Cybersplice enables and secures Operational Technology in Mining environments

Mining environments leverage Operational Technology (OT) for a number of functions, ranging from life preserving environmental systems, to those enabling operations such as sensors, access control, surveillance and time and attendance. Due to the primary requirement around safety and reliability, as well as environmental protection concerns, incidents involving Operational Technology failures could be devastating.

OT in mining environments have historically been designed to cater for environmental, chemical, electrical and mechanically induced failures. Intentional attacks and collateral damage from IT cyber incidents can however cause major damage when spilling into the OT environment, as these threats were never anticipated until IT and OT networks started connecting and converging.

Management of this OT landscape is complicated by the number of vendors involved, inherent vulnerabilities in OT, dated and insecure Industrial Control Protocols, and long lifecycles of deployed devices. The business benefit of IT / OT Network connection and convergence is however undeniable as it enables desirable features such as predictive maintenance, ERP integration, advanced analytics, real time monitoring and remote support.

Splice provides **security visibility** into OT networks and enables **connectivity and convergence** through secure integration inside an encrypted overlay network. Splice capabilities specifically applicable to the Mining industry include:

Standardised and secure remote access

Facilitate standardised, seamless and secure remote access for all partners, operators and engineers. Remote Access Users connect into the overlay network

Identity shielding

Strengthen fragmented and weak identities across the OT landscape through authentication offloading and multifactor injection.

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.

Behavioral monitoring

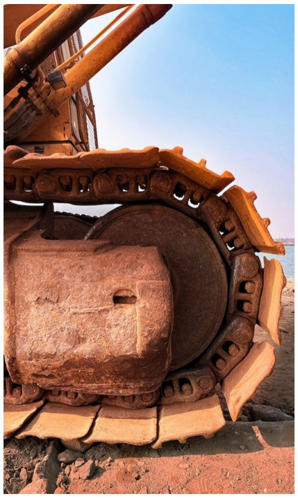
Leverage the near-deterministic nature of OT traffic to identify attacker behavior and unauthorised changes to the network or nodes.

Outlier detection

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

In-core isolation

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



https://cybersplice.com

CYBERSPLICE

Secure access edge

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

Untangle

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

Role based access control

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

Insecure protocol wrapping

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

Increased resilience

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

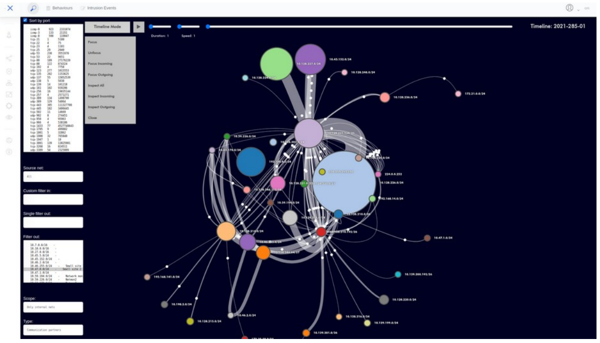
Autopilot

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

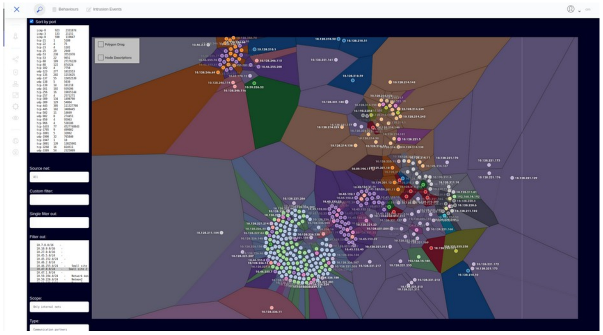
Deep visibility in Operational Technology networks, the good, the bad and the ugly

The screenshots below show some of the Cybersplice advanced visualisations and behavioural tracking:

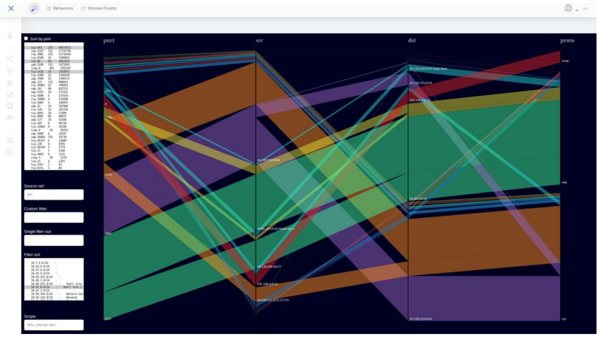
Cybersplice timeline replay of OT comms



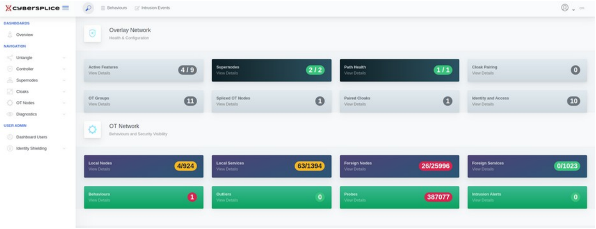
Clustering of communication partners



Who’s talking to who: flow summary



Cybersplice dashboard birds eye view



Overlay Network
Health & Configuration

Active Features View Details 4 / 9
Supernodes View Details 2 / 2
Path Health View Details 1 / 1
Cloak Pairing View Details 0
OT Groups View Details 11
Spliced OT Nodes View Details 1
Paired Cloaks View Details 1
Identity and Access View Details 10

OT Network
Behaviours and Security Visibility

Local Nodes View Details 4/924
Local Services View Details 63/1394
Foreign Nodes View Details 26/25996
Foreign Services View Details 0/1023
Behaviours View Details 1
Outliers View Details 0
Probes View Details 387077
Intrusion Alerts View Details 0

https://cybersplice.com