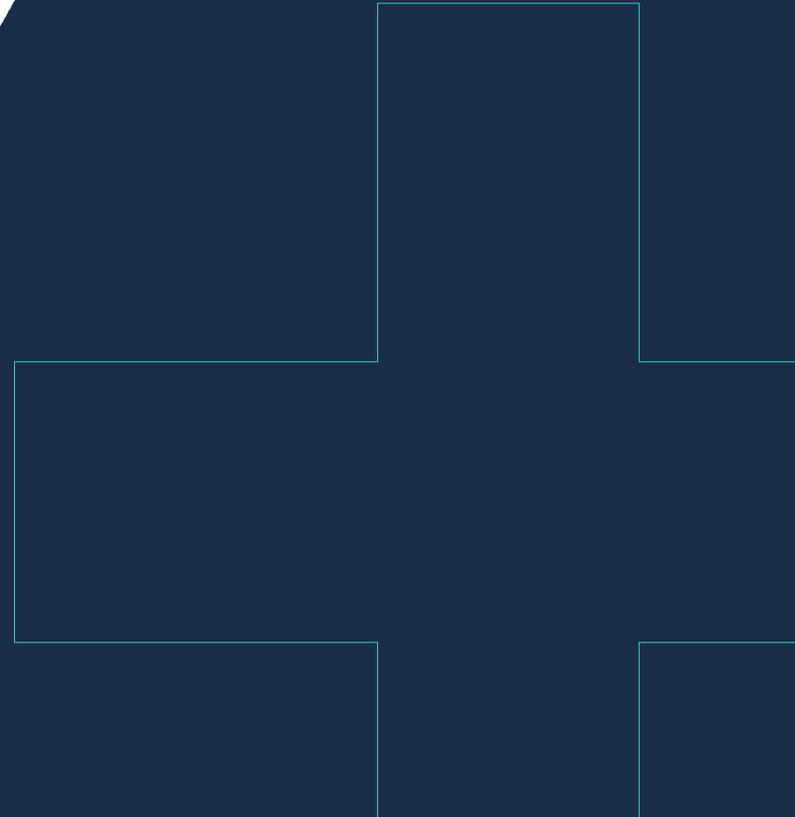# REGIONAL RAIL SERVICES PUT AT RISK BY CYBER EXPLOIT

KINETIC IT PROTECT+ AND MICROSOFT

April 2021

PROTECT +
kinetic IT

CRITICAL INFRASTRUCTURE SERVICES EXPLOITED

CONTEXT SETTING

A critical regional rail services provider on the east coast of Australia had concerns about the security posture and the potential exploitation of the environment due to lack of visibility across a comprehensive range of data sources within the environment.

INCITING INCIDENT

The customer had a known vulnerability on an externally facing web service. This was exploited by threat actors and malware was installed and used as a staging service to attack other organizations.

