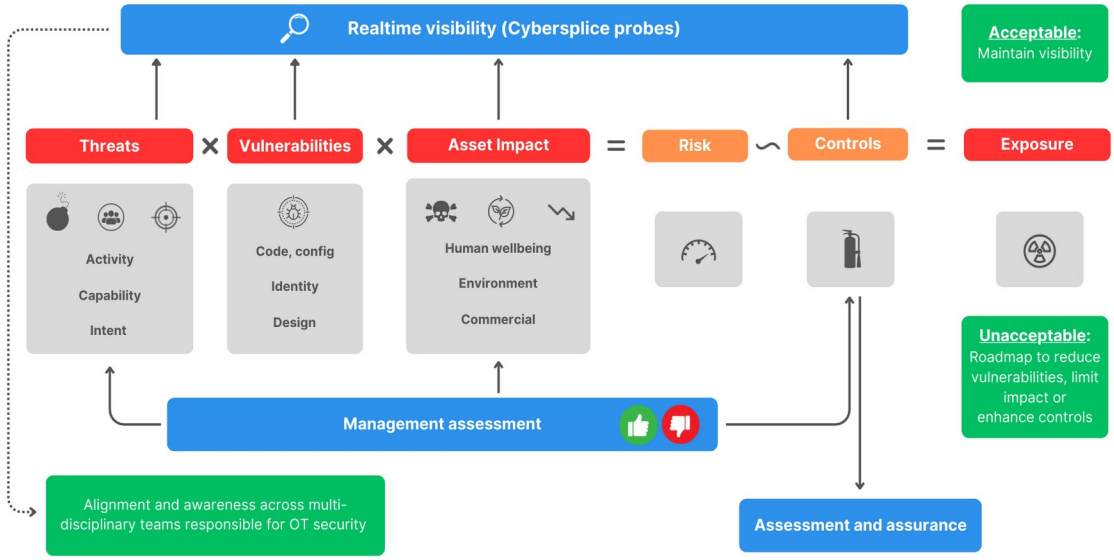
Cybersplice professional services

visibility, measurement and management of cyber-physical exposures

Cyber-physical resilience is the point where technical, process and people-orientated controls are balanced with an informed view of threats, vulnerabilities and asset impacts. This requires both a shared **awareness** as well as **visibility** into the existing cyber-physical security posture.

Awareness requires understanding threat capability and intent, vulnerabilities, the potential impact on assets, environment and human well-being, as well as the options available to manage risk (ie to reduce the likelihood of these elements connecting or to reduce the potential resulting impact).



OT networks usually have a very high level of **visibility** into the process (chemical, environmental, mechanical etc.) that is being managed. This visibility is obtained through set-point monitoring, collection, analysis and trending, and threshold monitoring. Visibility at the infrastructure level (ie cyber-physical visibility) is often however completely lacking.

Cybersplice enables rapid visibility into cyber-physical exposures on Operational Technology networks through our zero-touch, virtual and hardware probes.

In assisting customers with developing their cyber-physical security road-map, Cybersplice

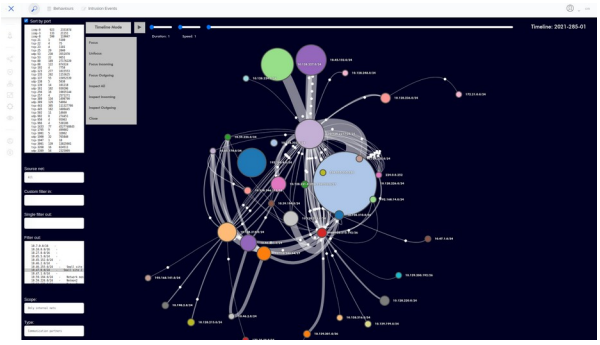
firstly facilitates a shared understanding of cyber-physical exposure elements. Management input is solicited to identify industry and geographical compliance requirements, unique Operational Technology safeguards in the environment (such as pressure release valves and SIS's), and to assess individual exposure elements.

This view is supplemented with visibility gained from Cybersplice probes to understand immediate exposure, avoidable risks and mitigation options for unacceptable exposure levels.

