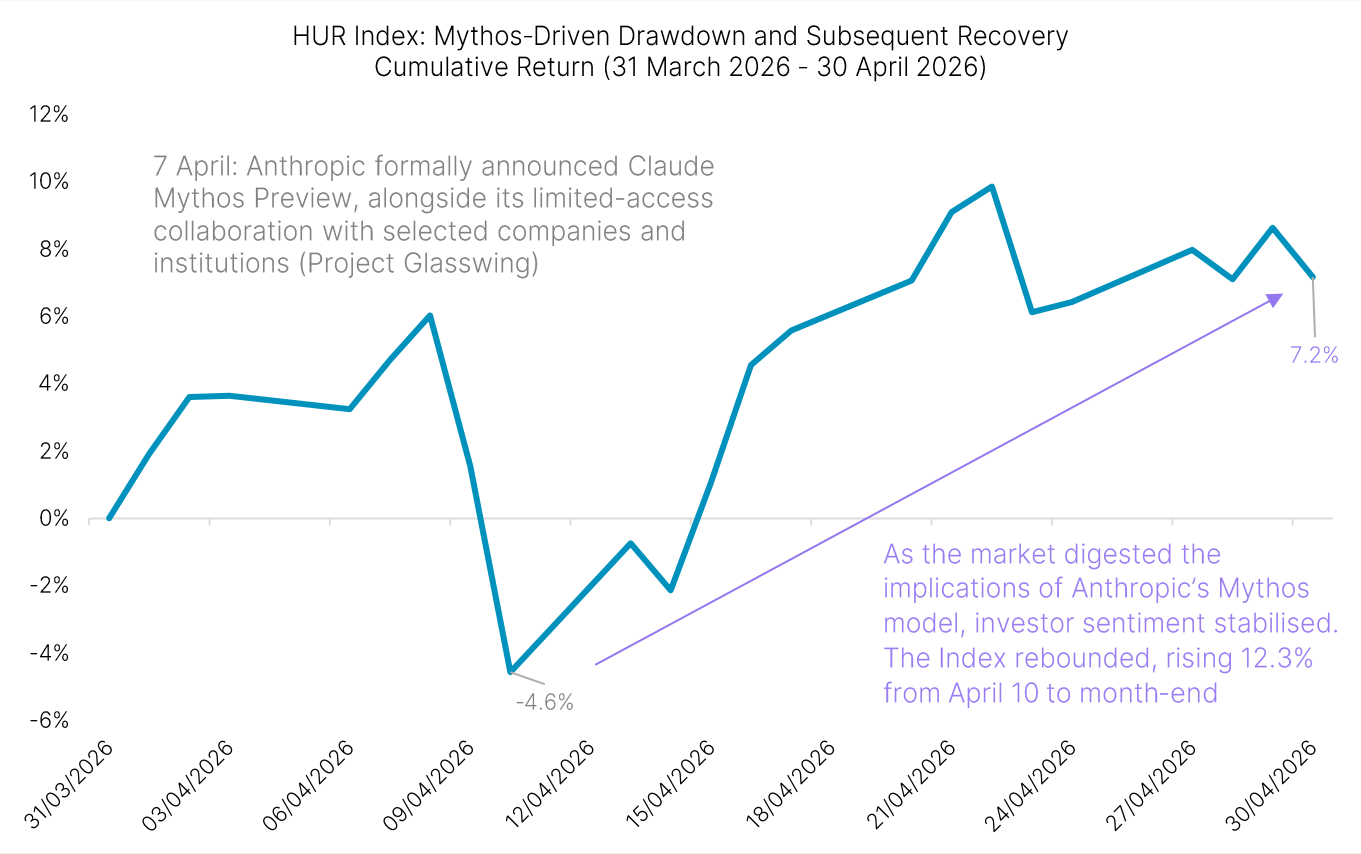
From Digitalisation to Disruption: OT Security in Critical Infrastructure

April 2026 – Cybersecurity Monthly Update

Ilaria Sangalli, *Head of Index Insights, EMEA*

April marked a period of adjustment and subsequent recovery for the ISE Cyber Security UCITS™ Index (HUR™) and the broader cybersecurity space, following a late-March disclosure around Anthropic's Mythos model that briefly unsettled cybersecurity equities. Initial market reactions reflected concerns that frontier AI could materially accelerate vulnerability discovery, raising questions about the durability of parts of the existing security stack.



Source: Bloomberg

As April progressed, sentiment recovered as further disclosures, independent assessments, and industry commentary clarified that Mythos-type capabilities are primarily concentrated in pre-deployment vulnerability discovery, rather than displacing core cybersecurity functions such as endpoint, network,

cloud, or security operations. With fundamentals and demand trends largely unchanged, investors differentiated business models more clearly and the sector rebounded.
The Index ended April with a total return of +7.2%, while the S&P 500 and MSCI World gained 10.5% and 9.6%, respectively.

Deep Dive - From digitalisation to disruption: cyber risk in critical infrastructure. Shaping the next phase of cybersecurity demand

Critical infrastructure - power grids, utilities, industrial systems, transport, and AI-driven data centres - is undergoing rapid digitalisation and electrification. As infrastructure becomes more digital and distributed, traditional boundaries between information technology (IT) and operational technology (OT) continue to blur. Systems that were once isolated and manually operated are increasingly connected, automated, and software-defined.

This structural shift is changing the nature of cyber risk. Cyber incidents in critical infrastructure are less about data theft alone and increasingly about disruption: loss of operational visibility, manipulation of control systems, or forced shutdowns that can affect energy supply, industrial output, or the delivery of essential services.

Electrification further compounds these risks. Power grids are becoming more complex as renewable generation, EV charging infrastructure, and distributed energy resources are added at scale. Many of these assets operate at the network edge and are remotely managed, increasing reliance on digital connectivity between local devices and central control systems. This creates conditions in which cyber attacks can directly affect availability and reliability, rather than just data integrity.

This exposure has already materialised in practice. In December 2025, Poland's energy sector experienced a cyber attack targeting OT and industrial control systems (ICS) across multiple electricity and renewable energy facilities. According to CERT Polska and CISA, attackers exploited internet-facing edge devices and remote access systems to gain access to control environments at renewable plants and a combined heat and power facility.[1]

A similar pattern was observed in the water sector. In April 2025, a cyber intrusion affected a water-management dam in Norway after attackers gained remote access to the control systems of the Lake Risevatnet facility. The incident stemmed from a poorly secured, internet-facing control interface protected by weak authentication, allowing external actors to directly access and manipulate operational technology systems. During the intrusion, a water discharge valve was forced fully open for approximately four hours, resulting in water outflow above mandated minimum levels. Although the incident caused no physical damage or public safety impact, it demonstrated that cyber attackers were able to gain direct access to infrastructure controlling real-world physical processes, highlighting persistent security gaps in exposed OT environments.[2]

These incidents align with broader threat intelligence trends. Trellix reports that OT and ICS environments are now being deliberately targeted as strategic objectives for both state-sponsored actors and

[1] https://www.cisa.gov/news-events/alerts/2026/02/10/poland-energy-sector-cyber-incident-highlights-ot-and-ics-security-gaps
[2] https://industrialcyber.co/industrial-cyber-attacks/lake-risevatnet-dam-hack-exposes-industrial-cyber-gaps-as-weak-passwords-risk-critical-infrastructure-attacks/

ransomware groups. Between April and September 2025, Trellix detected 272,512 OT/ICS-related threats across 572 organizations, with manufacturing, energy, utilities, and transportation the most exposed. Attacks frequently pivot from IT into OT, exploiting weak segmentation, insecure remote access, and engineering workstations, enabling disruption of physical processes, safety systems, and availability rather than just data theft.[3]

Growth outlook and implications for cybersecurity providers

This framing reflects a broader shift in how cybersecurity is perceived. Rather than a standalone IT function, it is increasingly seen as an enabling layer for safe electrification, resilient infrastructure, and scalable AI deployment. This shift is driving sustained growth in cybersecurity investment focused on OT, continuous monitoring, asset visibility, and infrastructure resilience - areas where cyber incidents can have economic, physical, or societal consequences rather than purely digital impacts.

According to MarketsandMarkets, the global critical infrastructure protection (CIP) market (covering physical security, IT cybersecurity, and OT cybersecurity) is projected to reach around USD 200 billion by 2030, growing at an annual rate of approximately 5-6%. Within this broader market, OT cybersecurity stands out as a structurally distinct and significantly faster-growing segment. MarketsandMarkets estimates that global spending on OT security solutions will increase from roughly USD 23 billion in 2025 to more than USD 50 billion by 2030, implying a CAGR of around 16-17% - well above the overall CIP growth rate. This expansion is driven primarily by demand for asset discovery and visibility, network security and segmentation, vulnerability management, identity and access management, and OT-specific SIEM[4] platforms, with large industrial and critical-infrastructure operators representing the largest share of spending.[5]

Within this broader expansion, OT-focused cybersecurity solutions are gaining relevance. Palo Alto Networks launched its expanded OT security offering in late 2024, as a response to this shift, citing both the rising frequency of attacks on industrial systems and the growing operational impact when those attacks occur. Palo Alto Networks expanded its OT security offering by extending its existing AI-driven cybersecurity platform into industrial environments, adding capabilities designed for legacy systems, remote operations, and harsh on-site conditions - such as guided virtual patching, secure privileged remote access, and ruggedized industrial firewalls.[6]

In March 2026, SentinelOne partnered with Armis to unify asset visibility and threat detection across IT, IoT, OT, and cloud environments. Armis provides continuous, agentless visibility of all assets (especially IoT, OT, and unmanaged devices) by observing network traffic. SentinelOne brings XDR, threat detection, correlation, and automated response across endpoints, cloud, and networks. Together, they deliver unified visibility and faster incident response across managed and unmanaged assets, a growing problem as IT and OT environments converge and the attack surface expands.[7]

[3] https://www.trellix.com/assets/reports/ot-threat-report-nov-2025.pdf
[4] Security Information and Event Management
[5] https://www.marketsandmarkets.com/Market-Reports/critical-infrastructure-protection-cip-market-988.html
https://www.marketsandmarkets.com/Market-Reports/operational-technology-ot-security-market-18524133.html
[6] https://www.prnewswire.com/news-releases/new-ot-security-solutions-from-palo-alto-networks-address-growing-cybersecurity-threats-to-industrial-operations-302280797.html
[7] https://keepnetlabs.com/blog/sentinelone-partners-with-armis-for-unparalleled-asset-intelligence

This strategic focus is also translating into commercial momentum for Fortinet. In the last quarter, the company highlighted accelerating growth in its OT security business. CEO Ken Xie noted that demand for operational technology solutions is contributing meaningfully to performance, with related billings growing by more than 25%.

OT exposure within the ISE Cyber Security UCITS™ Index (HUR™)

Within the HUR Index, a subset of constituents show identifiable exposure to Operational Technology (OT) and Industrial Control Systems (ICS) security, reflecting varying degrees of involvement in protecting industrial and critical infrastructure environments

The following section examines selected examples in greater detail.

- Fortinet (index weight of 5.78%)[8]: dedicated OT Security solutions including FortiGate Rugged appliances and the FortiGuard OT Security Service, designed specifically for industrial protocols and ICS networks.[9]
- Palo Alto Networks (index weight of 6.26%): a standalone Industrial OT Security offering providing OT asset visibility, risk assessment, and OT-specific protection, recognized by Forrester as an OT security leader.[10]
- Cisco (index weight of 6.61%): a clearly defined Industrial Security portfolio (notably Cyber Vision) embedded in industrial networking equipment, focused on OT visibility, segmentation, and protection of ICS environments.[11]
- Check Point (index weight of 3.63%): ruggedized industrial firewalls and ICS/SCADA security gateways focused on perimeter protection and OT protocol enforcement.[12]
- CrowdStrike (index weight of 6.39%): Falcon for XIoT, explicitly designed to provide visibility and protection for OT and industrial assets.[13]
- Qualys (index weight of 4.56%): Dedicated ICS / OT visibility and vulnerability management modules (VMDR-OT).[14]

[8] Weight as of EOD April 30, 2026
[9] https://www.fortinet.com/solutions/ot-security
https://www.fortiguard.com/services/operational-technology-security-service
[10] https://www.paloaltonetworks.com/network-security/ot-device-security
https://www.paloaltonetworks.in/company/press/2024/palo-alto-networks-recognized-as-a-leader-in-operational-technology-security-solutions
[11] https://www.cisco.com/site/us/en/products/security/industrial-security/cyber-vision/index.html
[12] https://www.checkpoint.com/quantum/next-generation-firewall/industrial-control-systems-appliances/
[13] https://www.crowdstrike.com/en-us/platform/falcon-for-xiot/
[14] https://docs.qualys.com/en/vmdr-ot/latest/get_started/vmdrot_overview.htm

Disclaimer:

Nasdaq®, ISE Cyber Security UCITS™, and HUR™ are registered trademarks of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.

Information set forth contains forward-looking statements that involve a number of risks and uncertainties. Nasdaq cautions readers that any forward-looking information is not a guarantee of future performance and that actual results could differ materially from those contained in the forward-looking information. Forward-looking statements can be identified by words such as "will," "may", and other words and terms of similar meaning. Such forward-looking statements include, but are not limited to, statements related to future activities and results. Forward-looking statements involve a number of risks, uncertainties or other factors beyond Nasdaq's control. These risks and uncertainties are detailed in Nasdaq's filings with the U.S. Securities and Exchange Commission, including its annual reports on Form 10-K and quarterly reports on Form 10-Q which are available on Nasdaq's investor relations website at http://ir.nasdaq.com and the SEC's website at www.sec.gov. Nasdaq undertakes no obligation to publicly update any forward-looking statement, whether as a result of new information, future events or otherwise.