

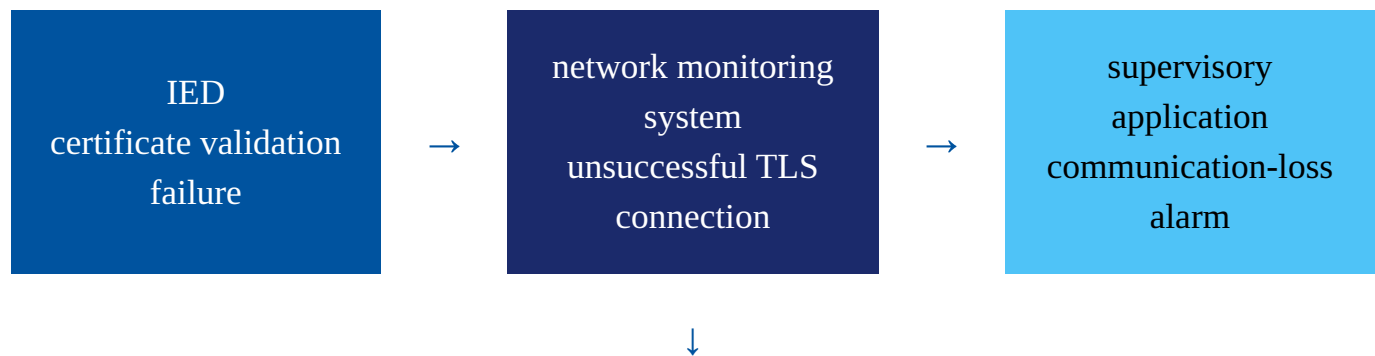
From Security Events to Trustworthy Evidence: What OT Cybersecurity Monitoring Must Preserve

Cybersecurity Awareness Month | Technical Perspectives on Power System Cybersecurity

Author: Kiran TS

Designation: Lead Research Engineer

Organization: PGCoE



But are they describing the same event?

Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

When Three Systems Report the Same Incident, Are They Telling the Same Story?

Consider a digital substation where a supervisory system fails to establish secure communication with an intelligent electronic device (IED).

The IED records a certificate validation failure. A network monitoring system reports an unsuccessful TLS connection, while the supervisory application generates a communication-loss alarm.

Three systems have reported information associated with the same incident.

But are they describing the same event?

More importantly, when these records are collected, standardized and correlated, **how can we ensure that their original meaning has been preserved?**

This is an important challenge in operational technology (OT) cybersecurity. Security monitoring increasingly depends on collecting information from heterogeneous devices, communication protocols and software applications.

However, collecting more security events does not necessarily provide a more accurate understanding of what happened.

The Challenge Is Not Just Collecting Logs

Power automation systems contain IEDs, engineering workstations, supervisory applications, communication gateways and network infrastructure.

Each component may produce security events using different formats, terminology, severity classifications and timestamps.

For example, an IED may report an authentication rejection, while a network sensor identifies a failed communication session.

Although these observations may be related, they do not necessarily establish the same cause.

A failed TLS connection could result from certificate validation, incompatible security configurations or other connection-establishment problems.

If monitoring platforms treat these observations as equivalent, important diagnostic information may be lost.

IEC 62351-14, being developed for cybersecurity event logging in power systems, addresses the need for more consistent security-event information [1].

Does Event Normalization Preserve Meaning?

Security monitoring platforms often transform device-specific records into standardized event representations.

The Open Cybersecurity Schema Framework (OCSF) provides common categories, event classes and attributes for representing security events across heterogeneous systems [2].

Such approaches can simplify event processing and support analysis across different products.

However, normalization introduces an important engineering responsibility.

Consider an IED event reporting a certificate validation failure and a network sensor reporting a failed TLS handshake.

Both records might be assigned a generic communication-failure category.

Although this may simplify searching, it could conceal the difference between a device-confirmed certificate rejection and a network-observed connection failure.

A reliable normalization process should therefore preserve the original event, its source, relevant attributes and the transformation used to produce the normalized record.

A standardized event should be easier to understand, but it should not claim more than the original observation establishes

When Did the Event Actually Occur?

Another challenge is correlating events generated by different systems.

An IED may timestamp an event using its internal clock. A network sensor may timestamp packets using its acquisition host, while a monitoring application may record when it received the event.

These timestamps may represent different moments, but the common time server can solve this issue.

OpenTelemetry's logging data model distinguishes between the time associated with an event and the time at which the event was observed [3].

This distinction is particularly relevant when reconstructing events in time-sensitive power automation systems.

Even when devices use time-synchronization mechanisms, the presence of synchronization traffic does not independently establish the accuracy of their timestamps.

Without understanding the time sources and acquisition delays, monitoring systems may correlate unrelated events or infer an incorrect sequence.

Events occurring close together in time are not necessarily causally related.



Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

Secure Event Transport Is Not the Same as Trustworthy Evidence

Security events may be transmitted through protected logging channels.

For example, RFC 5425 describes TLS-based transport for Syslog messages, helping protect communication between participating systems [4].