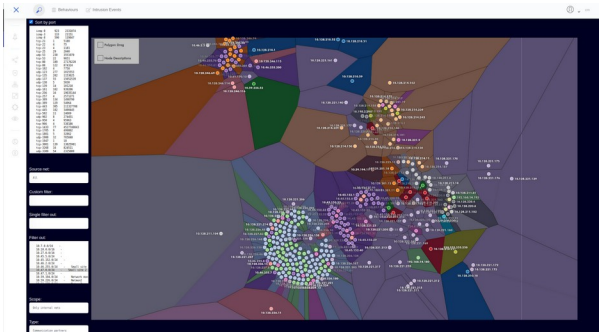
These inputs form the basis of the cyber-physical security roadmap. Following the initial assessment and development of the roadmap, Cybersplice probes may remain in the environment for ongoing visibility and providing an early warning system. Visibility could mean the difference between an incident with a minor impact and a catastrophe.

Deep visibility into OT networks: the good, the bad and the ugly. The screenshots below show some of the Cybersplice advanced visualizations and insights available from the rapid visibility offering:

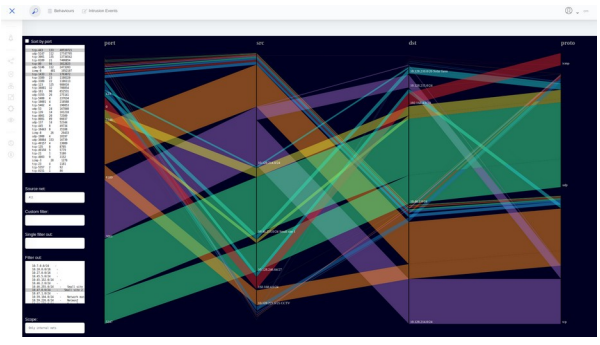
Cybersplice timeline replay of OT comms



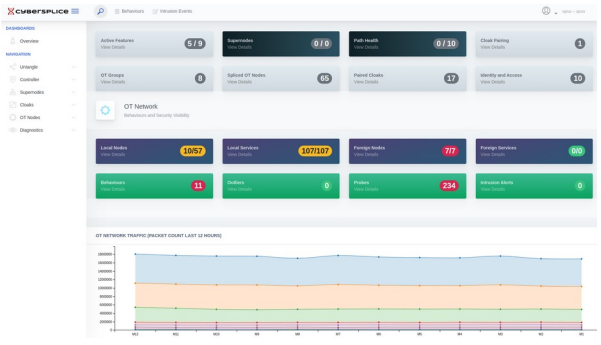
Clustering of communication partners



Who's talking to who: flow summary



Cybersplice dashboard birds eye view



Cybersplice **prevents**

destructive cyber-physical attacks

by shielding vulnerable equipment inside an encrypted overlay network in edge and in-path modes

Insecure protocol wrapping

Cybersplice draws OT communications into an encrypted overlay network, shielding unauthenticated and vulnerable ICS protocols from adversaries.

In-core isolation

Prevent cross talk between OT groups across the entire network, at the edge as well as right inside the overlay network core.

OT network traffic profiling

Profile OT network traffic at key points with out-of-band mirror mode, or the entire network using in-path mode.

Behavioural monitoring

Leverage the near-deterministic nature of OT traffic to identify attacker behaviour and unauthorized changes to the network or nodes.

Outlier detection

Cybersplice uses AI to identify anomalies in device to device communication, and to detect compromised devices and command-and-control back channels.

Secure remote access

Facilitate seamless and secure remote access for partners, operators and engineers.

Untangle

Cybersplice acts as a flight recorder for OT communications, bringing visibility down to the infrastructure level. Visualize and understand OT network traffic, perform threat hunting and forensic analysis going back a full year.

Identity shielding

Strengthen fragmented and weak identities across the OT landscape through authentication offloading and multi-factor injection.

Role based access control

Build role based access controls into legacy systems without touching the code.

Increased resilience

Scale Cybersplice Supernodes to increase resilience, leveraging underlay redundancy, and building parallel paths across the overlay network.

Eliminate bridges

Eliminate unauthorized and unintentional bridges between IT and OT networks through edge mode deployments.

Autopilot

Automatically triage newly detected behaviours for rapid on-boarding or in noisy converged networks.

Secure access edge

Cybersplice provides a secure access edge across the entire OT environment, mediating crypto-keys for all nodes using cloaks, including limited spec legacy devices.

Intrusion detection

Detect common attack signatures with IDS in the network core.

Transition from mirror mode to in-path protection at your own pace, or deploy Cybersplice on-site in mirror mode with in-path available as a contingency when under attack.