AI EDGE LABS

ENERGY AND UTILITIES CYBERSECURITY

Energy and Utilities Under Cyber Attack

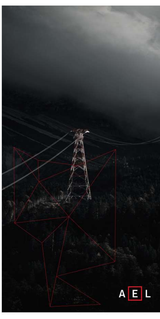
The average cost of a data breach in the energy sector ranges between $4.65 to $4.72 million.

8.2%

of observed attacks targeted energy organizations, ranking it the fourth-most attacked industry.

85%

of respondents have experienced a security incident in the last 12 months.



IoT Transforms Energy and Utilities

$110B

Expected market for Industrial IoT in energy and utilities by 2025

46%

of energy organizations report completing some IIoT/OT security projects.

69%

of energy organizations consider IoT devices critical to map their critical grids.

Cyber Threats at a Glance

25%

of respondents have been impacted by mega-attacks involving skills established by nation-state actors.

77%

of assets in energy networks have porous IT or OT boundaries, leading to a larger attack surface.

90%

of internal controls were shut down by the Delta-Montrose Electric Association due to malicious cyberware that wiped 25 years of data.

$4,4M

Leak colonial Pipeline paid $4.4M in ransomware as a result of a single password suspected to be taken from a dark web.

Top Attack Types

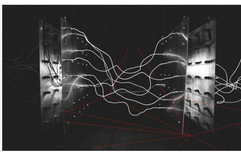
Ransomware	25%
RAT`s	17%
BEC	17%
DDoS	17%

Top Attack Vectors:

Vulnerability exploitation

40% 60%

Fishing



Cybersecurity Landscape in Energy & Utilities

Energy and utilities companies will spend $10B on cybersecurity by 2025.

84%

of energy professionals believe a cyber attack is likely to cause physical damage to energy assets.

57%

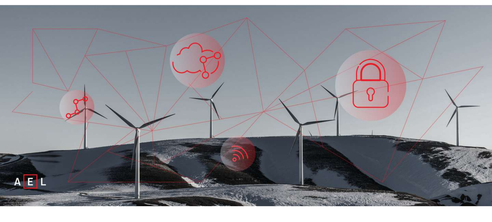
anticipate the loss of life within the next two years as the result of a cyber attack.

Cybersecurity Maturity in Energy and Utilities

Cybersecurity and privacy baked into every business decision or plan	50%
New budgeting process for cyber spend or investments	44%
Better and more granular quantification of cyber risks	44%
Respondents assert confidence in knowing what to do if there's a potential cyber attack.	30%

18%

of energy organizations use AI and big data analysis to monitor and recognize threats.



AI EdgeLabs can provide full visibility and protection for IoT/IIoT assets in the energy and utilities industry by monitoring your devices 24/7, even in unstable or offline operations. The AI EdgeLabs agentless Sensor is quick to deploy and can deliver early and advanced threat detection to prevent malfunction, misuse, and system damage.

AI EdgeLabs delivers network data analysis in real-time and remediation by preserving low latency. Thanks to our mix of reinforcement learning and machine learning algorithms, our security platform protects your edge and OT/IT environments from network threats, malwares, and zero-day attacks with up to 99% accuracy.

PROTECT YOUR EDGE & IOT ENVIRONMENT

AI EDGE LABS