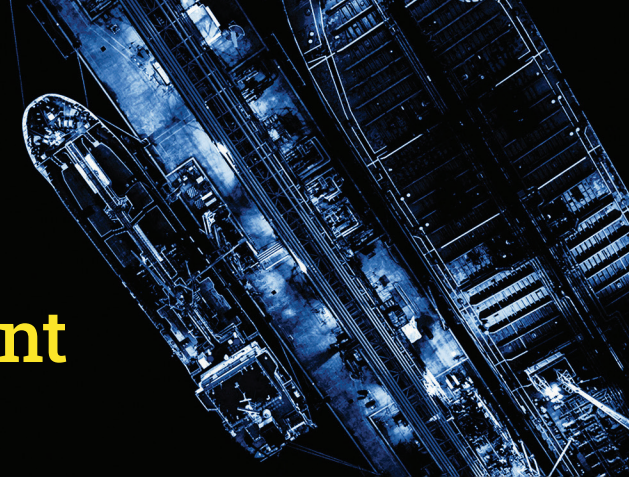
SAPIEN CONDOR

Vulnerability Management



Condor is Sapien's vulnerability management system, designed specifically for Industrial Control System (ICS) security requirements. Condor uses the IEC 62443 risk methodology to give a clear picture of critical systems and their risk drivers, then identifies and prioritises the vulnerabilities so patching and mitigation activities achieve the highest risk reduction possible.

Condor delivers in-depth vulnerability assessment of hardware and software in OT and IT networks. We map devices against systems, and systems against your organisation's risk assessment matrix to produce a network vulnerability baseline (NVB). This provides a comprehensive view of your assets from a vulnerability, impact, and associated risk perspective. The system then processes daily intelligence feeds from several industry leading sources against your NVB and alerts users of potential threats, the associated risks and recommended remediation activities.

Sapien, providing cutting edge sovereign technology for immediate and adaptive protection across Operational Technology (OT) and Information Technology (IT) assets.

Key Benefits

- Vulnerabilities described and prioritised in terms of risk to the client's built environment.
- Rapid Response reports delivered for emerging high and critical risk vulnerabilities on a daily basis.
- Clear view of the nature and extent of legacy vulnerabilities.
- Routine maintenance plans which identify remediations to address all legacy vulnerabilities.

Contact us to explore how the Condor suite can protect and defend your organisation.

1800 378 200 sales@sapiencyber.com.au **www.sapiencyber.com.au**

SAPIEN CONDOR

OT networks are becoming more and more connected to corporate environments and are therefore rapidly becoming increasingly visible to threat actors.

Condor provides a risk-driven approach to closing the gaps that threat actors exploit, describing and prioritising vulnerabilities in terms of risk to the built environment and the client's risk model.

In an OT environment, finding and patching every vulnerability can range from difficult to impossible. Active scanning of networks, which is commonly used in IT environments to detect and manage vulnerabilities, can cause instability and shutdowns in an OT environment and therefore is rarely deployed, or is deployed only in limited segments of OT networks. The Sapien Condor system uniquely handles newly reported and legacy vulnerabilities through two key functions:

The Vulnerability Engine

Enables our client to focus their rapid response on only the most serious issues.

- Ingests external vulnerability feeds and matches vulnerabilities to client inventory.
- Identifies and provides recommendations for where failure presents serious consequences.
- Risk driven approach that incorporates organisational risk models, not theoretical risk models.
- Targeted response that filters low-risk events and keeps the focus on key systems and highly exploitable vulnerabilities.
- Reports all high risk inventory and quantifies the associated risk per device.
- Effective coverage, driven by multiple 3rd party threat intelligence feeds. ICS Specific.
- No-touch - doesn't require network connection or scanning.

The Attack Surface Engine

Provides an overall view exposure, enabling organisations to reduce the overall threat surface of their facilities.

- Maps all vulnerabilities by matching inventory to the global threat and vulnerability databases.
- Identifies the worst vulnerabilities, a full catalogue of vulnerabilities and the current recommended remediations for incorporation into routine maintenance activities.
- Total coverage, identifies every vulnerability on every device; and the worst vulnerability on each device.
- Targeted recommendations, distinguishes between security and functionality patching - reports security updates ONLY.
- No-touch - doesn't require network connection or scanning.

Cyber criminals are becoming more sophisticated and more creative in architecting attacks against critical infrastructure.