However, securing the transport does not establish that the originating device reported the event correctly.

A securely transmitted log may still contain an inaccurate timestamp, incomplete information or an incorrectly classified event.

Similarly, ISO/IEC 27037 provides guidance for identifying, collecting, acquiring and preserving potential digital evidence [5].

These principles are important for maintaining the integrity and traceability of original records.

Yet correctly preserving an event does not automatically establish the accuracy of its contents.

For cybersecurity monitoring, this creates three distinct responsibilities:

Preserve the original observation.

Preserve its meaning.

Preserve its traceability.

Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

Preserve the original observation. Ensure that the source record remains available and its integrity can be examined.

Preserve its meaning. Ensure that parsing, normalization and correlation do not alter what the source actually reported.

Preserve its traceability. Maintain the relationship between the original record and the information subsequently used for analysis.

These are complementary requirements, not interchangeable properties.

What Should Trustworthy OT Monitoring Provide?

A meaningful cybersecurity monitoring system should enable engineers to trace an interpreted security event back to its original observation.

For example, when a monitoring platform reports a certificate-related communication failure, engineers should be able to determine which device reported the event, what was actually observed, when it was recorded and how the conclusion was reached.

This does not require every device to generate identical logs.

Rather, it requires the monitoring architecture to preserve relevant context while enabling information from different sources to be analyzed together.

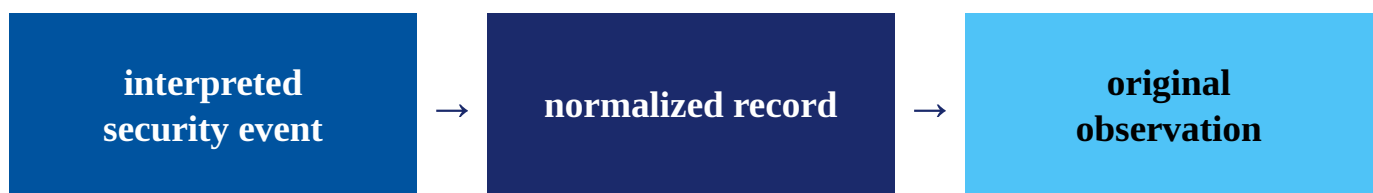
For power utilities, this capability can improve incident investigation, security-related fault diagnosis and operational decision-making.

For researchers, it can support more defensible experimental evidence and reproducible analysis.

The important shift is from treating security monitoring as a process of collecting and correlating alerts toward treating it as a process of maintaining traceable observations.

The Key Takeaway

Modern power automation systems generate security information across multiple devices, networks and applications.



which device reported the event · what was actually observed · when it was recorded · how the conclusion was reached

Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

Standards and frameworks such as IEC 62351-14, OCSF, OpenTelemetry and ISO/IEC 27037 provide complementary approaches to event representation, telemetry processing and evidence handling.

However, the reliability of security monitoring ultimately depends on whether the original meaning and context of collected observations are preserved.

A security event becomes useful evidence not simply because it has been collected, standardized or securely transmitted, but because its origin, meaning and interpretation can be examined and justified.

As utilities increasingly depend on centralized OT cybersecurity monitoring, this raises an important question:

Are our monitoring systems helping us understand what actually happened, or are they simply making it easier to collect and correlate what different devices reported?

References

- [1] IEC TC 57, *IEC 62351-14 Cyber Security Event Logging*, IEC 62351 series, developing specification. Final publication status and edition to be confirmed before release.
- [2] Open Cybersecurity Schema Framework Community, *OCSF Schema and Documentation*. <https://github.com/ocsf/ocsf-schema>
- [3] OpenTelemetry Project, *OpenTelemetry Specification , Logs Data Model*. <https://opentelemetry.io/docs/specs/otel/logs/data-model/>
- [4] F. Miao, Y. Ma, and J. Salowey, *Transport Layer Security (TLS) Transport Mapping for Syslog*, RFC 5425, March 2009. Updated by RFC 9662 (2024). <https://www.rfc-editor.org/rfc/rfc5425>
<https://www.rfc-editor.org/rfc/rfc9662>
- [5] ISO/IEC 27037:2012, *Information Technology ,Security Techniques, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. International Organization for Standardization. <https://www.iso.org/standard/44381.html>

Acknowledgment

The author acknowledges the contributions of colleagues and research collaborators involved in operational technology cybersecurity, power automation security monitoring, communication analysis and digital-evidence management. The technical discussions and engineering experience associated with security-event collection, heterogeneous data processing and event correlation have informed the perspectives presented in this article. The author also acknowledges the IEC, ISO/IEC, IETF, OCSF and OpenTelemetry communities whose standards and technical specifications provide a foundation for this discussion.

About the Author

Kiran TS is a Lead Research Engineer at PGCOE, working in operational technology cybersecurity and power system automation. His technical interests include IEC 61850 communication security, IEC 62351 implementation, cybersecurity monitoring, security-event normalization, digital-evidence management and security assessment of critical power infrastructure.