MOMENT OF CHOICE

The Kinetic IT PROTECT+ solution always made sense to the Customer, however, this incident highlighted the need to senior leadership that not only advanced tools are required but advanced methods of management and detection.
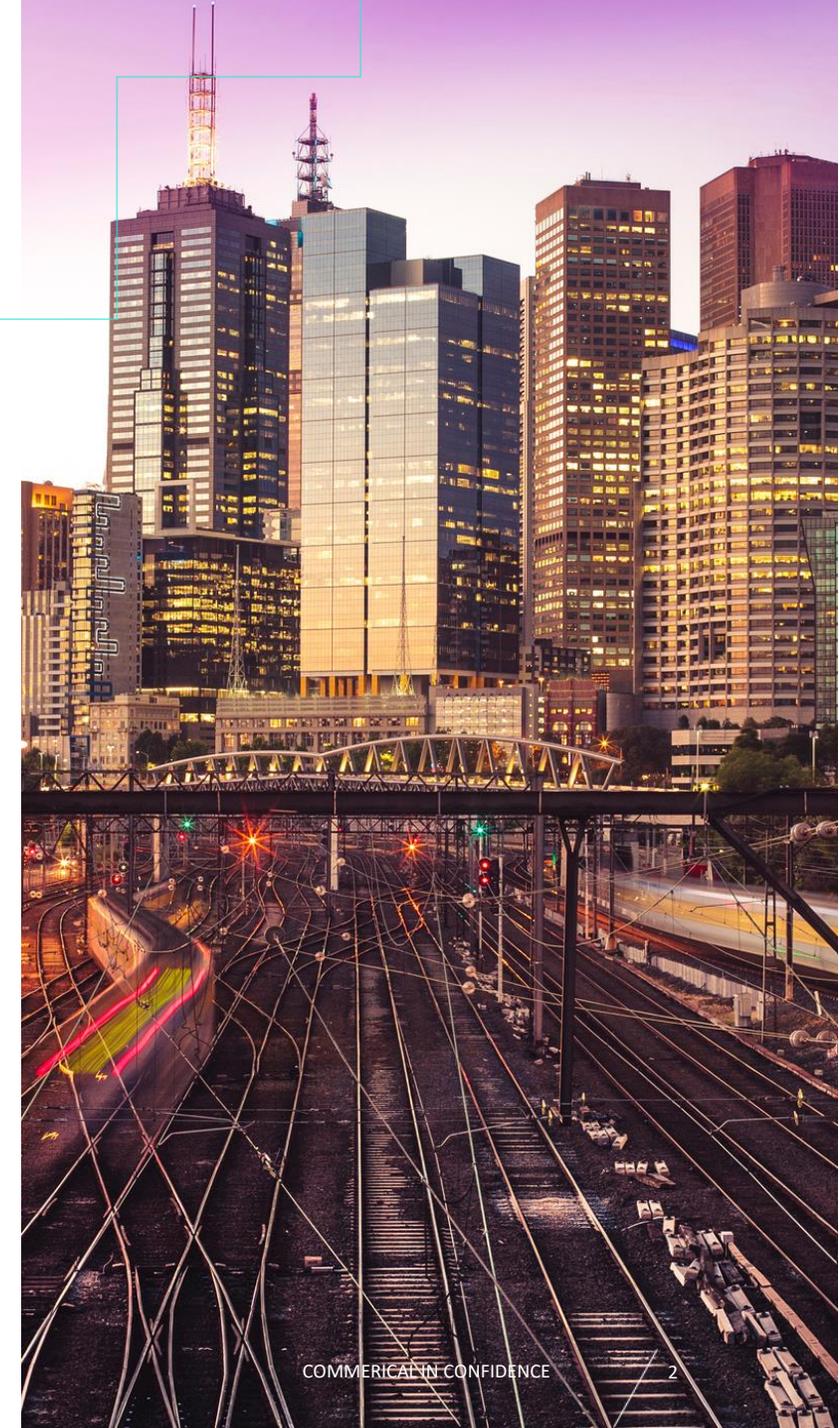
PROTECT +/
kinetic IT

# RAPID RESPONSE AND PROTECTING THE ENTERPRISE

RISING ACTION

To a critical services infrastructure provider such as regional rail, the exploitation of external services the risk is now a company board priority. This now drives a holistic approach to risk and response. The Kinetic IT PROTECT+ service provided these assurances to all levels of management.

CLIMAX

The Kinetic IT PROTECT+ team deployed and rapidly expanded the collection of disparate data sources using Microsoft platforms including ATP and Office365 into the SOC. This coupled with a proactive security program covering people and process, including activities such as risk assessments, threat hunting, incident response planning, and forensic readiness.

