WHITE PAPER

A Beginner’s Guide to Tripwire Log Center Industrial Deployments

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

The need for cybersecurity in corporate networks is clear and well-known—there is an almost constant stream of reports about hackers, identity theft, ransomware and data breaches. Until recently, industrial networks have been relatively immune to these concerns. This is no longer the case. Threats to critical infrastructure by state actors and ransomware attacks by criminal organizations have forced industrial network operators to educate themselves on cybersecurity techniques, strategies and tools.

This paper is intended to familiarize readers with the process of logging cyber events in an industrial network, where a cyber event is defined as anything that can affect the ability to view, monitor and control your industrial process. It assumes that the reader has minimal background in industrial networking and no experience with cybersecurity event logging.

The Industrial Network

Whether you are running an industrial network that manages a continuous process (e.g. oil, natural gas, petrochemical) with distributed control systems (DCS), or a discrete process (e.g. automobile assembly) with programmable logic controllers (PLC), your industrial network most likely uses a data historian.

The data historian in industrial network captures telemetry information about the measurements made and the actions taken by the industrial process. Each device on the industrial network contributes information about its activities, relative to the performance of the industrial process, to be added to the data historian, which effectively is information stored in a central relational database management system (RDBMS).

If there is an incident on the production line, the data historian provides a way to understand what went wrong. A control engineer can review the point values, alarm events and batch records, and reconstruct events leading up to the failure. With a clear understanding of how events unfolded, control engineers can then make changes needed to prevent a recurrence.

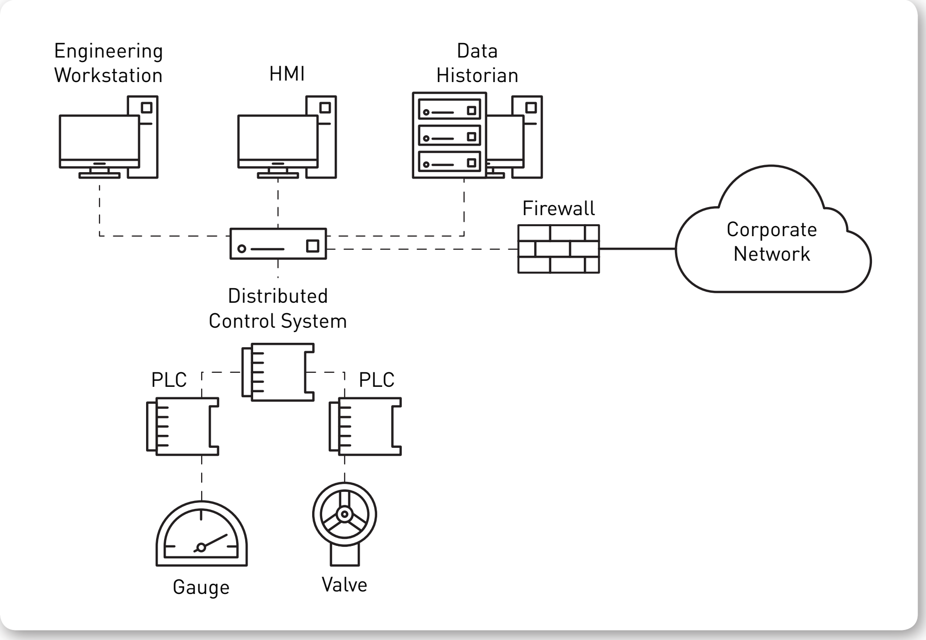


Fig. 1 A simple DCS network

Cyber Event Logging

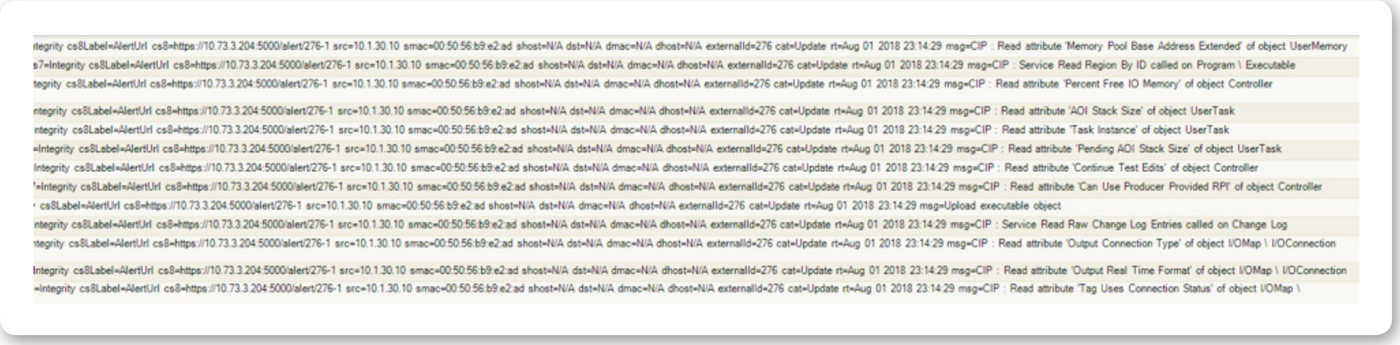
In the same way that a data historian captures and replays process events and sensor measurements, there is an equivalent function in cybersecurity with log management solutions. One such solution is Tripwire® Log Center®. Tripwire Log Center captures and stores log events that are relevant to understanding the industrial network's cybersecurity state and operations. It would not be unfair to think of the Tripwire Log Center as a "cyber historian" for the industrial network.

