Threat Hunt Guide for BESS Environments

[INL/RPT-25-89299]

Center for Securing Digital Energy Technology (CSDET)

DECEMBER 2025

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

ABSTRACT

The rapid digitalization of the electric grid - driven by the integration of inverter-based resources (IBRs), battery energy storage systems (BESS), and advanced grid control platforms - has significantly enhanced grid efficiency, visibility, and flexibility. However, this evolution also introduces new cybersecurity risks, particularly through supply chain dependencies and operational blind spots at the grid edge.

To address these challenges, Idaho National Laboratory (INL), through the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Rapid Risk initiative, conducted a series of rapid risk assessment engagements with energy organizations across the United States.

Drawing on lessons learned from these engagements, INL developed the following threat hunting guide for asset owners and operators (AOOs) to enhance their cybersecurity visibility within BESS and IBR systems. The guide demonstrates how to use passive network monitoring to baseline device behavior, detect adversarial activity, and investigate anomalies without disrupting operations. By implementing these practices, energy sector stakeholders can improve coordination between cybersecurity and operations teams and strengthen the resilience of distributed energy resources (DERs) within the modern power grid.

Prior to implementing any network monitoring, packet capture, or threat hunting activity described in this guide, AOOs are strongly advised to review applicable governance frameworks, legal requirements, and organizational policies. **This guide is intended for informational and educational purposes only.** It does not replace compliance with any federal, state, or local cybersecurity mandates or industry standards. Implementation of described configurations, technologies, or analytic workflows is performed at the discretion and responsibility of the asset owner and operator.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

ACRONYMS

AOO	Asset Owner and Operators
BESS	Battery Energy Storage System
BMS	Battery Management System
CPU	Central Processing Unit
CSDET	Center for Securing Digital Energy Technology
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol Version 3
DOE	U.S. Department of Energy
GDO	Grid Deployment Office
HMI	Human-Machine Interface
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IBR	Inverter-Based Resource
ICS	Industrial Control System
IDS	Intrusion Detection System
INL	Idaho National Laboratory
IOA	Indicator of Attack
IPsec	Internet Protocol Security
IT	Information Technology
NTP	Network Time Protocol
OT	Operational Technology
PCAP	Packet Capture
PCS	Power Conversion System
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
TADA	Technical Assistance for Digital Assurance
TLS	Transport Layer Security
VLAN	Virtual Local Area Network

Page intentionally left blank

Threat Hunting Guide for BESS Environments

1. INTRODUCTION

The accelerating deployment of digital energy infrastructure, ranging from inverter-based resources (IBRs) and battery energy storage systems (BESS) to advanced grid control platforms, has brought unprecedented visibility, flexibility, and efficiency to the electric grid. However, this digital transformation also introduces new challenges, particularly in the form of supply chain risks and operational blind spots at the edge of the network.

Over the past year, Idaho National Laboratory (INL), through its rapid risk assessments sponsored by the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), INL has conducted a series of on-site network observation engagements. These engagements, conducted in partnership with organizations across the U.S., have focused on identifying vulnerabilities and misconfigurations in operational technology (OT) environments. On-site network hunts and edge monitoring have proven to be essential in uncovering latent risks introduced through supply chain vulnerabilities and configuration weaknesses. These risks often stem from third-party components, firmware inconsistencies, or insecure default configurations that persist in the field long after commissioning. Based on the lessons learned from these engagements INL has compiled a guide for asset owners and operators (AOOs) to conduct their own threat hunting within BESS/IBR environments. This guide shows AOO how they can leverage passive network monitoring to:

- **Baseline** normal BESS/IBR communications and device behavior;
- **Hunt** proactively for evidence of adversary techniques;
- **Detect** anomalous or unsafe commands and credential misuse;
- **Investigate** with full fidelity packet and log correlation without disrupting operations.

Through publishing this guide, we aim to help AOOs maintain consistent visibility across OT field sites to strengthen the safety, reliability, and resilience of the broader power grid.

1.1. Network Intrusion Detection in BESS and IBR Environments

Network Intrusion Detection Systems (IDS) can provide continuous, passive visibility into communications occurring across OT system networks. Unlike host-based security tools, an IDS does not interfere with real-time operations or modify any control logic. It simply observes mirrored network traffic and analyzes it to identify anomalous behaviors. For AOOs, this capability enables early warning of unsafe or unexpected behaviors before it becomes an operational outage or safety event.

An IDS enables passive, protocol-aware observation of control traffic between components such as battery management systems (BMS), power conversion systems (PCS) and inverter controllers, human machine interfaces (HMI), remote terminal units (RTU), and site gateways, along with other devices that are often on the same networks or subnets, such as meters or relays. Because the tooling reads copies of traffic rather than interacting with endpoints, it avoids process disruption while providing early warning of unsafe or unexpected commands, unusual authentication patterns, configuration drift, and exfiltration paths. The intent is to move from reactive alert processing, where IDS tools generate notifications based on predefined rules, to proactive hunting that tests hypotheses, uncovers unseen activity, and hardens the environment through evidence-based detections. The primary goal of BESS/IBR threat hunting is to:

- Establish comprehensive baselines of normal network behavior, system processes, and user activity specific to BESS/IBR components (e.g., BMS, inverter control units, supervisory control and data acquisition (SCADA) systems). This is necessary for identifying deviations.
- Understand the unique operational characteristics, protocols (e.g., Modbus, DNP3) and critical assets that can be observed within BESS/IBR environments.

- Employ statistical methods (e.g., standard deviation, frequency analysis, outliers) to identify anomalies that may not trigger signature-based alerts.
- Continuously integrate open-source cyber threat intelligence (OSINT), including Indicators of Attacks (IOAs), Tactics, Techniques, and Procedures (TTPs), and known attack patterns relevant to industrial control system (ICS)/OT environments.
- Map observed behaviors and potential threats to the MITRE ATT&CK for ICS framework to categorize and understand adversary techniques specific to BESS/IBR operations.
- Shift from a purely reactive alert-driven approach to a proactive hunting methodology.

1.2. About Malcolm

An IDS detects and reports suspicious activity, whereas a Security Information and Event Management (SIEM) collects and analyzes those alerts alongside logs from across the network to reveal larger attack patterns. Throughout this guide, Malcolm is frequently mentioned for illustrative purposes, however, **AOOs should use whichever SIEM platform best suits their needs**.

Malcolm[1] is a SIEM platform that is primarily used for aggregating and analyzing operational technology (OT) network traffic, though it can also be used for information technology (IT) network traffic. It is comprised of a collection of open-source tools which can capture network traffic, process it with Zeek[2] and store the resulting logs and alerts in OpenSearch[3]. The platform contains a suite of pre-built dashboards to serve as starting points for analyzing different protocols and security events of interest. These dashboards highlight specific events and trends that may be of interest from an OT security perspective - for example, this could include failed authentication attempts to HMIs, Modbus write operations to programmable logic controllers (PLCs), and external connections to/from field devices.

Together, these components provide a streamlined system for data collection, processing, and centralized storage to facilitate analysis of large datasets. This enables automated searching for known indicators of attack (IOAs), complex event correlation, and statistical analysis of OT network traffic for behavioral anomaly detection and threat hunting.

While there are a variety of ways to architect a Malcolm deployment, for the purpose of this document, we describe the use of a Malcolm deployment in which network sensors at BESS or IBR sites can parse and forward encrypted telemetry to a central Malcolm instance, where it is indexed and presented for analysis.

1.2.1. Intrusion Detection System Requirements

An effective IDS or network hunting platform must support the complete data lifecycle from raw packet capture through analysis and visualization. Each capability contributes to the accuracy and value of detections and hunts:

- **Packet capture:** The foundation of any IDS is the ability to capture and retain network packets for inspection. Without raw packet data, analysts cannot validate detections or reconstruct events.
- **Packet storage and retrieval:** Captured packets must be stored efficiently and indexed for rapid retrieval, supporting both real-time analysis and retrospective investigation.
- **Packet parsing and enrichment:** Raw network data must be parsed into structured metadata that identifies protocols, conversations, and field-level details to support behavioral analysis.

---

[1] Malcolm. *Malcolm: A powerful, easily deployable network traffic analysis tool suite for network security monitoring*. Accessed December 3, 2025. https://malcolm.fyi/

[2] Zeek. *Zeek: An Open Source Network Security Monitor.* Accessed December 3, 2025. https://zeek.org/

[3] OpenSearch. *OpenSearch: Home page.* OpenSearch.org. Accessed December 3, 2025. https://opensearch.org/

- **Signature-based detection:** IDS tools use known malicious patterns or signatures to identify recognizable threats.
- **Asset identification and inventory:** Visibility into which devices are communicating provides context and helps prioritize alerts and potential risks.
- **User interface and analytical workflow:** Analysts need flexible visualization, search, and dashboard capabilities to explore data, test hypotheses, and correlate detections efficiently.

1.2.2. How Malcolm Meets These Requirements

The following tools, while not an exhaustive list, are core elements of the Malcolm toolstack[4] and are noted here to help readers better understand this hunt guide.

- **Arkime:** Arkime[5] indexes and stores full packet captures (PCAPs) for analysis. Arkime supplements Zeek and Suricata by allowing analysts to review captured packets from a given timeframe. This capability validates whether a detected command was legitimate or malicious. Timing analysis within Arkime can also identify low-and-slow exfiltration or automated command bursts. Analysts can extract the exact packets corresponding to a suspicious event, allowing reconstruction of communications to confirm the precise sequence and content of control messages.
- **Zeek:** Zeek[6] functions as the behavioral engine of the system. It translates network activity into rich logs that describe conversations, protocol details, and behavioral indicators. Zeek detects abnormal traffic frequency, unexpected function codes, or unusual certificate use. Malcolm ships with a tailored set of Zeek scripts to augment its logging and detection capabilities beyond its default configuration.
- **Suricata:** Suricata[7] performs signature-based inspection of packets using established threat rules. It flags known malicious traffic or malformed frames. When combined with Zeek, Suricata allows analysts to correlate known bad patterns with unknown behavioral anomalies.
- **NetBox:** NetBox[8] provides an asset inventory system that can be populated on the observed network traffic. Assets can then be enriched with additional details, which can be overlayed onto the network logs to improve the context of the data to aid in analysis.
- **OpenSearch:** OpenSearch[9] provides the search and visualization interface for analysts. It enables real-time queries across Zeek, Suricata, and host logs and supports dashboard creation for protocol analysis, user behavior monitoring, and anomaly detection. Analysts can create specialized queries and dashboards to focus on specific BESS/IBR threats or anomalies. For example:
    - **PLC Write Commands by Source IP:** Monitor Modbus/DNP3 write operations to critical BESS/IBR PLCs.
    - **High Volume of Failed Logins to HMI:** Track authentication attempts on Human-Machine Interfaces.
    - **External Connections to Field Devices:** Visualize connections to PLCs or RTUs.

---

[4] Malcolm. *Components.* Accessed December 3, 2025. https://malcolm.fyi/docs/components.html

[5] Arkime. *Arkime: Network Analysis & Packet Capture.* Arkime website. Accessed December 3, 2025. https://arkime.com/

[6] Zeek. *Zeek: An Open Source Network Security Monitor.* Accessed December 3, 2025. https://zeek.org/

[7] Suricata. *Home page.* Suricata. Accessed December 3, 2025. https://suricata.io/

[8] NetBox. *Home page.* NetBox Labs. Accessed December 3, 2025. https://netboxlabs.com/

[9] OpenSearch. *Home page.* Last modified 2025. https://opensearch.org/

- **Segment-Specific Dashboards:** Create dashboards tailored to different BESS/IBR network segments (e.g., IT-OT DMZ, Process Control Network) to focus on relevant traffic patterns and typical behaviors.

- **Additional capabilities:** Malcolm also integrates automated file analysis, identity and access management features, rule-based pattern matching, and GeoIP data enrichment to strengthen situational awareness.[10] Together, these capabilities provide the foundational components required for both signature-driven IDS detection and proactive network hunting.

This toolstack provides AOOs with a framework for scalable visibility across distributed sites, with a central place to analyze data, threat hunt, and investigate potential incidents without risking process disruption.

Note: Where budget or infrastructure constraints exist, Malcolm may be deployed in a virtualized environment. For large or multi-site deployments, dedicated physical servers are recommended to ensure sustained throughput and data retention capacity. Virtual Machine configuration instructions are provided on Malcolm's Documentation page.[11]

1.3. Key BESS/IBR Components

A BESS or IBR installation typically includes a Battery Management System (BMS), a PCS or inverter controller, HMIs, SCADA systems, and one or more gateways or remote terminal units (RTUs) providing external communication (see Figure 1).

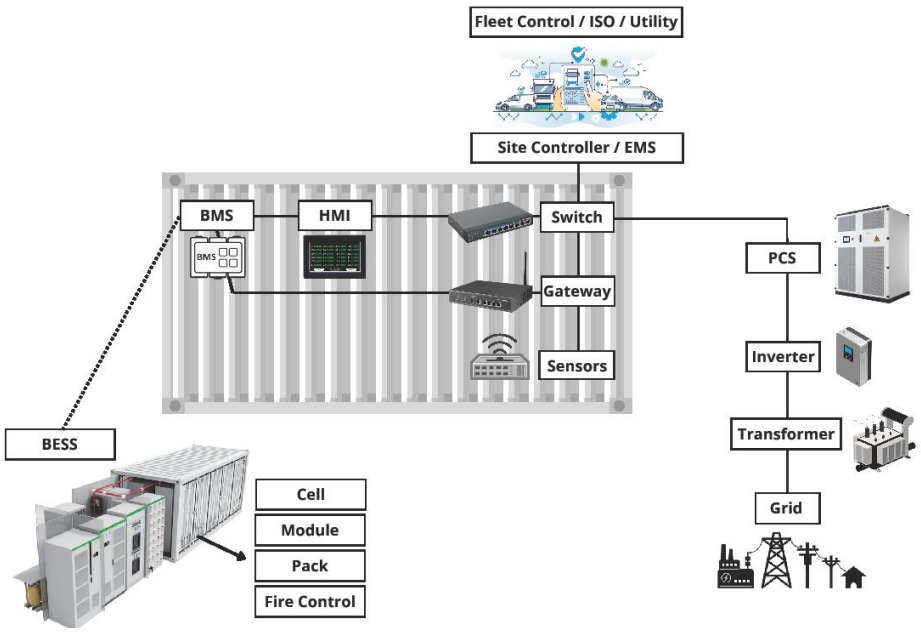

Figure 1. Key components within a BESS site.

Understanding the function and threat surface of each component is necessary for determining where and how to monitor network traffic for anomalies:

- **BMS (Battery Management System):** Protects cells by enforcing voltage, current, and temperature limits.

[10] Malcolm. *Components.* Accessed December 3, 2025. https://malcolm.fyi/docs/components.html

[11] Malcolm. *Documentation.* Malcolm official website. Accessed December 3, 2025. https://malcolm.fyi/docs/

- Risk lens: A compromised BMS could disable protective logic or induce unsafe charge states, potentially resulting in thermal events or forced shutdowns. IDS should monitor for unauthorized firmware updates, suspicious Modbus register writes, and command sequences inconsistent with expected operating states.

- **PCS/Inverter Controller:** Converts DC↔AC and manages grid-forming/following modes.
  - Risk lens: Attackers may manipulate inverter controls or setpoints to destabilize frequency or voltage, creating localized outages or equipment damage. Continuous monitoring of setpoint changes and inverter state transitions can aid in detection.
- **Human-Machine Interfaces (HMIs) and SCADA Workstations:** Human oversight and supervisory commands.
  - Risk lens: Weak authentication, credential reuse, and insecure remote administration are common weaknesses. Compromised credentials may allow for lateral movement between enterprise and control networks. Role-based access control and endpoint monitoring are key defenses.
- **Gateways/RTUs:** Protocol translation and remote telemetry.
  - Risk lens: These devices bridge proprietary field protocols and IP-based networks (e.g., Modbus RTU ↔ Modbus/TCP, DNP3). Their role and position make them targets for localized process manipulation or denial of service once inside operational networks. Continuous configuration integrity checks and access monitoring are necessary to prevent unauthorized modification or data exfiltration.
- **Web APIs:** Web Application Programming Interfaces (APIs) provide remote monitoring, control, and data exchange between site systems, cloud platforms, and vendor management services. APIs are often used for telemetry uploads, firmware updates, and integration with energy management or fleet aggregation systems.
  - **Risk lens:** Exposed APIs expand the attack surface beyond local networks. Weak authentication, hardcoded credentials, or excessive privileges may allow remote command execution or data manipulation. Malicious actors can exploit poorly secured endpoints to alter setpoints, access sensitive operational data, or push unauthorized updates. Network monitoring should include inspection of outbound API traffic, authentication logs, and deviations in normal call patterns or payload structures.

1.4. Common BESS/IBR Protocols

Understanding the components and communications within BESS and IBR systems is critical for identifying cyber entry points and monitoring abnormal network behavior. Table 1 below summarizes network protocols commonly observed in the field and some of the security considerations that AOOs should keep in mind.

Note: The 2024 DOE CESER BESS report, developed by Idaho National Laboratory (INL), provides additional insight into the cyber and supply chain risks associated with specific BESS components and architectures,[12] including PCS, BMS, and site control/EMS networks. The report highlights that as these

[12] U.S. Department of Energy. *Battery Energy Storage Systems Report.* Prepared by Idaho National Laboratory. November 1, 2024. https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf

systems become more digitally interconnected, the communications interfaces and control logic represent growing vectors for compromise.

Table 1. Common BESS/IBR network protocols and security considerations.

Protocol	Use	Common Ports	Security Considerations
Modbus/TCP	Device-to-controller communication (BMS → EMS, PCS → SCADA)	TCP/502	No authentication or encryption
Modbus RTU (RS-485)	Serial comms within racks/ battery packs	N/A	Physical access risk; often bridged to TCP/IP via converters
CAN / CANopen	Battery cell and pack-level communication	N/A	No security controls; vulnerable to spoofing/injection
DNP3 / DNP3 over TCP	Utility or grid communication	TCP/20000	Legacy plaintext protocol; supports unsolicited responses; exploitable for spoofing
IEC 61850 / MMS	Substation-level control; grid interface	TCP/102	Complex, often poorly segmented; needs whitelisting and certificate management
OPC-UA	Industrial interoperability; EMS/SCADA integration	TCP/4840	Better security options (certificates), but often misconfigured
MQTT	Cloud telemetry / vendor monitoring	TCP/1883, 8883	Weak authentication; potential exfiltration path
HTTP / HTTPS / SSH	Web management / vendor access	TCP/80, 443, 22	Web exploits, default credentials, and lateral movement vectors

2. PREPARING FOR A THREAT HUNT

2.1. Disclaimer

Prior to implementing any network monitoring, packet capture, or threat hunting activity described in this guide, AOOs are strongly advised to review applicable governance frameworks, legal requirements, and organizational policies. **This guide is intended for informational and educational purposes only.** It does not replace compliance with any federal, state, or local cybersecurity mandates or industry standards. Implementation of described configurations, technologies, or analytic workflows is performed at the discretion and responsibility of the AOO.

2.2. Planning and Preparation

Effective endpoint and network-based collection begins with a clear understanding of the operational environment. Involving their IT and OT system administrators can help AOOs gain insight into the system architecture and the current state of security monitoring, enabling the design of a unified strategy for endpoint and network monitoring that supports threat hunting across multiple data sources. The following sections cover issues AOOs should consider during the planning and preparation stage before a hunt. The following considerations are merely starting points; solicit further input from system administrators and operators.

2.2.1. System Architecture Documentation

Begin by gathering documentation of your system architecture. Involve both IT and OT personnel in discussions – OT engineers know which devices communicate for normal operations, while IT staff can advise on network architecture, bandwidth constraints, existing security controls, etc. Together,

determine **where** you should monitor network traffic, collect logs, and how to forward them to the SIEM. For example, some key architectural documents to gather include:

- Site layouts identifying physical locations for sensor placement
- Maintenance windows and change control schedules
- Network diagrams showing IT/OT boundaries, VLANs, and segmentation
- Asset inventories listing control systems, workstations, and field devices
- Data flow diagrams showing normal communication patterns between zones
- Existing security controls (firewalls, IDS/IPS, endpoint protection)

2.2.2. Endpoint Visibility

Endpoint/host-level visibility is critical for detecting adversary behaviors that occur within the context of a single workstation or server, without generating network traffic. In OT environments, threats often start on remotely accessible endpoints before moving to lower-level, control system-facing systems. Endpoint visibility can help detect:

- **Living off the land** using tools and scripts native to a given system
- **On-target reconnaissance** of a workstation/serve where a threat actor already has access
- **Credential theft** targeting privileged engineering accounts
- **Privilege escalation** to expand access and permissions
- **Configuration changes** performed on target

Without endpoint logging, adversaries can operate undetected on workstations that can directly control industrial processes. Table 2 highlights key OT endpoints to monitor, along with the common risk factors.

Note on Field Devices: PLCs, RTUs, IEDs, and safety systems often have limited or no endpoint logging capabilities; some telemetry may be possible via syslog, but security relevance will vary. Monitor these devices through network traffic analysis and protocol-specific monitoring rather than endpoint logs. Engineering workstations that program these devices are the primary visibility point for detecting unauthorized field device modifications.

Table 2. Critical OT endpoints for monitoring.

Endpoint Type	Purpose/Function	Potential Risk Factors
Domain Controllers	• Managing Active Directory and all other functions of the domain	• Credential theft • Full domain compromise
Engineering Workstations	• Program PLCs • Configure SCADA • Maintain industrial networks	• High-privilege access • May transit between multiple networks • Potential USB malware entry point
Field Devices (PLCs, RTUs, IEDs, Safety Systems)	• Execute control logic • Control physical processes • Communicate with sensors/actuators	• No endpoint logging capabilities • Rarely patched • Direct process impact
Human-Machine Interfaces (HMIs)	• Direct control of industrial processes	• Outdated operating system (OS), limited security tool support • Unauthorized access risk

Historian & Data Servers	• Store operational data and process information	• Dual network connections (IT/OT) • Ransomware targets • Data theft exposure
Jump Server / Remote Access Gateways	• Vendor and administrator access points	• External access vectors • Privileged credential use

2.2.3. Network Visibility and Sensor Placement

When determining where to capture network traffic, AOOs should evaluate both technical feasibility and operational value at each potential site. Considerations AOOs may consider when identifying where to capture network traffic include:

2.2.3.1. Distribution

- **Diversify vantage points:** Select monitoring points that provide visibility into different network zones or operational functions (e.g., control center, OT DMZ, field substation, or remote generation site).
- **Represent network variety:** Ensure at least one capture point covers north-south traffic (IT↔OT boundary) and another captures east-west traffic within the OT zone (e.g., between HMIs and PLCs).
- **Ensure full coverage:** Avoid monitoring only the paths that represent normal or expected operations. Attackers often exploit overlooked or rarely used network segments, alternative egress points, or vendor maintenance channels. When defining sensor locations, include coverage for both routine traffic and potential out-of-band communication routes to ensure anomalous activity can still be observed. This aligns with north-south and east-west visibility goals — providing both boundary and internal monitoring necessary for effective hunts.
- **Balance reach and maintainability:** Begin with a limited number of capture sites at different levels (e.g., OT DMZ, control center, and nearby BESS substation) to gauge data volume and security value. This provides a sampling of visibility without overextending resources. Optimizing the data collection configuration will require iterating between capture and analysis to refine what is captured/logged, how it's parsed, forwarded, indexed, etc.
- **Support scalability:** Choose sites that could later serve as aggregation points if monitoring is expanded.

2.2.3.2. Interface & Hardware Requirements

- **Connectivity and compatibility:** Identify network media (fiber, copper, serial, etc.) and ensure compatible transceivers or converters are available.
- **Tapping feasibility:** For fiber interfaces, assess whether optical taps can be installed without service disruption. If not, coordinate a safe maintenance window.
- **Network design considerations:** Confirm that SPAN or mirror ports are available if passive optical taps aren't practical.
- **Physical requirements:** Validate available rack space, power, and cooling for at least:
    - A "shoebox-sized" network sensor.
    - A small router or aggregation switch (optional).
    - A TAP or SPAN aggregation device (if used).
- **Bandwidth and packet load:** Estimate expected network throughput to ensure the capture device can process and store full packets without dropping data.

2.2.3.3. Environmental & Operational Constraints

- **Permissions and notifications:** Determine what permissions are required and who needs to be notified before installation or data collection, especially at sites with third-party monitoring, maintenance, or operational involvement. Coordinating with all stakeholders helps avoid unintentional disruptions and ensures compliance with contractual and safety obligations.
- **Site conditions**: Field sites often lack temperature-controlled environments; consider ruggedized or industrial-grade equipment for substations or outdoor enclosures.
- **Power and connectivity:** Verify stable power and network backhaul; in remote areas, plan for store-and-forward data collection or periodic retrieval.
- **Operational coordination:** Work with site operations and maintenance teams to schedule installation and minimize downtime.
- **Safety and compliance**: Ensure installation does not interfere with safety instrumented systems, certified control devices, or vendor support agreements.
- **Access control:** Confirm that maintenance and monitoring of capture devices can be performed remotely or securely onsite under proper access control procedures.

2.2.3.4. Network, Data Management, and Sensor Placement

- **Data retention:** Determine how long to store captured traffic and where (on-prem, secure cloud, or SIEM).
- **Data privacy and protection:** Apply encryption and access controls for captured traffic containing sensitive OT communications.
- **Integration:** Plan how captured data will integrate with existing OT monitoring platforms (e.g., ICS-aware IDS, historian logs, or SIEM).

Note: Additional considerations for Site Selection are included in Section 2.2.4.

To support network visibility and effective hunt operations, it is important to identify monitoring points that align with the logical and functional boundaries of the control system architecture. Figure 2 below illustrates the recommended secure network architecture from the Department of Homeland Security's (DHS) Defense in Depth report. The original figure from the DHS Defense in Depth report has been adapted with red arrows to illustrate representative locations for network sensor placement across enterprise, control, and field layers.[13] Although this model does not depict specific BESS components, it provides a reference framework for where sensors can be deployed to capture the most relevant network traffic within a typical OT environment.

[13] U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.* September 2016. https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

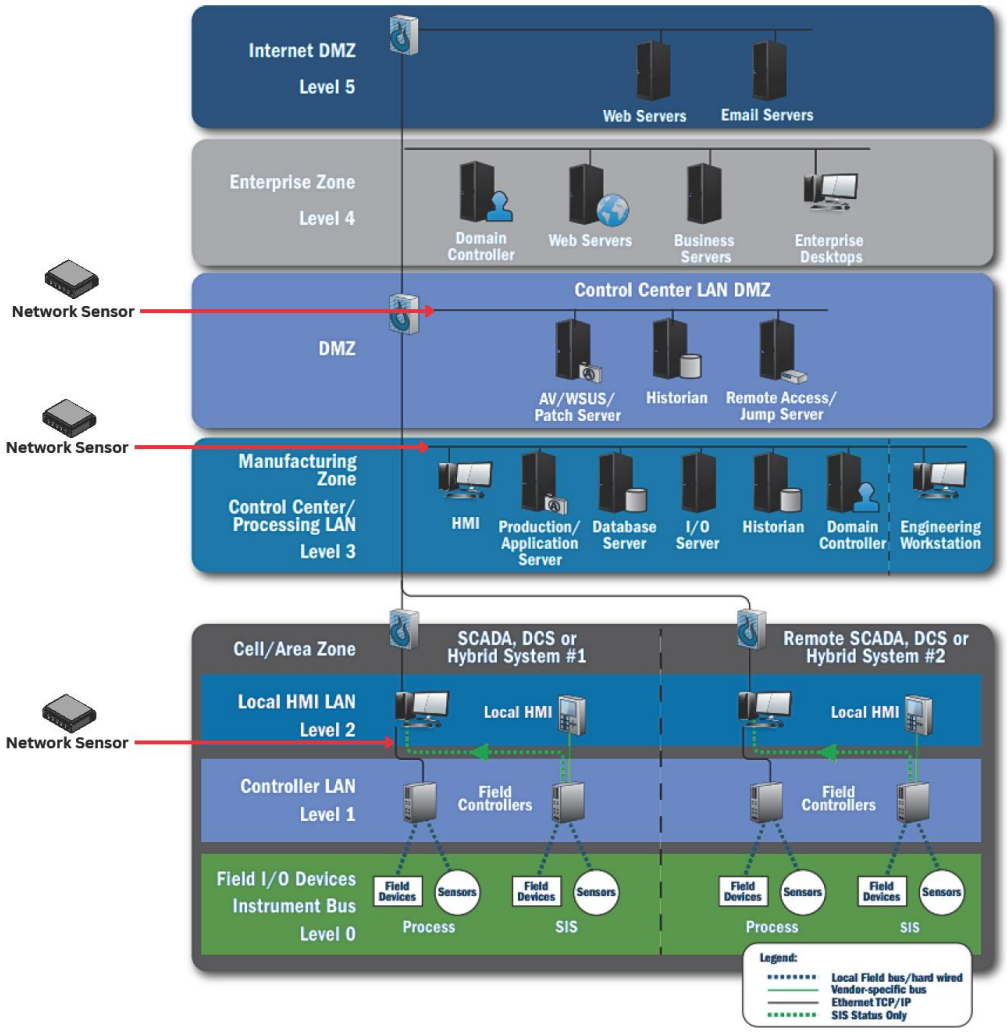

Figure 2. Purdue Model Adapted to show sensor placement locations - from Defense in Depth: Recommended Practice (NCCIC/ICS-CERT, U.S. Department of Homeland Security, 2016).[14]

In this structure, sensors are positioned at the OT DMZ (sometimes referred to as Level 3.5), Level 3 (where the fleet controller would live) and Level 2. Sensors should be monitoring the traffic – traversing the core switch at each level. AOOs should coordinate with site operations to schedule sensor installation. If a tap is required, and the expected duration of interruption is not acceptable, a planned maintenance window may be necessary.

Deployment of Malcolm sensors and a central analysis server should follow the official documentation at malcolm.fyi,[15] ensuring appropriate protocol parsers (such as Modbus and DNP3 within Zeek) are enabled.

2.2.4. Site Selection for Initial Deployment

Starting with a single site is recommended – AOOs can validate data capture and gain insights, then expand to other sites later. Choose a site that is representative of your typical OT architecture and

[14] Ibid

[15] Malcolm. *Malcolm – A powerful, easily deployable network traffic analysis tool suite for network security monitoring.* Accessed December 3, 2025. https://malcolm.fyi/

protocols, ensuring it provides an accurate reflection of your operational environment. It is recommended that AOOs begin with one representative site to validate data capture and connectivity before scaling across the fleet. A common approach in OT is to deploy sensors in three primary locations:

- **OT DMZ:** The boundary between corporate IT and the OT network (e.g. at a firewall or router connecting the control center to field sites). Monitoring here catches any external or enterprise-originating traffic to the site and vice versa.
- **Control Center Network:** If you have a central control or SCADA network separate from field sites, monitor there to see traffic among SCADA servers, historians, and operator workstations.
- **Field Site (BESS Substation):** Place a sensor at a representative BESS site within the local OT network to capture inverter and site-level communications. Note that many component-level links (e.g., BMS↔PCS, PCS↔inverter) are hardwired and may require supplemental monitoring at gateways or controller interfaces for full visibility.

When choosing which BESS/IBR site to monitor first, AOOs should consider the following factors. This list provides common considerations, but it is **not exhaustive** — additional factors may be relevant depending on your specific operational environment, organizational requirements, and site characteristics.

- **Risk Profile** - Prioritize sites with:
    - External network connectivity (cloud monitoring, vendor remote access)
    - Higher criticality to grid operations or revenue generation
    - History of configuration changes or maintenance activity
    - Dual IT/OT network connections (common entry point for threats)
- **Representative Architecture** - Choose a site that reflects your typical BESS/IBR deployment:
    - Standard BMS, PCS, and inverter controller configuration
    - Typical communication protocols (Modbus, DNP3, proprietary)
    - Common network topology and segmentation approach
- **Accessibility** - Select a site where you can:
    - Physically access equipment for sensor installation and troubleshooting
    - Coordinate with on-site personnel during deployment
    - Respond quickly if issues arise during initial setup
- **Technical Feasibility** - Verify the site has:
    - Managed switches with available SPAN ports (or electric power and rack space for a physical tap)
    - Sufficient bandwidth to handle mirrored traffic without packet loss
    - Physical space and power for sensor equipment
    - Stable network connectivity back to your central monitoring server
- **Operational Coordination** - Confirm you can:
    - Schedule installation during planned maintenance windows (if necessary)
        - If installing a physical network tap, there will be a temporary disruption to network communications; depending on the tolerance for such a disruption, it may be necessary to install the tap during a planned maintenance window.

- Coordinate with site operators to validate normal communication patterns
- Test monitoring without impacting real-time battery control or grid services

2.2.5. Generalized Equipment List for OT Network Hunt Engagements

A general equipment list for a network hunt typically consists of a central server, one or more network sensors, analyst workstations, and supporting network hardware. Table 3 below provides equipment that is likely needed for a network hunt, along with deployment considerations.

Table 3. Generalized equipment list for hunt engagements.

Equipment Needed	Description/Purpose	Deployment Considerations
Network Taps (Optional but Recommended)	Physical network taps for non-intrusive traffic capture without relying on switch SPAN ports. Fail-safe design ensures no disruption to monitored links.	• Copper or fiber taps based on media type • Aggregation taps for full-duplex links • Bypass capability for critical paths
Network Sensors	Ruggedized edge devices installed at each OT site to capture mirrored network traffic and forward metadata to the central server. One sensor per monitored location or network segment.	• Industrial-rated for harsh environments • Minimum 128 GB RAM, 48 CPU cores • Dual NICs (management + capture + management & forwarding) • Local SSD storage for packet buffering
Server (SIEM)	Central analysis platform for log ingestion, storage, and visualization (e.g., Malcolm, Splunk, etc.). Deployed in a secure data center or control facility.	• Minimum 64-128 GB RAM • 16+ CPU cores recommended • NVMe for hot data, HDD for archives • Redundant power supply recommended
Unmanaged Switch	For analyst laptops to connect to server to access data for analysis.	• Sufficient ports for analysts + connection to server • May connect to server via a
Analyst Laptop(s)	Workstations used for data review, hunting, validation, and report generation. Each analyst requires one system with sufficient memory and storage for local analysis.	• Minimum 16 GB RAM • SSD storage • Dual monitors recommended • VPN client for remote access
USB-C Dock/Adapter	Provides Ethernet connectivity between analyst laptops and switches when direct RJ45 ports are unavailable.	• Gigabit Ethernet support • Additional USB ports for peripherals • Power delivery if needed
Cabling	Cat6 or Cat6a Ethernet cables of varying lengths (1m, 3m, 10m, 25m) to interconnect sensors, switches, and laptops. Fiber patch cables for fiber-based monitoring. Provides Ethernet connectivity between analyst laptops and switches when direct RJ45 ports are unavailable.	• Clearly labeled cables • Color-coded by function (management/capture) • Appropriate length to avoid clutter

Optional: Routers for IPsec VTIs (Virtual Tunnel Interfaces)	May be used to establish encrypted tunnels between sensors & server, and server & laptops. Note: Malcolm supports certificate-based encryption between sensor(s) and server, but VTIs could be used instead, or as a second layer of encryption.	• Router capable of terminating IPsec VTIs for additional encryption between sensor and server and/or server room and analyst switch • Ample VTI throughput capacity for sensor telemetry or analyst-to-server communication, depending on where it will be used.
Optional: Uninterruptible Power Supply (UPS)	Provides short-term power protection for network sensors, switches, and critical equipment during outages. Essential for remote or unmanned sites.	• Runtime: 15-30 minutes minimum • Pure sine wave output • Network management (SNMP) for alerts • Capacity for all connected devices
Optional: Mounting / Rack Hardware	For stable and secure installation of servers, switches, sensors, and network equipment — especially at substations, control rooms, or harsh industrial environments.	• Wall-mount or rack-mount options • Cable management accessories • Locking cabinets for physical security
Optional: Temperature Control and Debris Resistance	Ruggedized enclosures, cooling fans, or climate control for field-deployed sensors in extreme temperatures, dusty environments, or outdoor installations.	• NEMA/IP-rated enclosures • Temperature range appropriate for environment • Ventilation or active cooling as needed
Optional: Out-of-Band Management	Serial console servers or KVM-over-IP devices for remote management of sensors and servers without relying on the primary network.	• Cellular or satellite backup connectivity • Separate management VLAN • Multi-factor authentication (MFA)

2.3. Establishing Your Hunting Foundation

2.3.1. Develop Hypothesis

AOOs can begin establishing their hunt foundation by starting with specific, testable questions based on known BESS/IBR risks and their understanding of normal operational behavior. Rather than searching environments randomly, hunts should be guided by foundational knowledge about the system and attack surface, which should inform data collection and hypotheses/threat hunting questions about relevant tactics, techniques and procedures (TTPs) against equipment and/or services that exist within the system. The following questions are provided as examples of foundational questions that can inform data collection as well as establish hypothesis framed towards threat hunting.

- *Foundational questions to inform data collection:*
  - *"What are my most critical systems, and where are they located within the network architecture?"*
  - *"What is the worst-case consequence that could occur at this site if a critical system were compromised?"*
  - *How can I monitor or instrument systems to observe the network paths or dependencies that would be required for that consequence to occur?"*
- *Example Hypotheses framed towards Threat Hunting:*
  - *"Are any control systems initiating outbound connections to unknown external IPs?"*

- *"Are there unauthorized Modbus write commands to BMS setpoints outside maintenance windows?"*
- *"Is vendor remote access occurring during unapproved times or from unexpected locations?"*

AOOs should begin with simple, testable hypotheses based on realistic risks (e.g., remote access abuse, update compromise, or command manipulation). Focus on where those behaviors would appear first, and whether you find something or not, work backward to either pull the thread and correlate events, and/or identify an initial piece of evidence upstream in the system or network. The goal is not to find every anomaly (though you may find some interesting ones, and should run them to ground), but to build confidence that your visibility covers the attack paths that matter most for your BESS/inverter fleet.

Malcolm Tip: Malcolm's pre-built dashboards like "Connections", "ICS/IoT Security Overview", and "Software" can reveal patterns that inform threat hypotheses specific to your BESS/IBR environment.

2.3.2. Establishing Baselines

Establishing baselines for endpoint and network data within BESS and IBR environments is essential for detecting anomalies amid high volumes of routine traffic. Without a baseline, normal operational noise can obscure indicators of compromise (IOC). By applying methods to define what constitutes "normal," AOOs can more efficiently identify deviations that may signal potential security events.

AOOs can focus on establishing baselines for:

- **Network communications**: Which devices talk to each other, how often, and using which protocols
- **User activity**: Normal login times, locations, and account usage patterns
- **Device behavior**: Common processes, file access patterns, and system activities
- **Protocol patterns**: Typical Modbus/DNP3 commands, polling frequencies, and control sequences

Because operational conditions evolve over time, detection models and baselines should be periodically reviewed and updated. It is recommended to collect data for at least **30 days** to capture normal variations including weekday/weekend differences and routine maintenance. Use your monitoring platform to identify common communication patterns, frequent processes, and typical user activities. Document approved schedules for vendor access, maintenance windows, and configuration changes. Because operational conditions evolve over time, detection models and baselines should be periodically reviewed and updated.

3. THREAT HUNTING WITH MALCOLM

3.1. Installation and Configuration

For comprehensive step-by-step installation and configuration instructions, AOOs should refer to the official Malcolm documentation at https://malcolm.fyi. The documentation provides detailed guidance on hardware requirements, network architecture options, sensor deployment strategies, and protocol-specific configurations. When deploying Malcolm in BESS/IBR environments, pay particular attention to:

- Enabling industrial protocol parsers (Modbus, DNP3, BACnet, etc.) in Zeek configuration
- Configuring appropriate log retention policies based on regulatory and storage constraints
- Establishing secure, encrypted tunnels for sensor-to-server communication

- Implementing time synchronization across all sensors and the central server for accurate log correlation

Malcolm's modular design allows for phased deployment — start with a single representative BESS/IBR site to validate the configuration before scaling to additional locations.

3.2. Filtering Log Sources

Malcolm aggregates multiple types of security telemetry into a unified OpenSearch database, enabling hunters to correlate network traffic, endpoint activity, and threat signatures in a single interface. Understanding which log sources contain evidence of specific threats is essential for efficient hunting. Malcolm categorizes data into distinct log sources based on where and how it was collected. Each log source provides different visibility into your BESS/IBR environment. To access log sources through Malcolm's OpenSearch Dashboards interface:

1. Navigate to the Malcolm web interface (typically https://<malcolm-host>)
2. Click "OpenSearch Dashboards" from the main menu
3. Use the "Discover" tab to explore raw logs
4. Use pre-built dashboards for structured views of specific protocols or behaviors

From the “Discover” OpenSearch tab, AOOs can explore following log sources outlined in Table 4 to find specific types of activity in your environment**.** For example:

- To see all Modbus traffic, you may search: event.dataset: "modbus"
- To see successful Windows logins, you may search: winlog.event_id: “4624”

Table 4 lists of some of the most relevant log source filters for BESS/IBR threat hunting. The following log source commands can serve a variety of purposes depending on the environment. The following table is generalized and provides examples of potential uses. It is worth noting that there are many more types of Windows and application-specific logs that may have relevance as well. Linux-based systems also have security-relevant logs that can and should be collected for analysis (/var/log/auth.log or secure.log, /var/log/audit/audit.log, and many more[16]).

Table 4. Malcolm log sources for BESS/IBR threat hunting.

Category	Log Source	Description	BESS/IBR Hunt Use Cases
Network Traffic Analysis (Zeek)	`conn.log`	All network connections (source, destination, ports, bytes transferred, duration)	Baseline device communication patterns; detect unexpected connections; identify data exfiltration
	`modbus.log`	Modbus/TCP traffic including function codes, register addresses, and values	Monitor BMS/PCS write commands; detect unauthorized setpoint changes; identify unusual register access
	`dnp3.log`	DNP3 protocol traffic with function codes and object variations	Track grid interface commands; monitor inverter control operations; detect unauthorized operate commands

[16] Graylog. *25 Linux Logs to Collect and Monitor.* September 12, 2024. https://graylog.org/post/25-linux-logs-to-collect-and-monitor/

	`rdp.log`	Remote Desktop Protocol sessions	Monitor vendor/engineer remote access; detect off-hours connections; identify unusual source IPs
	`dns.log`	Domain name queries and responses	Identify command-and-control domains; detect DNS tunneling; find unauthorized external connections
	`http.log`	HTTP requests, responses, and user-agents	Analyze web-based device management; detect unusual API calls; identify malicious user-agents
	`notice.log`	Alerts generated by Zeek based on script-defined heuristics	Can identify network scanning, brute-forcing, invalid certificates, and more
	`ssl.log`	TLS/SSL certificate details and cipher information	Identify self-signed certificates; detect weak encryption; find encrypted C2 channels
	`smb.log`	File sharing and lateral movement activity	Track file transfers; detect lateral movement; identify credential harvesting
Signature-Based Detection	`suricata.log`	Triggered IDS signatures for known threats	Detect known malware; identify exploit attempts; flag policy violations
Endpoint Telemetry (Windows Event Logs + Sysmon[17])	`Windows Security Event Logs`	Security-relevant logs from the Windows operating system	Track user account creation, logins/failures, changes to account privileges, group membership, etc.
	`Windows PowerShell Event Logs – Event ID 4104 - Script Block Logs`	Use of PowerShell; Script Block Logging must be enabled in the registry or via Group Policy	Identify scripts run for reconnaissance, propagating files, establishing persistence, evading detection, etc.
	`Sysmon Operational Logs`	A variety of security-relevant operating system-level events	Process creation/termination, process access, network connections, registry modifications, drivers loaded, and more.

3.3. Operationalizing Indicators of Attacks within Malcolm

Populated with network traffic and endpoint logs, Malcolm can provide continuous visibility into the operational and cybersecurity health of BESS/IBR systems**.** Appendix A includes details of how indicators of attacks (IOAs) can be operationalized using specific data sources within the Malcolm ecosystem. By co-locating logs from Zeek, Suricata, Windows, Linux (and optionally, supplemental Sysmon logs) in OpenSearch (plus PCAP in Arkime), AOOs can correlate events related to the actions and communications occurring across their BESS/IBR control environments.

[17] Sysmon. *Sysmon – Sysinternals*. Microsoft Learn. Published July 23, 2024. HYPERLINK "https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon"https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

4. IDENTIFYING INDICATORS OF ATTACKS (IOAs)

Effective network threat hunting focuses on identifying anomalies that could impact availability, safety, or control integrity across power system assets. The following sections focus on specific IOAs for AOOs to look out for within their BESS/IBR networks.

4.1. Unauthorized or Unexpected Communications

BESS and IBR systems typically operate on tightly scoped communication paths, for instance, between inverters, BMS units, and supervisory controllers. Connections that deviate from the established pathways may indicate misconfiguration, malware presence, or adversary behavior. AOOs should focus on:

- East-west traffic between devices that normally have no reason to communicate (e.g., inverter-to-inverter connections).
- Repetitive outbound connections resembling beaconing to an external address. Note: software checking for updates may also resemble beaconing.
- Port and protocol anomalies, such as common protocols using new or non-standard ports; unrecognized that are not explained in the product or system documentation.
- Outbound communications to non-corporate or internet domains, which could represent data exfiltration and/or command-and-control (C2) activity.

One or more of these behaviors may represent internal discovery (network reconnaissance).

4.2. Industrial Protocol Anomalies

Protocols such as Modbus, DNP3, and IEC 61850 are fundamental to BESS and IBR control. They enable inverter telemetry, supervisory control, and real-time grid coordination. However, they are inherently trust-based and unauthenticated, making them ideal vectors for manipulation if network boundaries are breached. AOOs should monitor for:

- Unauthorized write or operate commands, especially those targeting setpoints for voltage, current, or charge/discharge limits.
- Function codes rarely seen during normal operations, particularly outside maintenance windows.
- Timing anomalies, such as control messages sent at irregular intervals or outside expected master-slave cycles.

When such traffic is detected, AOOs should immediately correlate it with authorized work orders or maintenance activity. If no legitimate explanation exists, the event should be treated as a potential control-plane compromise.

4.3. Off-Hours or Unscheduled Command Activity

In control environments, time of activity is a powerful detection dimension. Operations generally follow predictable cycles, and commands executed outside scheduled windows often point to remote compromise or misuse of credentials. AOOs should watch for:

- HMI or SCADA sessions initiated during overnight or unstaffed hours.
- Configuration changes or firmware updates occurring outside planned maintenance windows.
- Use of remote desktop, SSH, or VPN connections into the OT network from non-standard IPs or times.
- Repetitive command bursts consistent with automated scripts or unauthorized tooling.

An effective threat hunter will correlate such events with authentication logs (e.g., Windows Event IDs 4624/4625 or Sysmon data) to identify responsible accounts and origin systems. Any deviation from normal operator access patterns warrants deeper investigation.

4.4. Data Exfiltration or Payload Anomalies

While the loss of control is the most visible risk, data theft represents an equally dangerous vector. Adversaries often extract control logic, configurations, or credentials before disruptive actions. AOOs should watch for:

- Sustained TCP sessions or large data transfers from OT segments to external destinations.
- Encrypted outbound sessions (SSL/TLS) from devices that rarely initiate them.
- Sudden spikes in data volume relative to baselines for the host or subnet.
- Unscheduled file transfers between control servers and engineering workstations.

Once detected, AOOs should confirm whether the transfer aligns with approved vendor activity, patch distribution, or firmware updates. If not, the event should trigger containment and forensic collection.

4.5. Beaconing and Persistence Behaviors

Persistent access often manifests as subtle, rhythmic network activity. Adversaries use beacons to maintain control while avoiding detection. Indicators of beaconing include:

- Regular outbound connections to the same IP or domain at consistent intervals.
- Low-volume, short-lived TCP sessions that repeat identically.
- Usage of uncommon protocols (ICMP, UDP, or custom ports) for periodic check-ins.
- Encrypted traffic with self-signed or short-lived certificates that do not match enterprise PKI standards.

These behaviors are best detected through time-series analysis and correlation across Zeek logs and OpenSearch anomaly detection jobs. Persistent beaconing within OT subnets should always be treated as a high-confidence compromise indicator.

4.6. Logging and Visibility Gaps

Sometimes, the absence of data can itself be a signal. A compromised asset or adversary toolset may intentionally disable or corrupt logging to obscure activities. Indicators of visibility loss include:

- Sudden gaps in host logging from high-value assets such as HMIs or control servers may be evidence of tampering with the logging policies, configuration files, and/or forwarders.
- Significant changes in network traffic composition, or significant decrease in network traffic volume can be evidence of SPAN port config manipulation; it is not possible to manipulate a physical tap via software.

Threat hunters should treat these conditions as potential evasion tactics until proven otherwise.

4.7. Contextual Correlation and Baseline Deviation

Ultimately, network hunting in BESS/IBR environments is about contextual deviation rather than volume-based alerting. Every device, command, and protocol has a predictable operational signature deviations from those signatures signal change. AOOs should consider:

- Continuously compare current traffic patterns against established baselines for frequency, volume, and timing.

- Correlate anomalies across network, host, and process telemetry to identify root causes.
- Validate deviations against operational events such as system upgrades, maintenance windows, or site expansions.
- Integrate feedback from anomaly investigations into refined detection rules and updated baselines.

This process transforms detection from reactive alerting into proactive, intelligence-driven defense.

5. PHASING IMPLEMENTATION

Organizations seeking to deploy BESS/IBR threat hunting capabilities should view implementation as a phased, evolving program rather than a one-time project. Field experience has shown that the most successful outcomes come from validating capabilities incrementally, building institutional knowledge, operational maturity, and stakeholder confidence at each stage before expanding the scope.

5.1. Pilot Phase: Establish Foundational Capabilities

The initial pilot should focus on establishing baseline capabilities at a single representative site. This site should reflect the organization's typical architecture and operational conditions, as outlined in Section 2.2 of this guide. This stage serves primarily as a learning and validation phase, allowing teams to:

- Familiarize themselves with the tools and workflows.
- Establish a 30-day baseline of normal communications and activity.
- Conduct initial hypothesis-driven hunts using Malcolm's pre-built dashboards.

Early successes should be documented and shared responsibly to demonstrate value and secure continued stakeholder support. Teams can also consider recording lessons learned, configuration challenges, and visibility gaps to inform future expansion.

5.2. Expansion and Refinement Phase

With a solid foundation, organizations can expand monitoring and analytical coverage. Deploy additional sensors at key network segments, such as an OT DMZ boundary, a central control network, and one or more field sites with varying architectures. This phase introduces forwarding endpoint logs from engineering workstations and jump servers, tuning alerts, and developing cross-data source correlation searches for identifying more complex attack patterns.

Organizations can begin customizing queries and dashboards to reflect their unique BESS/IBR environment rather than relying exclusively on generic ICS templates. Baselines established during the pilot should be refined using operational feedback, acknowledging that "normal" may shift over time due to grid conditions or seasonal changes.

Regular review sessions between security and operations teams are critical to ensure hunting efforts remain contextually aligned. The creation of hunt playbooks for common scenarios helps transform ad-hoc investigations into standardized, repeatable procedures that improve consistency and scalability.

5.3. Operationalizing and Scaling

The final phase focuses on scaling proven capabilities across the organization while integrating threat hunting insights into broader security operations. Expansion should be risk-prioritized, targeting the most critical or exposed sites first.

Routine tabletop exercises involving security and operations personnel help maintain readiness and ensure clear communication during investigations. Measuring and reporting on the program's maturity, metrics, and outcomes supports continuous improvement and demonstrates value to leadership.

Ultimately, maintaining an effective threat hunting capability requires continuous evolution — regularly updating baselines, refining hypotheses, and integrating the latest threat intelligence to ensure resilience against emerging risks.

6. CONCLUSION

The deployment of IDS within BESS/IBR environments represents a critical step forward in achieving scalable, continuous visibility into OT networks. Throughout this guide, we have demonstrated how passive network monitoring, when combined with endpoint telemetry and hypothesis-driven hunting methodologies, can enable early detection of adversary activity without disrupting the critical grid operations that these systems support. This approach provides AOOs with the tools necessary to observe their BESS/IBR infrastructure through a security lens while respecting operational constraints.

By implementing baseline awareness of normal BESS/IBR communication patterns and device behaviors, organizations gain the ability to recognize deviations that may signal compromise or misconfiguration. Protocol-aware detection of unauthorized Modbus, DNP3, and other industrial control commands provides visibility into the command-and-control layer that traditional network monitoring would likely miss. The integration of network traffic analysis with endpoint activity creates opportunities for cross-layer correlation that can reveal sophisticated attack chains spanning multiple systems and time periods. When higher-fidelity investigation is required, full packet capture provides the forensic reconstruction capability necessary to confirm findings with certainty and understand exactly what occurred during a security event.

The ultimate value of these capabilities lies not merely in their technical sophistication, but in their ability to strengthen coordination between cybersecurity and operations teams. By providing a shared platform for understanding network behavior and investigating anomalies, threat hunting infrastructure creates a common ground where security professionals and operational engineers can collaborate effectively. This collaboration reduces attacker dwell time by ensuring that suspicious activity is not only detected but also understood in its operational context, enabling faster and more confident response decisions. Over time, this iterative process of hunting, detecting, and refining improves the overall resilience of DERs and contributes to the broader security posture of the electric grid.

Appendix A. Operationalizing IOAs within Malcolm

The following sections detail how IOAs can be operationalized using specific data sources within the Malcolm ecosystem. By co-locating Zeek, Suricata, Windows, Linux (and optionally, supplemental Sysmon logs) in OpenSearch (plus pcap in Arkime), AOOs can gain deeper insight into the actions and communications taken across their BESS/IBR control environments.

Zeek Log Analysis for BESS/IBR Environments

Zeek logs are the primary network data source analysts will interact with in Malcolm's OpenSearch instance to understand communication patterns between BESS/IBR assets. Below are some examples of how AOOs can use a selection of Zeek log types that may be of interest when hunting in these environments:

- **Conn Log (Connection Log):** Look for unusual source IP to destination IP + port + service (protocol) relationships, unusual connection duration (within a higher range than usual) for a given set of IPs, significantly higher than usual byte count for a given source/destination pair, or non-standard port usage to/from BESS/IBR assets.
- **DNS Log (Domain Name System Log):** Identify DGA (domain generation algorithm) patterns (high entropy), frequent new domain lookups, or spikes in NXDOMAIN responses, which can indicate C2 or reconnaissance.
- **HTTP Log (Hypertext Transfer Protocol Log):** Look for rare/unusual User-Agent strings, high volumes of POST requests to unusual paths, or frequent 4xx/5xx errors. Hunt for beacons (periodic, consistent HTTP requests) to external IPs.
- **SSL Log (SSL/TLS Log):** Identify self-signed, expired, or invalid certificates, and uncommon TLS versions/ciphers. Look for SSL connections to unusual external IPs from BESS/IBR assets.
- **DNP3 Log (Distributed Network Protocol 3 Log):** Focus on unusual function codes, abnormal polling frequencies, and write operations to critical DNP3 points.
- **Modbus Log (Modbus/TCP Log):** Identify unusual function codes, reads/writes to critical registers, and increases in exception responses.
- **RDP Log (Remote Desktop Protocol Log):** Monitor for RDP connections from unusual sources, connections on non-standard ports, and RDP login failures.
- **SMB Log (Server Message Block Log):** Detect unusual file access patterns, access to hidden shares, or spikes in SMB errors.
- **VPN Log (Virtual Private Network Log):** Hunt for unusual VPN user logins (new geo-locations, unusual times, dormant accounts) and high volumes of VPN connection failures.

Windows Event Log & Sysmon Analysis

While Zeek and Suricata provide network visibility, host-level telemetry from Windows Event Logs and Sysmon reveals the process-level and user-activity layer. Correlating both can help identify compromised devices, user accounts, and potential unauthorized access within control environments.

- **Security Event Log:** Identify high volumes of failed logins (4625), account lockouts (4740), new user account creation (4720), or group membership changes (4732/4733). Hunt for scheduled task

creation/modification (4698, 4702). Additional events to monitor can be found in Microsoft's events to monitor page.[18]

- **Process Creation (Event ID 1):** Look for unusual parent-child process relationships, processes executing from unusual directories, or with unusual command-line arguments. Calculate entropy of process names/command lines. Hunt for cmd.exe or powershell.exe executing unusual commands.
- **Network Connections (Event ID 3):** Correlate with Zeek. Look for internal processes connecting to external IPs or BESS/IBR assets that don't typically initiate connections.
- **File Creation (Event ID 11):** Identify executables dropped in unusual locations (e.g., public desktop, temp folders).
- **Registry Events (Event ID 12/13/14):** Monitor for modifications to run keys, service entries, or security-related registry values.

Advanced Correlation & Characterization (Cross-Log Examples)

Once network and host data are available, analysts should correlate events to uncover attacker behaviors that may appear benign in isolation but become high-risk when viewed together.

- **Malicious File Download (HTTP) → Execution (Sysmon) → C2 (DNS/SSL/Conn):** Correlate Zeek HTTP logs for suspicious downloads with Sysmon Process Create (Event ID 1) and subsequent Zeek network connection logs (conn.log, dns.log, ssl.log) for C2.
- **RDP Login (Zeek/Windows Event Logs) → Lateral Movement (SMB) → ICS Protocol Usage (Modbus/DNP3):** Correlate successful RDP logins (Zeek rdp.log, Windows Event Log 4624) with subsequent SMB activity (Zeek smb.log) and ICS protocol commands (Zeek modbus.log, dnp3.log) originating from the RDP destination.

Leveraging OpenSearch Security Analytics and Threat Intelligence

To maintain scalability and consistency, operationalize the above hunting workflows within OpenSearch Security Analytics. This enables automated alerting, rule-based detection, and enrichment with threat intelligence feeds.

- **Sigma Rules:** Upload Sigma rules into OpenSearch Security Analytics to detect common adversary techniques specific to BESS/IBR environments (e.g., PowerShell network connections to C2 ports).
- **Zeek Notices:** Utilize Zeek's built-in alerting for anomalous activities.
- **Zeek Intel:** Populate the Zeek Intel[19] configuration file with IOAs to match against IPs, domains, hashes, etc. your network traffic. Supports integration with:
    - STIX™ and TAXII™
    - MISP

---

[18] Microsoft. *Appendix L: Events to monitor.* Microsoft Learn. Last modified May 30, 2025. GitHub+1 https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

[19] Malcolm. *Zeek Intelligence Framework.* Accessed December 3, 2025. https://malcolm.fyi/docs/zeek-intel.html

    - Google Threat Intelligence
    - Mandiant
- **Suricata Rules:** Integrate Suricata for IDS/IPS. Deploy specific Suricata rules for ICS protocols (Modbus, DNP3) to detect known attacks or malformed packets.
- **IOA Enrichment:** Use lookup tables or OpenSearch Security Analytics Threat Intelligence Feeds to enrich logs with known bad IPs/domains and generate alerts.
- **CTI Workflow:** Regularly ingest and prioritize CTI, scan historical data with new IOAs/TTPs, configure proactive monitoring, and perform contextual analysis using all available logs and alerts (Zeek, Suricata, Windows, Sysmon).

Packet Analysis with Arkime

When higher-fidelity inspection is required, analysts can pivot into Arkime for raw packet inspection and forensic reconstruction. Arkime complements Zeek and Suricata by enabling payload-level review of suspicious communications. Arkime can also be leveraged to search for specific types of byte sequences using its built in "Hunt" feature, though a pre-filter query is required. Some examples of how it may be used are as follows:

- **Analysis of cleartext protocols (Telnet, FTP, HTTP, etc.):** can observe credentials and commands used in Telnet, files transferred via FTP, and full web session activity over HTTP, for example. Notably, FTP and HTTP have Zeek parsers, but Telnet does not due to its relatively unstructured nature.
    - **Note:** Zeek does have a dynamic protocol detector for Telnet but it's disabled by default and may cause performance issues. Telnet sessions can often be inferred to exist based on sustained connections to its default port (TCP 23) in the conn log. If you have pcap available in Arkime, these inferences can be fully validated or disproven.
- **DNP3/Modbus Packet Structure:** Use Arkime to inspect raw packet bytes for DNP3 and Modbus traffic to identify:
    - Unexpected object types or variations.
    - Unusual data values in write commands.
    - Non-standard message lengths or framing errors.
    - Proprietary extensions or custom fields that deviate from standard specifications.
- **Timing Analysis:** Visualize inter-packet timings to reveal "slow-drip" data exfiltration or bursts of traffic indicative of rapidly-issued, automated commands related to network scanning, active directory enumeration, or password spraying.

Crafting Custom OpenSearch Queries and Dashboards

Once detection baselines are established, custom dashboards and queries allow both analysts and AOOs to visualize key behaviors and refine operational awareness for their specific BESS/IBR network segments.

- **PLC Write Commands by Source IP:** Monitor Modbus/DNP3 write operations to critical BESS/IBR PLCs.
- **High Volume of Failed Logins to HMI:** Track authentication attempts on Human-Machine Interfaces.

- **External Connections to RTUs:** Visualize connections to Remote Terminal Units.
- **Segment-Specific Dashboards:** Create dashboards tailored to different BESS/IBR network segments (e.g., IT-OT DMZ, Process Control Network) to focus on relevant traffic patterns and typical behaviors.

Operational Rhythm and Review Cadence

Effective monitoring should blend continuous, automated detections of IOAs with analyst-driven hunting as they review the alerts and correlate events of interest. Regular communication between cybersecurity and operations personnel may help resolve erroneous alerts and ensure genuine risks are prioritized. Analysts and operators should collaborate periodically to review dashboards summarizing connection volume, top talkers, and protocol distributions, noting deviations from expected ranges.

- **Daily:** Observe key IOAs and alert trends for deviations.
    - As extraneous alerts are understood, resolved, and filtered out, these daily sessions may cease to be necessary.
- **Weekly:** Correlate events against current threat intelligence to identify delayed indicators of compromise/attack.
- **Monthly:** Conduct review sessions between cybersecurity and operations teams to validate alerts, assess persistent patterns, and refine baseline expectations.

AOOs should maintain a consistent engagement schedule with monitoring teams to align detection priorities with real operational context.