



ICS/OT Asset Discovery

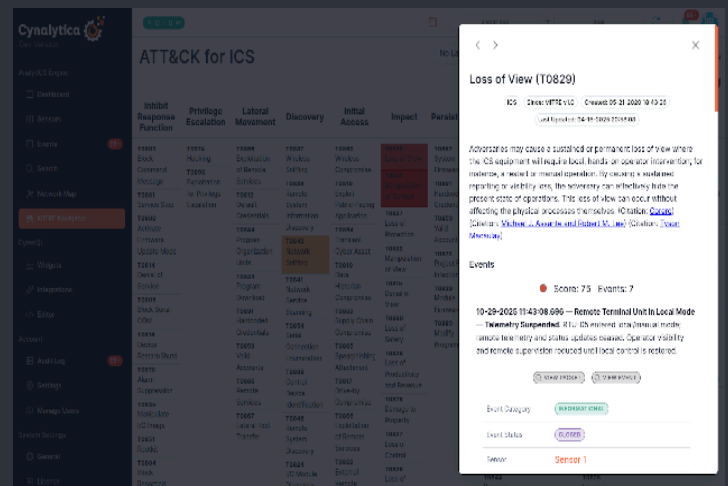
MITRE ATT&CK® for ICS Mapping Across IP, Fieldbus, Serial and Analog Communications

The AnalytICS Engine maps detections onto MITRE ATT&CK® for ICS techniques as they occur. Open a technique and you see the events from your own environment that matched it, and you can go from there to the packet.

An alert queue tells you what triggered. It does not tell you what happened.

Industrial environments generate alerts faster than anyone can read them, in a chronological list where a rogue master, a spoofed report, and a session reset arrive as three unrelated rows. The pattern connecting them is exactly what a queue cannot show.

Most teams answer this by maintaining an ATT&CK coverage map by hand. It is a picture of what they believe they could detect, drifting out of date the moment it is saved. Useful for planning, useless during an incident.



Populated by your telemetry, not by hand

Technique tiles carry counts and scores drawn from events the Engine observed. A current picture of the environment rather than an assessment written last quarter.

Reaching below Level 3, where other tools do not

The events feeding the matrix come from IP, fieldbus, serial, and analog monitoring. Techniques that manifest at the physical and serial layers, where most ICS tooling has no visibility, can be evidenced rather than assumed.

Every technique leads to the packet

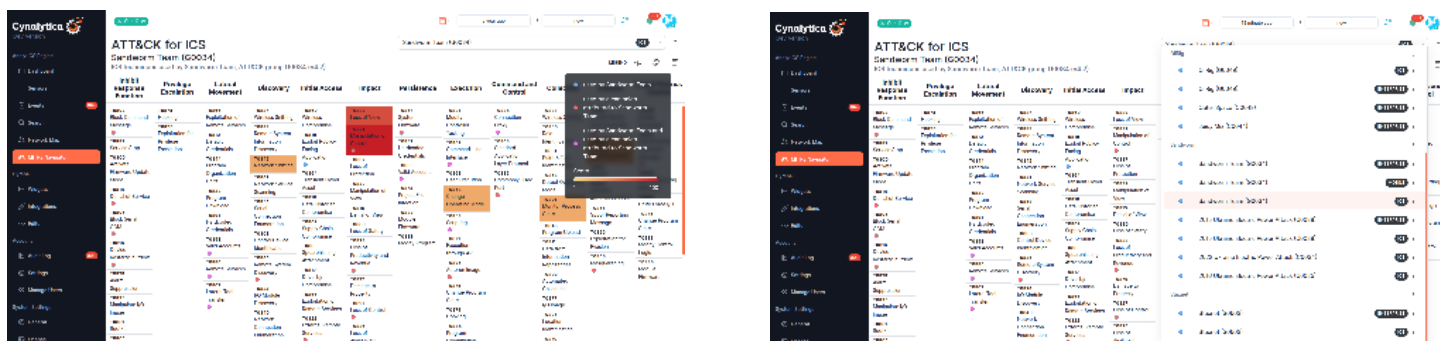
From a technique tile to the matching events to the underlying packet, without leaving the Engine. The definition, citations, and adversary-specific detail sit in the same panel.

IT and OT in one place

Adversary groups operate across both. Switch between the ICS, Enterprise, and Mobile matrices with the same layer selected and see how enterprise activity precedes impact in the control environment.

Adversary and Campaign Layers

Select a threat group, campaign, or piece of malware and the matrix highlights the techniques attributed to it. Use it to hunt for behaviors you do not normally see, and to check whether you have coverage where a relevant adversary is known to operate.



How Teams Benefit

Analysts start from the matrix rather than the queue, working from techniques with new activity and pivoting to evidence. Hunters select a layer relevant to their sector and look for techniques they never see, which is usually a visibility gap rather than good news. Engineers use techniques accumulating benign events to tune thresholds, and techniques with no detections to decide what to build next. Leadership gets tactic-level summaries in a taxonomy that means the same thing to everyone in the room.

Layers are Context, Not Attribution

Selecting an adversary layer shows which techniques that group has been observed using. It does not mean that group is in your network. Used well it sharpens what you investigate first. Used carelessly it produces a conclusion the evidence does not support, and the Engine keeps the two clearly separate.

Demonstrated in the field

Cynalytica has publicly demonstrated detection of specific MITRE ATT&CK® for ICS techniques in wastewater treatment operations through the collection and analysis of non-IP communications: Unauthorized Command Message (T0855), Alarm Suppression (T0878), Modify Parameter (T0836), and Block Serial COM (T0805).

See it against your own traffic

MITRE ATT&CK® for ICS mapping is included in the AnalytICS Engine:

cynalytica.com/mitre-attck-for-ics

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.