What are log events? Log events are nothing but information that is produced by network devices (routers, switches and firewalls), PLCs, SCADA, DCS, HMI, engineering workstations, authentication systems such as Active Directory, VPN systems, and many other kinds of systems/devices, articulating how they are operating or whether the system/devices has a fault or alarm that needs to be reviewed. An example would be a log event indicating that a power supply has failed. Depending upon the device, system or application, these log events can be sent over the network with syslog, stored in a local flat file, or stored within a database. Tripwire Log Center has the ability to harvest these logs from a variety of different devices and repositories.

What Does Tripwire Log Center Do?

A cyber historian like Tripwire Log Center performs five services for the industrial network: collection, storage, search, correlation and output.

1. **Collection**: The collection of logs is core to any cyber historian system. While this operation may appear simple at first, there are many considerations for secure and reliable log collection. Of course, missing log data can't be analyzed at all, so the ability to ensure logs get collected is primary to any cyber historian project. A cyber historian product should offer multiple means to collect logs,

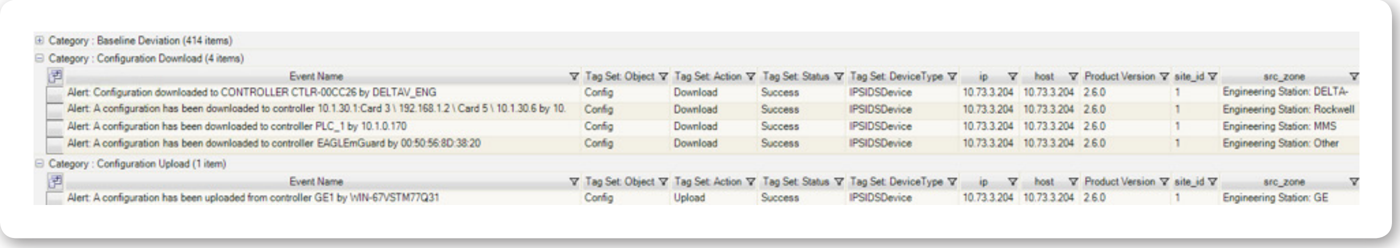


```
tegrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Read attribute 'Memory Pool Base Address Extended' of object UserMemory
s7=Integrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Service Read Region By ID called on Program \ Executable
tegrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Read attribute 'Percent Free IO Memory' of object Controller

ntegrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Read attribute 'AOI Stack Size' of object UserTask
ntegrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Read attribute 'Task Instance' of object UserTask
=Integrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Read attribute 'Pending AOI Stack Size' of object UserTask
Integrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Read attribute 'Continue Test Edits' of object Controller
'=Integrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Read attribute 'Can Use Producer Provided RPI' of object Controller
 cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=Upload executable object
ntegrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Service Read Raw Change Log Entries called on Change Log
tegrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Read attribute 'Output Connection Type' of object I/OMap \ I/OConnection

Integrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Read attribute 'Output Real Time Format' of object I/OMap \ I/OConnection
=Integrity cs8Label=AlertUrl cs8=https://10.73.3.204:5000/alert/276-1 src=10.1.30.10 smac=00:50:56:b9:e2:ad shost=N/A dst=N/A dmac=N/A dhost=N/A externalId=276 cat=Update rt=Aug 01 2018 23:14:29 msg=CIP : Read attribute 'Tag Uses Connection Status' of object I/OMap \
```

Fig. 2a Raw data from an ICS network is not easy to read or interpret reliably.



