1

Breaches - facts and figures.

73%
of security leaders say they have experienced a security incident because assets in their IT infrastructure were not managed or simply unknown.

58%
of security leaders have not implemented processes for continuous monitoring. "However, this would be necessary to proactively mitigate and contain risks before they impact operations".

31%
of hospitality organizations worldwide have reported a data breach in their company's history.

89%
percent have been affected more than once in a year

365 364 363

90%
of severe findings are dominated by 3 main root causes:

- Configuration and Patch Management
- Identity and Access Management
- Application and Development Security

Cost of a breach.

CCPA: **US $7,500** per record lost

GDPR: UP TO **€20m** or UP TO **4%** of global turnover the preceding fiscal year, whichever is higher.

Average cost of a hospitality breach:

US $3.4m

Reputational impact can cause significant harm to the bottom line due to the highly competitive nature of the industry.

58%
of hotel guests have increased concerns about cyber safety after recent cyberattack news, influencing their trust and booking decisions

Sources:
www.csoonline.com
Cyber CX 2024 Hack Report
www.hotelmanagement.net
www.gitnux.org

Only those who know their attack surfaces can defend against them effectively.

2

What causes network vulnerabilities?

Hardware **EOL** end of life

Misconfigurations

Non-approved **SERVICE PROVIDERS**

Firmware/OS Updates **NOT** being implemented

3

How can I reduce my risk?

The only way to **reduce risk** is to be receiving **independently validated data** about your network that proves your commercial interests are being taken care of.

4

How do I do this?

Discovery
Provides continuous independent network visibility of your critical vendors and equipment by automating data collection for centralised reporting.

Compliance
Automates continuous, independent risk identification of your network vendors' configurations, measured against your standards. Creates prioritised remediation suggestions to enhance security programs, with daily monitoring alerts of weighted risk rankings.

Configuration
Ensures your networks are configured to your exact standards, reducing reliance on human labour and oversight, eliminating error, lowering your risk profile to drive network compliance.

Monitoring
Monitors physical equipment status, leveraging approved configuration to maximise network uptime and ensure continuous adherence to your standards. Automatic alerts of any non-approved network changes address potential security vulnerabilities before they escalate.

Central
A horizontally integrated control platform leveraging all Stella modules to provide independent network visibility, configuration management and risk identification.

stella
STANDARDISE, CENTRALISE, AUTOMATE

SOC 2 TYPE 2 VERIFIED BY ASSURANCELAB

Stella is a product of BRIGHTSTAR