29:26	3409732
11	RDS1	05/01/2022 09:57:51	1889126
12	SP1	4/11/2022 6:44:09	452901
13	NM1	4/11/2022 6:44:09	128770
14	SP1	4/11/2022 6:44:09	5145623

	Host	Last Event	Total Events
1	IP address 1	5/1/2022 15:32:53	191
2	IP address 2	4/20/2022 09:16:30	781068
3	IP address 3	05/03/2022 14:44:06	2
4	IP address 4	05/01/2022 15:54:53	12
5	IP address 5	05/01/2022 18:40:19	2
6	IP address 6	05/02/2022 15:33:48	19
7	IP address 7	05/01/2022 09:57:51	16744855
8	IP address 8	05/02/2022 15:33:48	71772713
9	IP address 9	04/25/2022 09:57:55	68393368
10	IP address 10	04/25/2022 09:57:55	63939832
11	IP address 11	04/25/2022 09:57:55	1
12	IP address 12	04/25/2022 09:57:55	2
13	IP address 13	5/10/2022 19:20:29	3
14	IP address 14	5/10/2022 19:20:29	5

Baker Hughes

BHCS39267 (05/2022)

nexuscontrols.com