SCION ASSOCIATION

FACT SHEET

HOW SCION ENABLES COMPLIANCE WITH EU LEGISLATION: NIS2, DORA

In an era where cyber threats are growing in sophistication and scale, the European Union has taken significant steps to increase cyber resilience with the introduction of key legislation such as NIS2 and DORA. These regulations aim to protect critical infrastructures, ensure data privacy, and mitigate the risks of cyberattacks on vital sectors.

NIS2

The NIS2 Directive introduces principles for cybersecurity, resilience, and reporting obligations, especially for operators of essential critical systems (e.g., energy, finance, healthcare, defense).

DORA

DORA mandates financial entities to strengthen their digital resilience against cyberattacks and other IT disruptions. It includes risk management, reporting, testing, and third-party oversight.

LIMITATIONS OF TODAY'S SOLUTIONS IN COMPLYING WITH NIS2 & DORA

INTERNET

Critical infrastructures today rely heavily on the Internet for their digital communications. Yet the Internet's vast attack surface, with countless entry points for malicious actors, makes it easier than ever to infiltrate networks, steal data, or disrupt essential services. As a result, achieving the cyber-resilience standards set by DORA and NIS2 becomes extremely challenging.

PRIVATE LINES

To overcome the limitations of Internet-based connectivity, many critical infrastructures rely on costly and inflexible private lines often from a single connectivity provider. But this approach introduces its own risks, creating single points of failure in the event of cyberattacks or outages at the ISP level, ultimately failing to meet DORA and NIS2's mandate for cyber resilience.

info@scion.org

www.scion.org

SCION ASSOCIATION

HOW SCION MAKES CRITICAL SECTORS MORE SECURE & RESILIENT IN LINE WITH NIS2 & DORA STANDARDS

SCION enhances the resilience and security of critical sectors by addressing many of the limitations of both Internet-based connectivity and private lines when complying with DORA and NIS2.

ABOUT SCION

SCION is a path-aware Internet architecture that introduces the concept of trust networks (ISD), which are intentional groupings of entities under the same environment. Data can only be exchanged within an ISD or with explicitly authorized external ISDs. Within the ISD, users maintain full control over the paths through which their data travels.

1

SCION trust networks can choose to be private, limited access, or publicly accessible, which reduces the attack surface from the rest of the Internet. This minimizes the risk of route hijacking, leaks, MitM, and DDoS attacks.

✓ ROBUST OPERATIONAL CONTINUITY AND DATA SECURITY IN LINE WITH NIS2 & DORA

2

SCION's path control feature ensures that data flows through pre-determined secure paths, reducing the risk of interception and future decryption, the so-called "harvest now, decrypt later" attacks by quantum computing.

✓ EXTRA LAYER OF SECURITY, ALIGNING WITH THE EU'S FOCUS ON LONG-TERM CYBER RESILIENCE

3

SCION trust domains can be provisioned by multiple ISPs providing redundant connectivity. SCION's multi-pathing also allows for fast failover.

✓ REDUNDANCY MEANS RESILIENCE IN LINE WITH DORA & NIS2 STANDARDS

4

SCION allows organizations to select paths for data transmission based on criteria like geofencing.

✓ COMPLIANCE WITH DATA PROTECTION REGULATIONS

5

SCION's trust model enables organisations to build networks where they can explicitly choose whom to include and whom to exclude, including third-party providers.

✓ CONTROL OVER THE FULL SUPPLY CHAIN REQUIRED BY NIS2 AND DORA FOR CYBER RESILIENCE

SCION OPERATIONALIZES KEY NIS2 AND DORA PRINCIPLES: RESILIENCE, SECURITY, AND TRUST

Where NIS2 and DORA impose compliance obligations, SCION is the technical enabler that allows these to be implemented and auditable.

info@scion.org

www.scion.org