A digital twin in the Cloud to strengthen your cyber resilience

Cyber-Resilience by Nuabee · https://nuabee.com/documents/cloud-digital-twin-cyber-resilience/

Nuabee: a cloud-based digital twin focused on cyber resilience

The Nuabee solution acts as a complete, isolated digital replica in the cloud, built around a Configuration Management Database (CMDB) that accurately describes your IT environments. As a Disaster Recovery Plan (DRP), it can be activated immediately or on demand, ensuring optimal business continuity in the event of a major incident or attack.

Hosted in a public cloud, this digital twin inherently benefits from advanced cloud features: rapid scalability, availability of ready-to-use OS images and configurations, automated security tools, proactive monitoring, enhanced encryption, and strict isolation of production environments.

Extended uses for proactive cyber resilience

Beyond its initial function of ensuring business continuity in the event of a major incident, the Nuabee digital twin paves the way for a proactive cyber risk management strategy:

- **Proactive vulnerability analysis**: carry out regular automated scanning campaigns (networks, systems, applications) and manual or automated intrusion tests to detect, analyze, and anticipate potential vulnerabilities before they are exploited.
- **Realistic simulation of attack scenarios:** test realistic attacks such as ransomware campaigns, targeted intrusions, and denial-of-service attacks to assess your actual resilience and your teams' ability to respond.
- **Security team training and coaching:** leverage this digital environment to train your teams to effectively detect, respond to, and remediate various cyberattack scenarios in a secure and controlled environment.

Intrinsic limitations of a cloud solution

Although powerful, this approach has certain inherent technical limitations related to the difference in architecture between your original IT environments (often "on-premises") and the cloud environment:

- **Attacks targeting the source hypervisor:** certain specific attacks targeting your local hypervisor (e.g., VMware) cannot be accurately reproduced in the digital twin's cloud environment.
- **Specific hardware attacks:** scenarios related to vulnerabilities that are directly dependent on the original physical hardware (firmware, BIOS, specific hardware controllers) cannot be simulated in the cloud.

Conclusion: a comprehensive and proactive approach

Malgré ces limites, le recours à une architecture jumelle Cloud telle que Nuabee constitue une étape majeure vers une cyber-résilience accrue. Cette démarche proactive vous permet de maîtriser vos risques cyber avec une efficacité renforcée, tout en assurant une reprise d’activité rapide en cas de crise majeure.