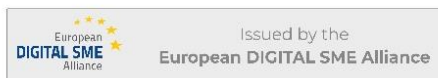


SecPoint - European on-prem cybersecurity for resilient critical infrastructure

Connect4Cyber Stockholm | 23 April 2026

Victor M. Christiansenn
CEO & Founder, SecPoint, Denmark



About SecPoint®



European cybersecurity company with its own in-house development



Serving customers and partners in more than 140 countries



On-prem cybersecurity solutions for trusted operational resilience



24-hour European support and strong customer commitment

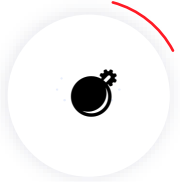


Donated cybersecurity software to support Ukraine's digital resilience



Western logistics under cyber pressure

Joint Cybersecurity Advisory | 21 May 2025



Russian GRU targeted Western logistics and technology companies.



Campaign targeted organisations supporting aid to Ukraine using spearphishing and Microsoft Exchange exploitation

European Commission cloud breach

CERT-EU analysis published 2 April 2026



A compromised Trivy update gave attackers access to an AWS account used for europa.eu.



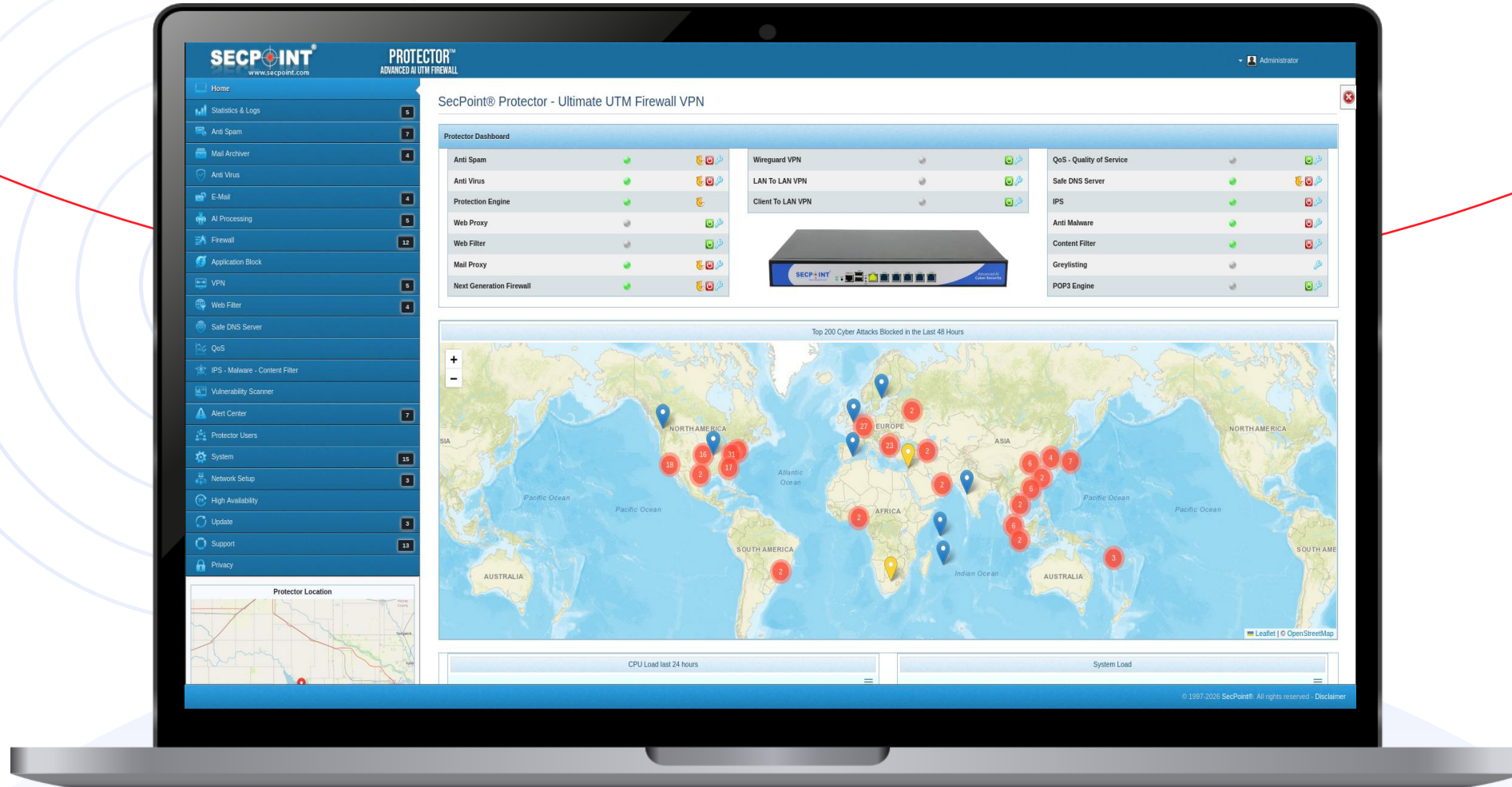
The case shows how trusted software and cloud environments can become attack paths.

The screenshot shows a document header with the title "Joint Cybersecurity Advisory" and "TLP: CLEAR". Below the header is a grid of logos from various national cybersecurity agencies, including the National Cyber Security Centre (UK), ASD (Australia), Estonian Foreign Intelligence Service, and others. The main title of the advisory is "Russian GRU Targeting Western Logistics Entities and Technology Companies". Below this is an "Executive Summary" section that begins with: "This joint cybersecurity advisory (CSA) highlights a Russian state-sponsored cyber campaign targeting Western logistics entities and technology companies. This includes those involved in the production, transport, and delivery of Russian products to..."

The screenshot shows the top of a CERT-EU website page. The header includes the CERT-EU logo and navigation links like "ABOUT US", "ANNUAL CONFERENCE", "BLOG", "PUBLICATIONS", "VACANCIES", "HALL OF FAME", "IICB", and "CONTACT US". The main heading of the article is "EUROPEAN COMMISSION CLOUD BREACH: A SUPPLY-CHAIN COMPROMISE". Below the heading is a breadcrumb trail: "HOME > BLOG > ARTICLE". The author information reads "By CERT-EU, on Thursday, April 02, 2026 03:16:00 PM CEST". The article starts with a "FOREWORD" section that says: "In the interest of transparency, and in full agreement with the European Commission, CERT-EU is publishing this blog post to inform the wider community about a cybersecurity incident affecting the European Commission's public website platform 'europa.eu' hosted on Amazon Web Services (AWS) cloud infrastructure."

SecPoint® Protector™ - On-prem cyber defence for operational resilience

- On-prem UTM firewall with VPN, IPS, anti-malware, web filtering
- Helps organisations detect, block, and manage cyber threats in real time





We are looking for

- Partnerships
- Pilot organisations / end users
- VARs / VADs / distributors
- European technology and project partners

Follow SecPoint on LinkedIn

<https://www.linkedin.com/company/secpoint>

Connect with Victor M. Christiansenn on LinkedIn

<https://www.linkedin.com/in/secpoint/>

