

CJX Aegis Incident Report

Company: BlueShield Enterprise

Title: Data Leak Despite Strong Perimeter

Summary:

A compliant enterprise missed enforcing proper data residency and endpoint patching for one shadow IT asset. A sophisticated actor used this to bypass defenses.

Triggered Alerts:

external_upload, geo_discrepancy, unusual_transfer_rate

Impact:

1.9GB of employee and vendor data was exfiltrated before being contained. CJX caught the anomaly, traced it to an unmonitored asset.

Action Plan:

CJX Agent blocked outgoing traffic, preserved forensic evidence, identified IP trail of attackers, initiated coordinated monitoring and delivered executive-level response report.

© 2025 CJX Secure Systems — www.cjxsecure.com