

# Secure the Entryway to Your OT Network

In the last year, there has been an alarming [87% increase](#) in cyberattacks directed at crucial Operational Technology (OT) assets. The risk of cyberattacks for OT is currently at an unprecedented peak, with malicious actors continuously discovering new ways to compromise organizations.

Visibility into the network is a paramount when protecting OT environments, where the consequences of an attack can be catastrophic. Lumu is continuously monitoring critical environments, keeping organizations steps ahead of pervasive cyber attacks. With advanced detection capabilities, organizations can gain real-time insights into anomalous activity helping security teams detect and automate responses to threats in real-time.

## Benefits



Proactively identify when OT environments attempt to contact adversarial infrastructure directly or through a malicious proxy in your IT environment.



Automate responses to attacks targeting your critical assets using out-of-the-box integrations with existing tools.



Quickly identify activity targeting your OT environment with the ability to prioritize and view OT incidents.



Get all of the details around threat actor activity with insights into MITRE Attack techniques and tactics being leveraged against critical environments.

## Key OT Features for OT Infrastructure:

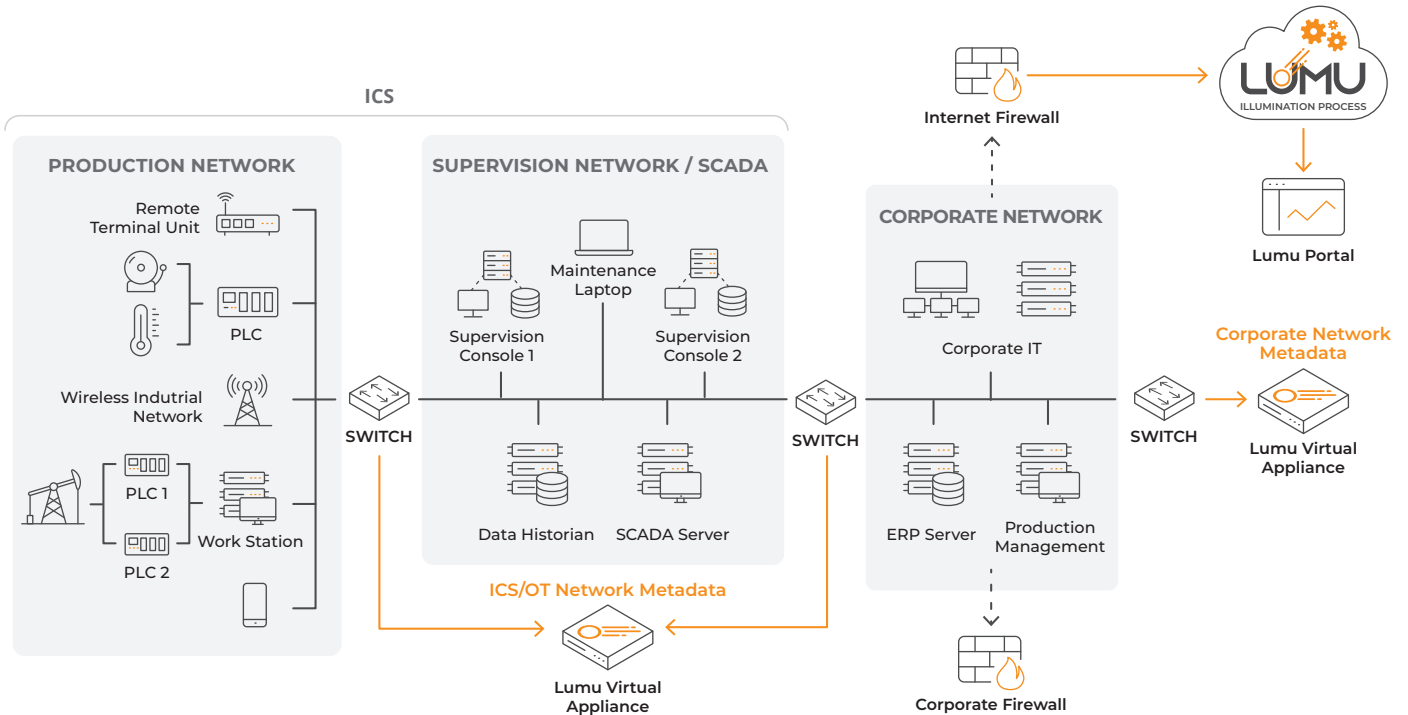
Lumu's approach helps organizations identify anomalies, unusual traffic patterns, and potential threats, while taking real-time action to maintain the security of OT systems.

- **Labels:** Sort and organize network traffic according to business relevance and source, helping you more precisely identify compromise activity targeting your OT infrastructure.
- **Compromise Context:** Gain comprehensive information about confirmed incidents that helps teams respond quickly with details around what happened and which OT assets were targeted.
- **Automated Response:** Integrate real-time information about confirmed compromise instances with your existing tools via API to orchestrate your defense.
- **Incident View:** Understand exactly what happened, how the attack originated, and which assets were impacted from a single view.



## How it Works:

Lumu is continuously monitoring your OT environment analyzing all network traffic. Metadata from across the network and connected OT devices is collected by Lumu for real time analysis.



When anomalous activity is detected, Lumu immediately investigates it, reports any malicious findings, and automatically blocks the incident. All incidents contain details about exactly what happened, how it happened and what actions were taken against the threat.

This rapid response helps prevent potential damage and keeps your critical OT systems running smoothly. With Lumu, OT devices stay one step ahead of cyber threats, ensuring the security and reliability of your OT infrastructure.

Contact Lumu: [sales@lumu.io](mailto:sales@lumu.io)