




# NASSAR




## Sector vulnerabilities

With almost one third of organisations in the energy and industry sectors recording at least six intrusions in 2024, cyber security incidents are becoming increasingly problematic. Data suggests\* that advanced technologies are contributing to the growing complexity of managing certain threats to which all manufacturing, logistics, energy, and utilities (MLEU) organisations are vulnerable. Select a vulnerability area below to learn more:




### Manufacturing

-  Legacy equipment
-  Unsecured IIoT devices
-  Third-party access




### Utilities

-  Water treatment facilities
-  Smart grids
-  Distributed energy resources

### Energy

-  Remote access monitoring
-  IoT-enabled smart meters
-  Distributed denial-of-service

### Logistics

-  Connected fleet systems
-  Warehouse management systems
-  IoT-enabled asset tracking

For more information on these and sector specific vulnerabilities view our whitepaper or eBook.



\*2024 State of Operational Technology and Cybersecurity Report [www.fortinet.com/resources/reports/state-of-ot-cybersecurity](http://www.fortinet.com/resources/reports/state-of-ot-cybersecurity)

