



TIPS FOR BOLSTERING INCIDENT RESPONSE CAPABILITIES

A comprehensive approach to incident response delivers more effective cyber risk mitigation.

1 EMBRACE A BROAD APPROACH

A sound approach to incident response should cover 7 steps, viewed through 3 different lenses:

01. DIGITAL EXPOSURE

02. GOVERNANCE

03. TECHNICAL



ASSESS



DESIGN



TRAIN



TEST



DETECT



RESPOND

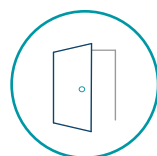


REMEDIATE

2 NEVER REST ON YOUR LAURELS

Do regular **self-assessments**, **tabletop exercises**, and **simulations** so your security program, and skills can keep pace.

3 ADOPT NEW RANSOMWARE BACKUP STRATEGIES



OUT WITH THE OLD:

Remove the 'easy, speedy' restore capabilities leveraged by ransomware attackers to encrypt or destroy backups.



IN WITH THE NEW:

Implement immutable backup solutions that even users with administrative credentials cannot delete.

4 RESPOND TO THE THREATS THAT MATTER

Work with an MDR provider who can tailor their service to **your unique threat model**, for accurate threat detection and response.

5 UNDERSTAND THE MOVE TO THE CLOUD PRESENTS NEW CHALLENGES

Using Kubernetes and microservice architectures may make you agile and efficient but unless you do it securely, will also expose you to greater risk.

Take a new approach to these 5 areas and train your staff to manage your new cloud environment, securely.



SECURE IDENTITIES



SECURE DATA



SECURE APPLICATIONS



BACKUP STRATEGIES



CONFIGURATION MANAGEMENT

There's no one-size-fits-all for incident response.
For comprehensive incident response that gives you the upper hand,

GET IN TOUCH

Get in touch today
info@kudelskisecurity.com | www.kudelskisecurity.com

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.

