Use Case: Eliminating Asset Visibility Gaps with Real Time Enforcement

Vertical: Transportation, International airport

Use Case:

During Nelysis' automatic assets discovery learning period, our system detected and identified an active, operating old CCTV & VMS legacy network, which was still connected to the new network while remaining undiscovered and unmonitored. The customer, from his end, was not aware of it; he thought the legacy systems had been disconnected years ago.

Sequence of events:

- Detected an unknown, unauthorized suspicious IP address connected to the network.
- Detected the asset was communicating, creating a behavioural violation & potential cyber breach.
- Detected the physical location of the asset with the suspicious IP.
- Actively isolated the asset while shutting down the suspicious communication session, yet kept the device active.
- Sent the CSO team to the physical location while alerting the CISO & the SOC.
- Identified the asset as a legacy system that should have been disconnected from the network a couple of years ago.

Business Value:

- Prevented security breaches by actively identifying blind spots in real-time, generating complete, accurate network visibility complemented by physical, logical & TDA maps.
- Provided real-time monitoring underpinned by an automated response to cyber threats, mitigating vulnerable assets & systems risks and enhancing security controls.
- Reduced MTTD & MTTR with real-time detection & enforcement, isolating any suspicious unauthorized behaviour preventing literal movement and insider threat, safeguarding business continuity.