A SIDE-BY-SIDE COMPARISON BETWEEN AN IT SOC AND A SPECIALIZED OT SOC SUCH AS THE HONEYWELL OT SOC

Scenario: An alert triggered due to unusual network traffic originating from an engineering workstation (EWork-1) located between the IT and OT network. This workstation is targeting a specific PLC in the process control network.

The deep packet inspection tool installed on the plant reports that this workstation is sending multiple Modbus/TCP “write multiple registers” commands to the PLCs, trying to change setpoint values.

Those changes are happening outside of any planned maintenance window.

Phase in the Incident Response	Generic IT SOC Response	Specialized OT SOC Response	Why a specialized OT SOC matters
Detection and Alerting	A firewall triggers an alert: "Policy violation – Traffic from EWork-1 to 10.100.20.22 (PLC-22) on TCP port 502." A generic IDS also detects: "MODBUS Application Protocol Detected." Since Modbus traffic on port 502 isn't considered high risk in most IT environments and no clear threat pattern is recognized, the alert is likely categorized as low or medium priority. It may be seen as odd, but not necessarily urgent.	A deep packet inspection (DPI) tool detects: "Anomalous Modbus Write Command from EWork-1 to PLC-22 attempting to change critical setpoint values." This alert is immediately flagged as high priority because it involves an unsafe Modbus write command sent outside of a scheduled maintenance window potentially impacting process safety.	The OT SOC treats this as a serious incident right away. They understand that any unplanned attempt to modify a PLC is highly suspicious, given how industrial systems are supposed to run. This operational awareness and knowledge of client procedures allows them to respond quickly. In contrast, the IT SOC lacks this specific context, so the alert might not raise red flags immediately.
Triage & Analysis	The IT analyst confirms that port 502 is used for Modbus and notices repeated attempts to write data. However, they don't recognize the risk tied to unauthorized changes to a PLC. Following standard IT procedures, they begin by scanning the engineering workstation (EWork-1) for malware or suspicious software, focusing only on the source system.	The OT analyst recognizes the Modbus write commands as a serious concern indicating an active attempt to change controller settings outside of any approved maintenance window. They cross-check internal governance notes and maintenance schedules and quickly determine that no authorized work is planned for EWork-1 or PLC-22, confirming likely unauthorized activity.	The OT SOC analyst immediately flags the unexpected controller modification as a high-risk event, understanding its potential operational impact. In contrast, the IT SOC analyst concentrates on the origin of the traffic rather than the nature of the traffic itself, delaying appropriate response while searching for evidence of malware.

Communication & Coordination	The IT analyst follows standard procedure opening a ticket and notifying the IT infrastructure team. Communication follows a formal chain and may take time to escalate to someone with operational insight.	The OT SOC analyst immediately reaches out to on-site personnel such as the plant supervisor using pre-established direct lines of communication. They quickly verify whether the Modbus write commands from EWork-1 to PLC-22 were expected or authorized.	A major difference between OT and IT SOCs is how fast and directly they can connect with the right people. The OT SOC is built for urgency it has clear procedures and active contact lists to reach key plant decision-makers within minutes. This rapid confirmation process is often critical, especially in time-sensitive industrial environments. In contrast, the IT SOC may experience delays due to layered internal processes and lack of familiarity with operational stakeholders. Even without knowing exactly what the PLC does, quick communication can prevent serious issues.
Containment & Mitigation	Once the IT infrastructure team contacts the plant manager, it's confirmed that the Modbus activity wasn't authorized. The IT SOC analyst recommends isolating the engineering workstation (EWork-1) using standard IT containment procedures such as network quarantine or system shutdown. However, this action is taken without full awareness of how it might affect plant operations, potentially creating further issues.	After confirming with on-site staff that the write command was unauthorized, the OT SOC analyst takes a more targeted approach. They immediately direct plant personnel to inspect PLC-22 and advise isolating EWork-1 using emergency firewall rules instead of broad disconnection. The top priority is to quickly restore PLC-22 to a known safe state to prevent any safety or production risks, while also stopping further unauthorized commands and gathering more context.	The OT SOC doesn't just react they act with purpose. They quickly identify the affected devices, communicate directly with the right people, and begin containment in a way that avoids unintended downtime or damage. Thanks to pre-established communication lines and operational awareness, their actions are both fast and informed.
Eradication & Recovery	The IT team focuses primarily on the affected engineering workstation (EWork-1), opting to clean or re-image the system. However, they lack the tools, processes, or contextual knowledge to investigate the PLC. As a result, the status and integrity of PLC-22 remain unknown, leaving potential risk unaddressed.	The OT SOC takes a broader, more process-aware approach by immediately directing the investigation toward PLC-22, recognizing the potential operational risk. The recovery effort ensures both EWork-1 and PLC-22 are fully checked and verified before the incident is considered resolved.	Unlike the IT SOC, the OT SOC is focused on preventing operational disruptions. It investigates both the source (EWork-1) and the target (PLC-22) to not only stop the incident at its origin but also confirm the integrity of affected systems—minimizing risk and restoring safe operations.

Conclusion: Why a specialized OT SOC matters

This scenario highlights why a dedicated OT SOC is essential in industrial environments. The OT SOC's advantage lies in its deep understanding of the client's operational norms, security governance, and the critical context surrounding industrial assets like PLCs. Unlike a traditional IT SOC, which often lacks visibility into

process-level risks and depends on formal escalation paths, the OT SOC can respond immediately flagging the event as high priority and contacting plant personnel within minutes.

This rapid, context-aware response enables faster containment, minimizes operational disruption, and ensures both the source and the target of the anomaly are properly assessed. Even if the situation doesn't pose an immediate safety threat, a delayed or misinformed response could lead to downtime, compliance issues, or unintended system behavior.

Ultimately, the OT SOC's procedural awareness, established communication channels, and vendor-agnostic expertise allow it to act decisively turning what could be a critical incident into a controlled event. This reinforces the strategic value of an OT SOC not just as a monitoring function, but as a business enabler that protects continuity, safety, and trust.