Case Study

SektorCERT disrupts critical infrastructure zero-day

THE CUSTOMER

Twenty-two Danish energy infrastructure companies were compromised in a coordinated zero-day cyber attack. The companies urgently needed to detect the attackers' hidden presence and respond immediately.

CHALLENGE

Attackers bypassed advanced defenses (firewalls and EDR) and moved quickly inside the network, rapidly adapting even as vulnerabilities were patched.

SOLUTION

Corelight sensors identified the attackers' activity through a single unusual network packet hidden among billions of others (only 1340 bytes, without a return ping), providing crucial evidence to pinpoint the intrusion.

RESULTS

Using Corelight, the attack was rapidly disrupted, vulnerabilities were patched, and critical national infrastructure remained secure.

Coordinated zero-day attacks disrupted by finding one critical packet

To learn more about the SektoCERT integration, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497