⊞ Category : Baseline Deviation (414 items)

⊟ Category : Configuration Download (4 items)

Event Name	Tag Set: Object	Tag Set: Action	Tag Set: Status	Tag Set: DeviceType	ip	host	Product Version	site_id	src_zone
Alert: Configuration downloaded to CONTROLLER CTLR-00CC26 by DELTAV_ENG	Config	Download	Success	IPSIDSDevice	10.73.3.204	10.73.3.204	2.6.0	1	Engineering Station: DELTA-
Alert: A configuration has been downloaded to controller 10.1.30.1:Card 3 \ 192.168.1.2 \ Card 5 \ 10.1.30.6 by 10.	Config	Download	Success	IPSIDSDevice	10.73.3.204	10.73.3.204	2.6.0	1	Engineering Station: Rockwell
Alert: A configuration has been downloaded to controller PLC_1 by 10.1.0.170	Config	Download	Success	IPSIDSDevice	10.73.3.204	10.73.3.204	2.6.0	1	Engineering Station: MMS
Alert: A configuration has been downloaded to controller EAGLEmGuard by 00:50:56:8D:38:20	Config	Download	Success	IPSIDSDevice	10.73.3.204	10.73.3.204	2.6.0	1	Engineering Station: Other

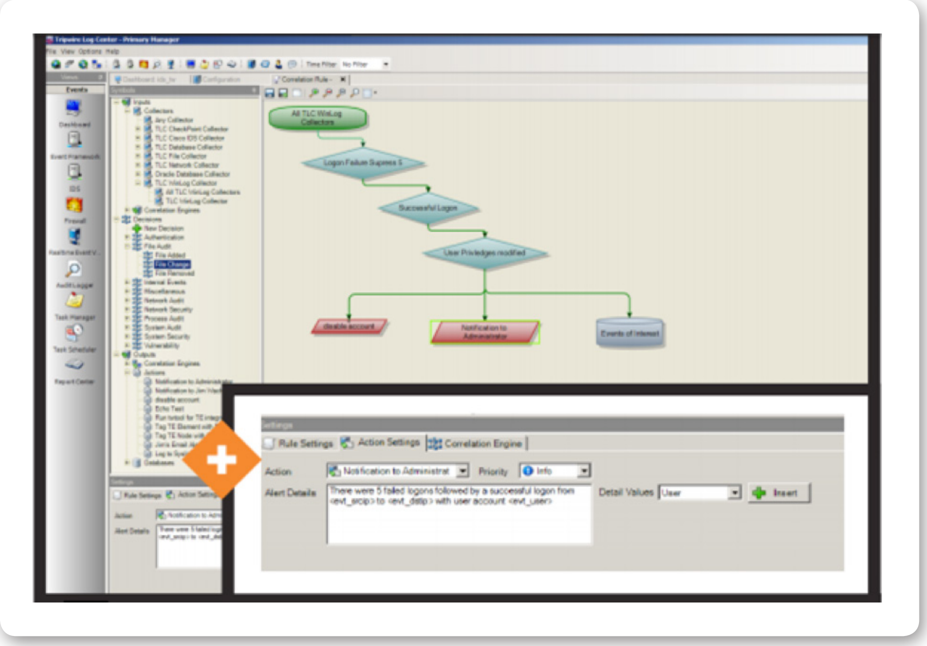
⊟ Category : Configuration Upload (1 item)

Event Name	Tag Set: Object	Tag Set: Action	Tag Set: Status	Tag Set: DeviceType	ip	host	Product Version	site_id	src_zone
Alert: A configuration has been uploaded from controller GE1 by WIN-67VSTM77Q31	Config	Upload	Success	IPSIDSDevice	10.73.3.204	10.73.3.204	2.6.0	1	Engineering Station: GE

Fig. 2b Normalized data is much easier to understand and interpret.

but should also recommend the most reliable method.

2. **Storage**: Collected logs need to go somewhere, and the volume of log data makes storage a significant issue for any deployment. Log storage needs to address at a minimum the requirements for preservation and compression of log data. More advanced features add flexibility around where the data is stored geographically, generally for compliance requirements and scalability. While storing log data, it is also necessary to "normalize" it. That is to say that manufacturers of different devices (such as PLCs, Windows workstations, and network switches) all will have the same information in their logs, but in different formats. Normalization is performed on the incoming logs to organize it into a single format, which simplifies viewing for operators when the data is recalled later.
3. **Search**: Collected data is meant to be used, and log searching is an activity that applies whenever it is valuable to reconstruct events and/or to search for an intrusion. In order for log search to be effective, it needs to provide the right balance of flexibility and performance; users should be able to directly affect the search by providing better filtering using classification tags. While it's preferred to search indexed, normalized log data, the ability to review raw logs is a key requirement as well. Log searching needs to facilitate directed queries, as well as broad queries that allow a control engineer to narrow down the results. For comparison purposes, it's also important that users be able to view the results of multiple queries at the same time.
4. **Correlation**: Cybersecurity events rarely occur in a single log entry from a single device. Much of what a cybersecurity specialist does is connect the dots between related events. While not all of this manual effort can be automated, a correlation capability in a cyber historian tool should alleviate the burden in most cases. Correlation capability provides users the ability to customize the events generated in their unique environments. While many events can be pre-populated with vendor-supplied rules, the most powerful correlation capabilities come from patterns of events that are specific to an individual organization or department. Tripwire Log Center provides an intuitive interface for creating new correlation rules in addition to its library of pre-built correlations. Finally, cyber event logs don't provide all of the data required to understand the impact to the industrial process. A cyber historian like Tripwire Log Center should support importing additional data sources to facilitate more complete correlated events. Examples include vulnerability information and asset context from other cybersecurity and asset management systems.
5. **Output**: Finally, the ability to get data out of the system, whether from log searching or correlated events, is a core requirement for any cyber historian system. While vendors may want to see their system as the ultimate destination for data, that's rarely the case. Whether that next stop is a human or another system, it's vital that the cyber historian tool facilitate the exchange of data. Customers should consider how search results are exported, whether they can be scheduled, how correlated events are delivered, and what options there are for destinations. The ability forward logs is a key requirement as well.



