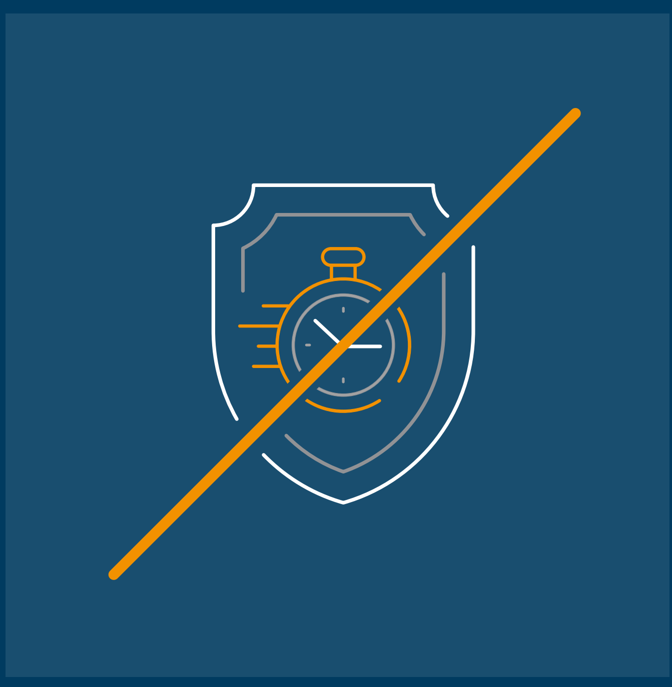
15 PRACTICAL TIPS

HOW TO BETTER PREPARE YOUR ENVIRONMENT FOR A SECURITY INCIDENT

As a security leader, you'll know that good cybersecurity incident response requires good foundations, open communication, and good teamwork. And the responsibility to make it happen is yours.

Three Common Pitfalls to Avoid

01.
Speed-Based Trust: No Security Vendor Can Address All Your Issues

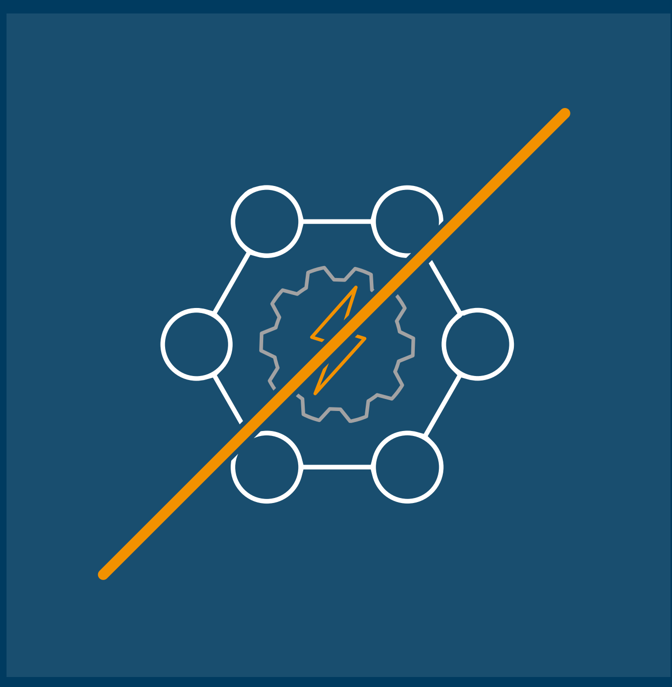


If you outsource 'trust', you end up with a Swiss Cheese Security Model . i.e., full of holes.

02.
Ignoring Cyber Hygiene

Absolute trust in your tech leads to a Cyber Titanic Mindset.

03.
Not Understanding Where to Harden vs Add New Solutions



Use MITRE ATT&CK to identify ways to harden your systems to reduce a likelihood of breaches.

Eight Actions to Take

01.
Understand Your Biases

They lead to blind spots. And blind spots make you vulnerable.

02.
Bridge Skills to Avoid Impact of Bias

Make the team solve a problem together. Create a purple team. Practice open communication and exchange.

03.
Develop KPIs with Value

Create actionable metrics e.g., # of common attack vectors removed or % decrease in attack surface.

04.
Shrink Your Digital Footprint

When data is no longer used, delete it. If you have to keep it, encrypt it and store the keys off the server.

05.
Augment Your Team

Bring in external partners. Think beyond security to system and cloud administration, IT operations etc.

06.
Explore Different Incident Response Paths

There's no one-size-fits-all. Always challenge recommendations from external security providers.

07.
Foster Open Dialogue During an Incident

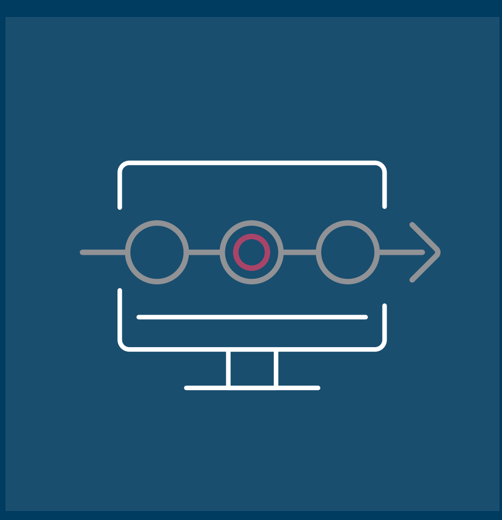
Create a culture of open dialogue. Ensure people have the right level of understanding to do their work.

08.
Show Your Appreciation

Incidents create stress. Offers of food, drink, or a place to stay near the incident are always appreciated.

Four Fixes to Reduce the Likelihood of a Breach

01.
Segmentation

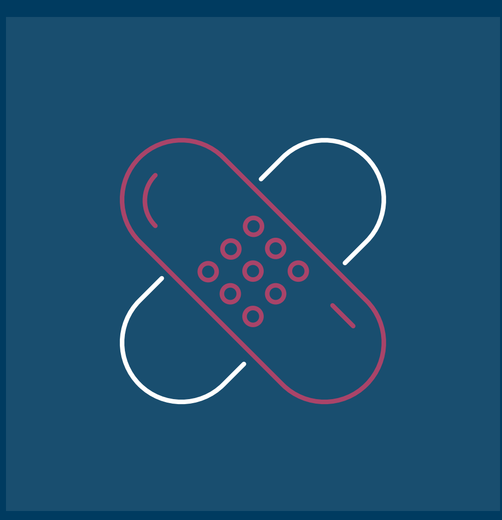


If your organization has a flat network, the attacker can move through it easily.

02.
Zero Trust

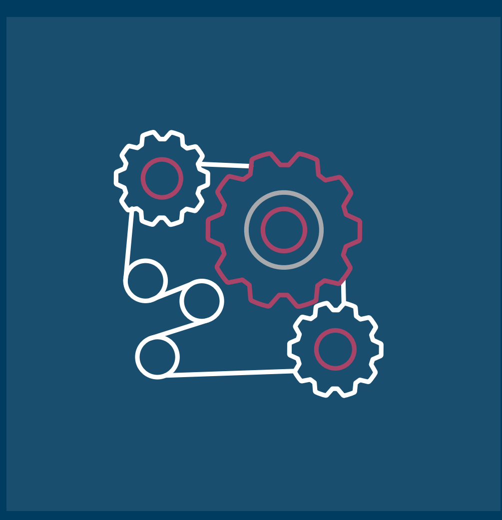
Apply a zero-trust approach to your organization

03.
Emergency Patch Plan



Ask yourself: Do you want an operational issue or a security issue? A system down or data leaked?

04.
Configuration



Get your systems properly configured. A tiny error can represent a wide-open door for an attacker.

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY