Blacklight

Securing the Backbone of Critical Infrastructure

Critical infrastructure operators worldwide are increasingly facing a growing number of sophisticated cyberattacks, driven by geopolitical tensions and heightened competition, according to Cybersecurity and Infrastructure Security Agency (CISA).

116%
year-over-year

RISK OF CYBERATTACKS
Surge of IoT-targeted cyberattacks in 2022 – *Gartner*

The utilities sector, including energy, water, and transportation, has become a prime target for complex threats engineered by nation-states, and other threat actors for advanced persistent threats (APT) and ransomware attacks.

42%

CRITICAL INFRASTRUCTURE
Experienced a data breach in the energy sector – *CISA*

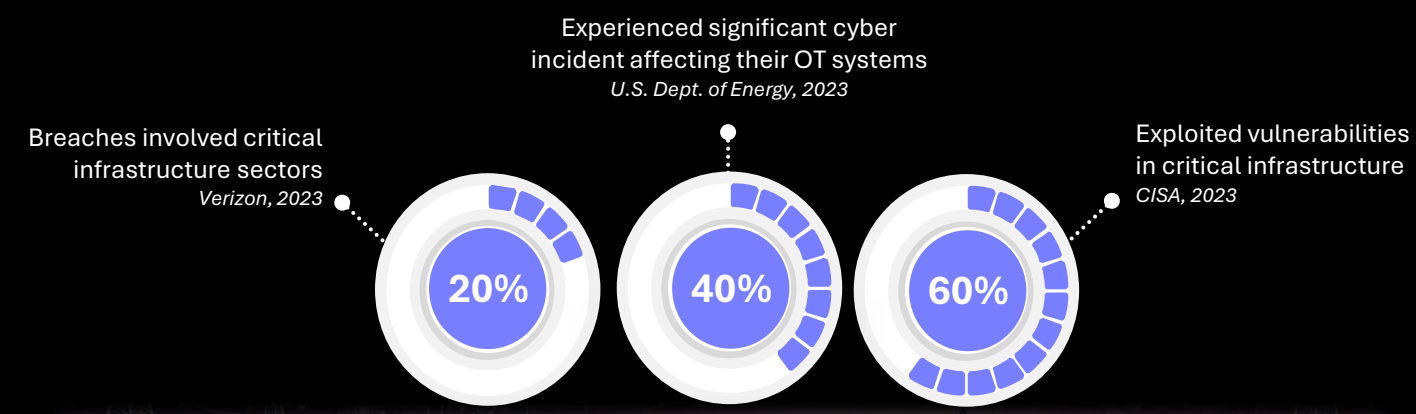
The integration of the Internet of Things (IoT) and Operational Technology (OT) with Information Technology (IT) networks has significantly amplified the vulnerability of industrial systems, as more devices become interconnected and data transfer increases.

3.1 MIL.
US dollars

FINANCIAL IMPACT
Average cost per incident for organizations – *Ponemon Institute*

Business Benefits of Proactive Monitoring & Detection Platform

In addition to addressing the technical challenges of cybersecurity, implementing proactive monitoring and detection software, such as the Blacklight's AI-driven platform, delivers several critical business benefits.



INFO@BLACKLIGHTAI.COM | WWW.BLACKLIGHTAI.COM

Blacklight

Blacklight AI – Sector Overview

Critical infrastructure organisation operate within both IT and OT environment. These include energy, water, transportation, telecommunication, healthcare and governments industries. Robust cybersecurity is essential for safeguarding these vital assets and must implement robust proactive cybersecurity measures to prevent disruptions and ensure the stability of society.

Key Challenges – Sector Focused

Addressing the evolving cyber threat landscape and maintaining robust security measures are critical challenges for both our clients and the broader sector. These challenges make comprehensive security monitoring and detection a complex task:

- Lack of advanced visibility & governance
- Increasing cyber threats
- Discrepancies between IT & OT environments
- Ineffective incident response

Blacklight AI – The Solution

Improving Critical Infrastructure Resilience

Unified IT/OT System Monitoring

Analyses and correlates data from diverse sources (SCADA, ICS, IT), including analytics of packets for signs of malicious activities, unauthorized modifications or unusual data flow patterns.

Advanced Threat Detection

Utilises AI, UEBA and CTI to detect sophisticated threats in real-time. While ML algorithms help establish baselines of activity to identify deviations indicative of potential threats or unseen sequences of malicious events.

Contextualized & Enriched Accuracy

Enhances detection accuracy and true positive rates with AI and CTI. Monitor and alert on variances of data source hygiene and predict long-term volume trends.

Incident Response & Automation

Accelerates response times with automated alert processing, escalations and threats remediations via Smart APIs.

Threat Hunting & Effective Search

Large Language Models (LLM) for plain English searches, enabling rapid data processing and refinement of results within seconds.

Blacklight AI Significantly Improves The Overall Cybersecurity Posture

60%
reduction in incident detection time

50%
reduction in false positives

60%
improved efficiency in security operations with automation & integration

> 40%
savings in Total Cost of Ownership (TCO) over 3-5 years

INFO@BLACKLIGHTAI.COM | WWW.BLACKLIGHTAI.COM