Action: Notification to Administrat
Priority: Info
Alert Details: There were 5 failed logons followed by a successful logon from <evt_srcip> to <evt_dstip> with user account <evt_user>
Detail Values: User

Fig. 3 Tripwire Log Center screenshot showing the creation of a correlation rule that correlates five failed logins to a successful login and to modified user privileges.

More investments are going into complex analytics on top of log and other data. A cyber historian system should focus on the core requirements of collection and correlation, but preserve the ability to deliver the log data to other systems—either in its entirety or filtered to specific events.

Using Syslog Data for Logging

There are several ways to get data into a data historian such as Tripwire Log Center; this paper will use syslog is as an example as it's the most universally-supported method.

Syslog was originally developed in the 1980s by Eric Allman. For a number of years, it existed as a de facto standard that was widely used but not recognized by any formal organization. Eventually, it was standardized by the Internet Engineering Task Force as (RFC 3164). Because of its usefulness and open design, it is incorporated into most devices.

For any device that you wish to monitor, syslog must be configured in that device with the address of the cyber data historian or syslog server. The device will then send all of its status messages to the syslog server for logging. Once the data has been received by the syslog server and recorded, it can no longer be modified. This is important in the event the original device is ever compromised

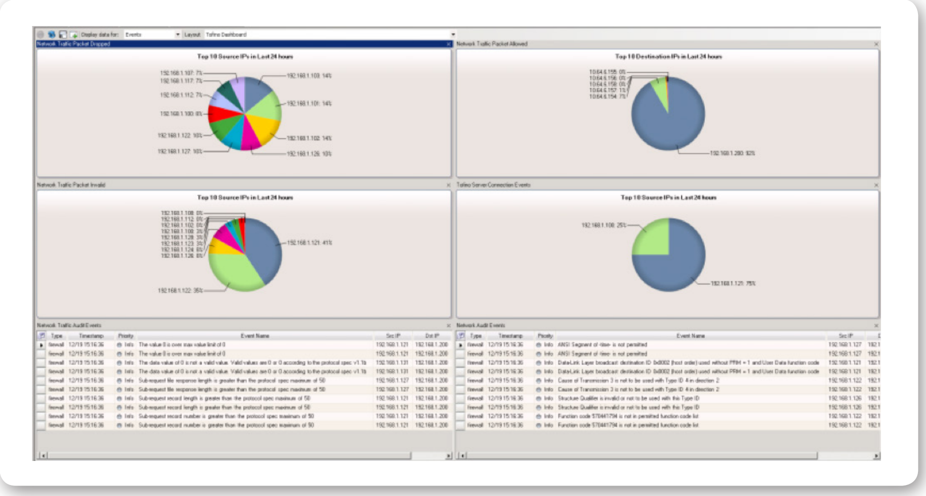

Tofino Dashboard
Network Traffic Packet Dropped
Top 10 Source IPs in Last 24 hours
Network Traffic Packet Allowed
Top 10 Destination IPs in Last 24 hours
Network Traffic Packet Invalid
Top 10 Source IPs in Last 24 hours
Tofino Server Connection Events
Top 10 Source IPs in Last 24 hours
Network Traffic Audit Events
Network Audit Events

Fig. 4 Sample ICS cybersecurity dashboard, showing what is allowed and blocked by a Tofino firewall, as well as operational events observed on the network.

Conclusion

Log management is a best practice that is referenced by many ICS cybersecurity frameworks and regulations (including but not limited to IEC62443, NERC CIP, NIST SP 800-82, and American Water Works Association Process Control Network Security Guidance). Even if you have not selected a cybersecurity framework to adopt or follow, you can still set up a centralized log repository and begin harvesting/analyzing log events. This can prove valuable for discovering if there are any cyber events impacting—or with the potential to impact—the industrial process.

Get started today. For more information regarding Tripwire Log Center visit tripwire.com/products/tripwire-log-center/

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc