BLACKNOISE

Directive & Réglementation

NIS 2 DORA

UN TABLEAU DE >_controles POUR LES GOUVERNER TOUS

7 février 2025

European Union

Digital Operational Resilience Act (DORA)

Le règlement européen 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (DORA) entrera en application le 17 janvier 2025.

Network & information security V2 (NIS2)

Le Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972 et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

Concrètement, qu'est-ce qu'on attend des organisations ?

VOS NOUVELLES OBLIGATIONS

Renforcement de la cybersécurité

Mise en place de mesures de gestion des risques, de surveillance des incidents et d'une gouvernance claire en matière de cybersécurité.

Obligations de reporting

Déclaration rapide des incidents significatifs aux autorités compétentes et coopération accrue en cas de cyberattaques ou d'incidents opérationnels.

Résilience des infrastructures critiques

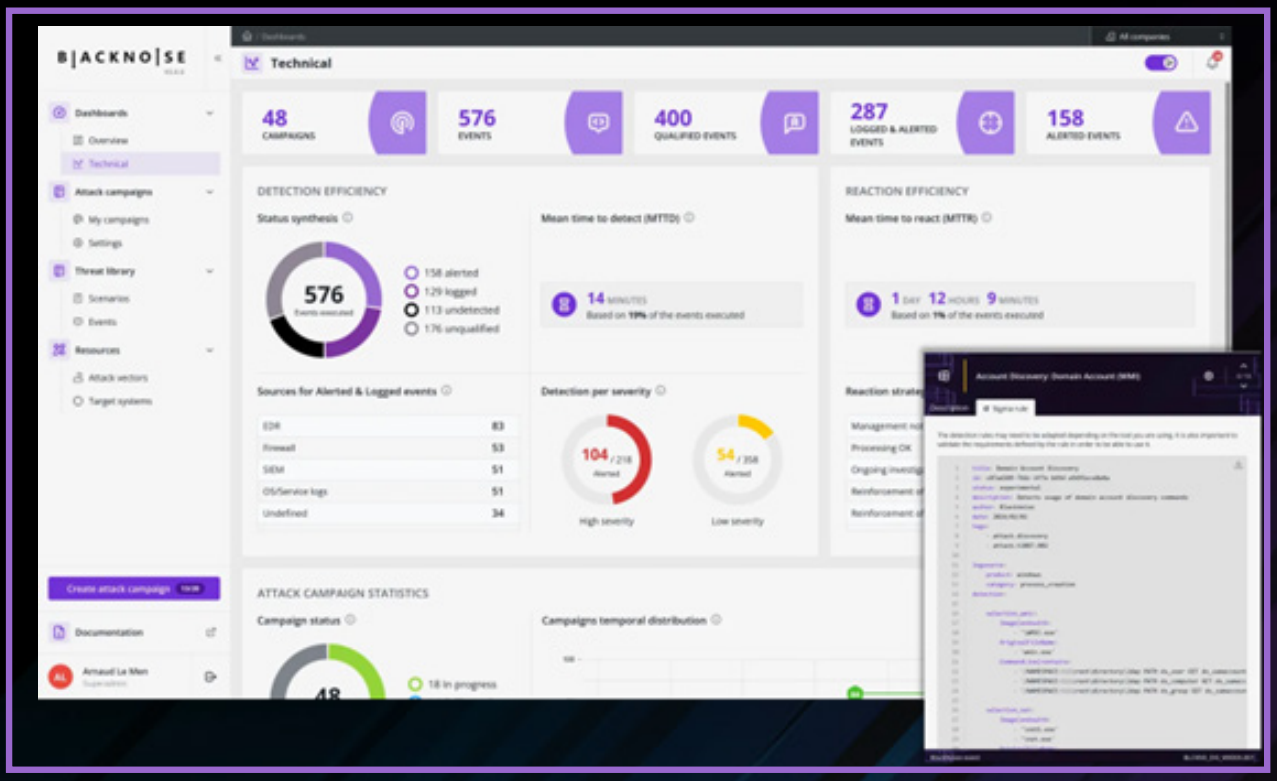
Mise en œuvre de plans de continuité et de reprise d'activité robustes pour assurer la résilience des services essentiels et financiers face aux menaces numériques. Digital Operational Resilience Act (DORA).

Pour démontrer vos conformités, testez les 11 points de contrôle opérationnels suivants

Points de contrôle	Priorité	Exemples de Preuves Techniques Attendues	Formats Possibles	Tactiques MITRE ATT&CK Associées	Articles DORA Associés	Articles NIS2 Associés
Démontrer la détection et réponse aux menaces (EDR/XDR/SIEM)	Haute	• Journaux SIEM • Rapports d'alertes et d'investigation SOC	Log, PDF, JSON, CSV	TA0001, TA0002, TA0003, TA0004, TA0005, TA0006, TA0007, TA0008, TA0009, TA0011	Articles 10-14, 25-27	Articles 21, 23
Tester les mécanismes de sécurité des endpoints et des serveurs	Haute	• Rapports de tests de Breach & Attack Simulation • Rapports de scans de vulnérabilité • Logs de protection EDR	PDF, Screenshot, JSON, CSV, Log	TA0002, TA0003, TA0005, TA0006, TA0007, TA0008	Articles 5-9, 25-27	Articles 20, 21
Tester la sécurité réseau et segmentation	Haute	• Rapports de tests de Breach & Attack Simulation • Tests de segmentation • Configurations firewall	Log, PCAP, PDF, JSON, CSV	TA0008, TA0009, TA0011, TA0010	Articles 5-9, 25-27, 28-30	Articles 20, 21, 23
Tester la sécurité des e-mails et des services de messagerie	Moyenne	• Rapports de simulation de phishing • Logs d'analyse des e-mails	Screenshot, PDF, CSV, Log	TA0001, TA0004, TA0006	Articles 10-14, 25-27	Articles 21, 23
Valider l'application de la politique de Gestion des identités et des accès (IAM/PAM)	Haute	• Journaux d'authentification • Tests de MFA • Rapports d'analyse de comptes privilégiés	Log, CSV, PDF, Screenshot	TA0006, TA0004, TA0003	Articles 5-9, 10-14, 25-27	Articles 21, 23
Tester la réaction face à des attaques avancées	Haute	• Rapports de tests de Breach & Attack Simulation • Journaux de mouvement latéral	PDF, Log, PCAP, Screenshot	TA0001, TA0003, TA0005, TA0007, TA0008, TA0011	Articles 25-27	Articles 21, 23
Découverte de vulnérabilités et suivi du patch management	Haute	• Rapports de CTEM • Rapports de scans de vulnérabilité	PDF, CSV, JSON, Screenshot	TA0002, TA0003, TA0005	Articles 5-9, 25-27	Articles 21, 23
Tester la résilience de l'organisation et les plans de réponse aux incidents (playbooks)	Haute	• Rapports de simulation d'incident • Journal d'exercices de crise • Playbooks opérationnels • Rapport de SOAR	PDF, Log, Screenshot	TA0007, TA0011, TA0009	Articles 10-14, 25-27	Articles 21, 23, 24
Valider des capacités de détection et de containment en mesurant le MTTD et MTTR moyen	Moyenne	• Rapports de tests de Breach & Attack Simulation • Rapports d'investigation SOC • Logs de containment	Log, JSON, PDF, Screenshot	TA0005, TA0006, TA0007	Articles 10-14, 25-27	Articles 21, 23, 24
Tester la détection de tentative d'exfiltration ou d'exfiltration avérée de données	Haute	• Rapports de tests de Breach & Attack Simulation • Journaux de transferts anormaux • Rapports de DLP et DLD • Logs de proxy	PCAP, Log, CSV, PDF	TA0010, TA0009	Articles 5-9, 25-27	Articles 21, 23
Évaluation des plans de continuité et de reprise après sinistre (BCP/DRP)	Moyenne	• Rapports de tests de PRA/PCA • Journaux de restauration	PDF, Log, CSV	TA0007, TA0011	Articles 5-9, 32	Articles 21, 23, 24

B|ACKNO|SE

BlackNoise exécute des scénarios de simulation d'attaque qui valident votre conformité Cyber en quelques minutes.



More info

contact@blacknoise.co

www.blacknoise.co