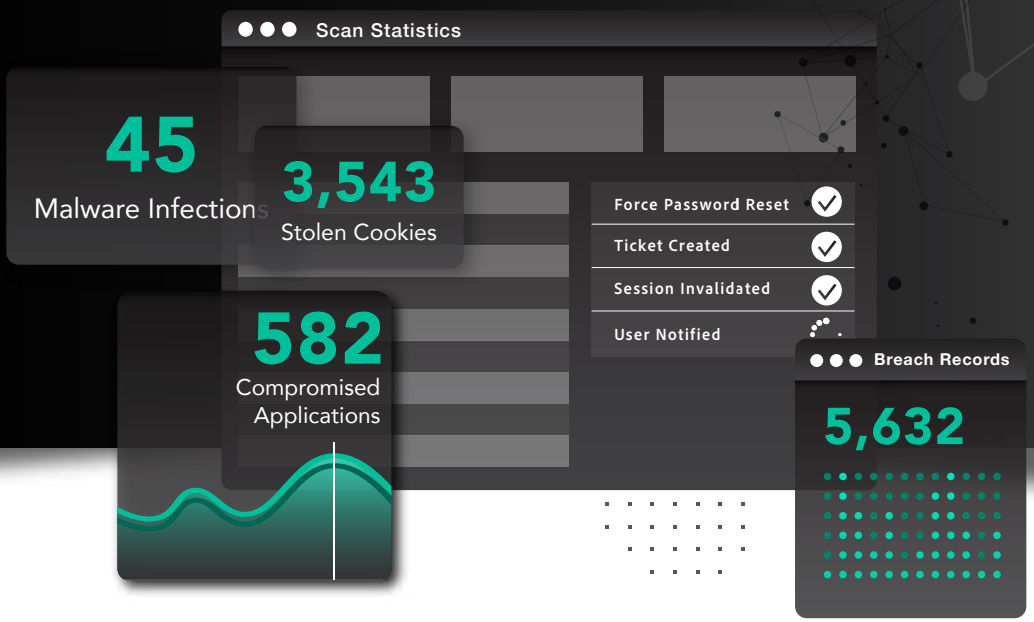
DATASHEET

SpyCloud

HOW SPYCLOUD HELPS WITH THE NIS2 DIRECTIVE



Compliance with NIS2 involves a multi-layered, strategic approach. With SpyCloud, it's possible to cover a range of NIS2 requirements and see value on day one.

SpyCloud's identity protection solutions, powered by Cybercrime Analytics, are a path forward to meeting the requirements of Paragraph 2, Article 21 of the NIS2 Directive – specifically requirements b, d, e, f, i and j.

For each of the remaining requirements – **a, c, g, h** – SpyCloud's alerts support the creation of appropriate policies and/or training.

ABOUT SPYCLOUD

SpyCloud provides solutions that actively protect organizations from targeted identity-centric attacks that rely on cybercrime data being traded on the darknet about the company, its employees, suppliers, and customers. SpyCloud continuously provides unparalleled access to relevant and actionable cybercrime data to clients through products and integrations that enable automated protection from account takeover, data breaches, business email compromise, session hijacking, and ransomware. SpyCloud also provides response tools and investigation capabilities to detect and respond to infostealer malware infections that have bypassed the organization's security controls.

Learn more at **spycloud.com**.

ARTICLE 21 SECTION	NIS2 REQUIRED RISK MANAGEMENT MEASURES	SPYCLOUD PROVIDES CRITICAL SUPPORT TO ENTITIES BY:
2(b)	incident handling	▸ Alerting on employee and supplier identities exposed by breaches and credential-stealing malware to drive **post-infection remediation** ▸ Identifying the root cause of an incident linked to employee exposures – determining how an incident started and why an employee was specifically targeted ▸ Providing **investigations** capabilities to empower thorough analysis of cybercrime and darknet data
2(d)	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	▸ Providing visibility into business applications accessed by third-party vendors and contractors with dark web-exposed credentials or cookies ▸ Detecting application credentials from suppliers using malware-infected personal or undermanaged devices ▸ Monitoring third-party domains of your supply chain vendors to identify threat exposure from individuals with privileged access
2(e)	security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure	▸ Identifying the identity-centric vulnerabilities to allow for detection, disclosure and **automated remediation** ▸ Alerting on malware infections, on both managed and unmanaged devices, that represent an ongoing vulnerability to the entity
2(f)	policies and procedures to assess the effectiveness of cybersecurity risk-management measures	▸ Continuous monitoring of employee exposure risks related to their identity security posture ▸ Offering a view into active malware infections that have circumvented implemented security controls, so policies and implementations may be reconsidered
2(i)	human resources security, access control policies and asset management	▸ Offering a device-agnostic approach with continuous monitoring of employee identities to detect exposed authentication data for critical business applications ▸ Delivering evidence of **infostealer malware-infected devices**, including non-compliant devices used for work purposes
2(j)	the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	▸ Monitoring of the entity's identities and authentication continuously and alerting when they are exposed to cybercriminals to properly protect the integrity of MFA and Identity Access Control implementations ▸ Securing MFA-protected web sessions from unauthorized access via **session hijacking**, detecting compromised cookies/tokens for invalidation/reauthentication