FALLING ACTION

The security program enabled a consistent and holistic approach to cyber risk management across the entire organisation thus providing the company board the assurances essential to running a critical infrastructure services business.
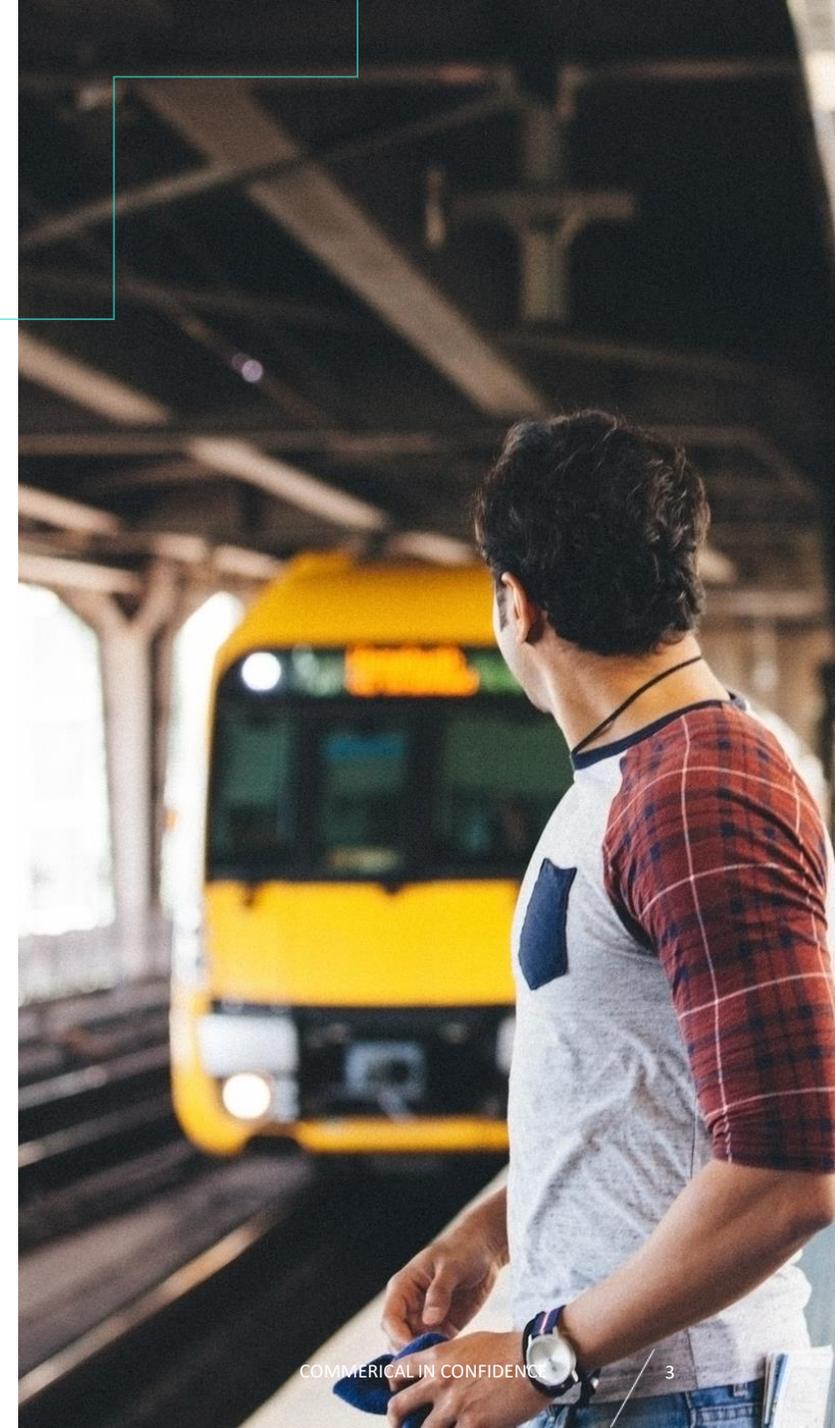
CRITICAL INFRASTRUCTURE SERVICES EXPLOITED

SOLUTION ROLLOUT

Within 3 months the services have been established as the new ways of working within BAU. This included holistic threat management , threat response, and forensic capable investigations.

SOLUTION BENEFITS

Since deployment of the Kinetic IT PROTECT+ solution, including the Microsoft platforms, the foundation has been set to further expand the visibility across all operational environments with integrated capabilities and reduced investment.

OTHER INDUSTRIES

Mining and Resources
- Iron Ore
- Oil and Gas

Critical Infrastructure
- Water Authorities
- Electricity Suppliers
- Law Enforcement

Transportation
- Railways
- Airlines
- Waterways

PROTECT +/
kinetic IT