RIEDEL Enterprise Defense

Choose R.E.D. to protect

PRODUCT SHEET

RIEDEL

About RIEDEL Enterprise Defense

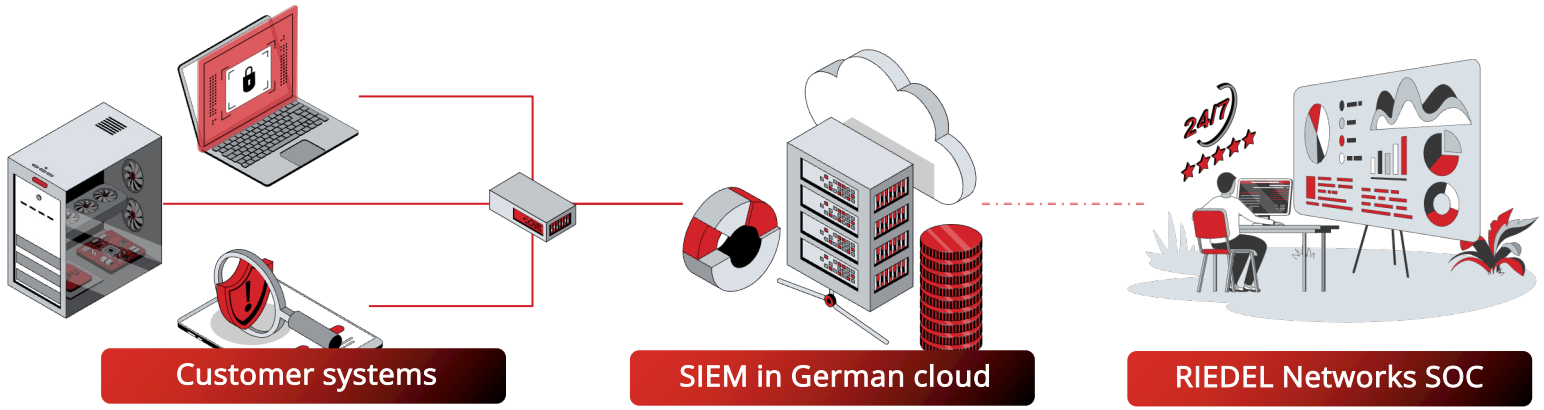
Get your company ready for the NIS2 directive

Overview of the solution

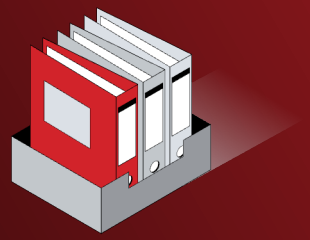
With **R**IEDEL **E**nterprise **D**efense (R.E.D.), you and your company are future-proof in the area of cyber security. R.E.D. brings together a variety of technologies and systems required for the successful **detection, defense and prevention of cyber attacks**. The **24/7 managed service** covers all aspects of vulnerability and threat analysis, active protection against targeted attack attempts and following preventive measures. All of this is proactively monitored via the Security Operations Center (SOC) and provided to the customer in a comprehensible manner.

About the NIS2 directive

The NIS2 directive is EU-wide legislation on network and information security. The aim is to strengthen the cyber security of companies and ensure a uniformly high level of security in the EU. Each company is responsible for assessing whether it is affected by the Network and Information Security Directive (NIS2 for short). The type of business activity in the EU is the main deciding factor. A total of 18 sectors are affected by the NIS2 directive.



Logs from all devices are aggregated and monitored 24/7 by the RIEDEL Networks Security Operation Center (SOC). Vulnerabilities are analyzed across all devices and all processes in the customer system are proactively recorded.



18 October 2024

Deadline for implementation of the NIS2 Directive.

RIEDEL

NIS2-RL as a security driver

Fines in the millions could be imposed - in addition to the potential costs of downtime

Affected sectors

Companies in the following sectors are covered by the new NIS2 directive and are legally obliged to implement specific cyber security precautions:

Energy, traffic / transportation, banking, financial market infrastructures, healthcare, digital infrastructure, waste management, production / manufacture / trade of chemical substances and production / processing / sales of food. In addition, drinking water, sewage, management of ICT services (B2B), public administration, space, postal and courier services, manufacturing/production of goods, providers of digital services and research.

Other companies in focus

In addition, companies that provide essential services or products in connection with the sectors affected by NIS2 are now also newly affected. The threshold in terms of company size is a number of employees of more than 50 or if the annual turnover reaches or exceeds 10 million euros. Responsibility for implementing NIS2 lies with the management and executive board, who are also personally liable in the event of violations.

EU-wide legislation on network and information security

Financial risk due to fines in the millions and accountability

Ignorance has no defence - obligation to report damage within 24 hours

Responsibility for implementation lies with management & executive board with personal liability

RIEDEL

Reporting obligations and requirements

Systems, IT departments and employees - in the event of damage, a quick reaction is required

Within 24 hours → First notification (early warning) to the responsible authorities, stating whether the security incident is due to illegal or malicious actions.

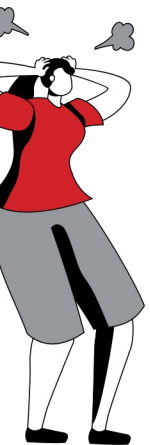
Within 72 hours → A report with the Indicators of Compromise (IOC) must be handed over to the authorities, for which dedicated security expertise is required.

After one month, a final report is due, which must contain at least a detailed description of the security incident, its severity and impact, as well as information on the type of threat and the measures taken.

ALARM! **ALARM!**

A security incident is an event that affects information security. The incident jeopardizes the confidentiality, availability or integrity of data, IT applications, IT systems or IT services.

A breach of just one of the protection goals of confidentiality, availability or integrity is already a security incident. Security incidents create risks for companies, organizations and individuals. Major damage can be the result.



Inadequately protected IT systems

External attackers

Software errors

Ransomware

(D)DoS

Mistakes at work

Careless employees

etc.

Cross-Site-Scripting

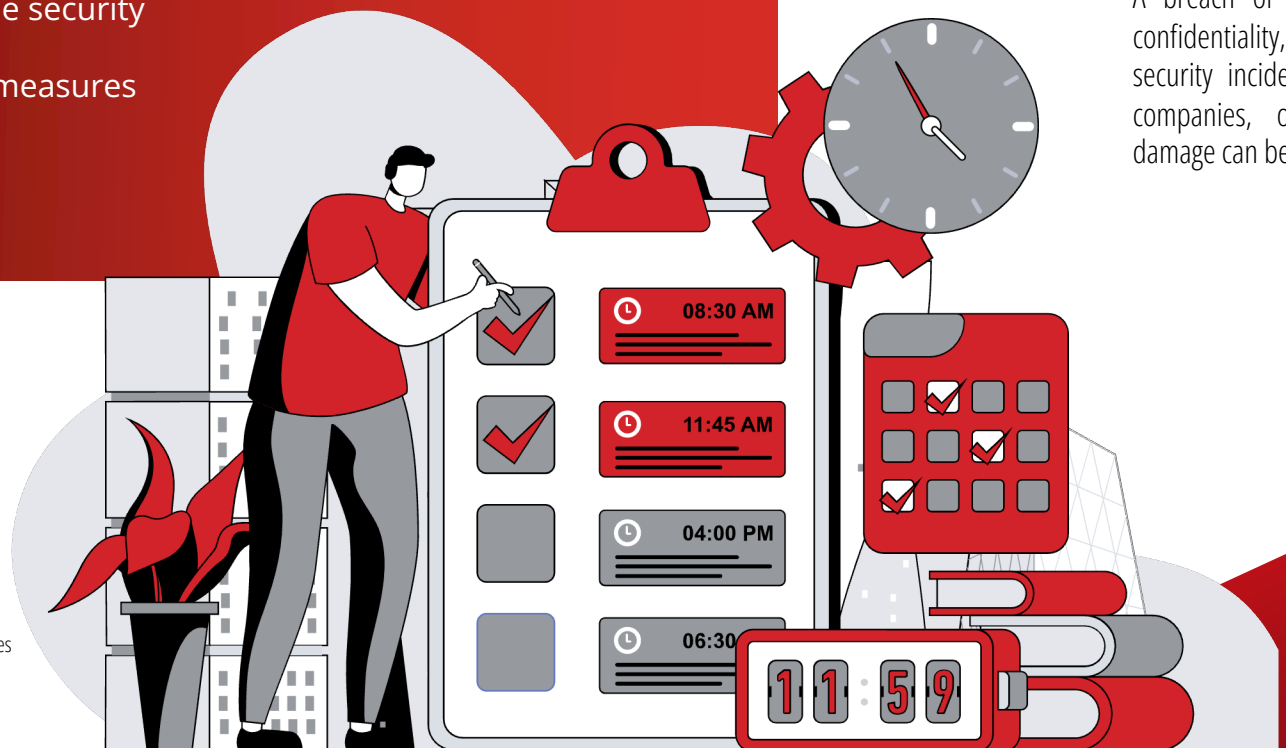
Phishing

Tail-gating, USB sticks ...

Postponed updates

Security gaps

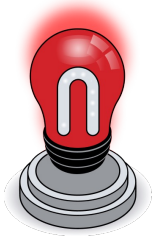
Violations of guidelines



RIEDEL

RIEDEL Enterprise Defense

Safe on the way - everything from a single source



Attack detected!

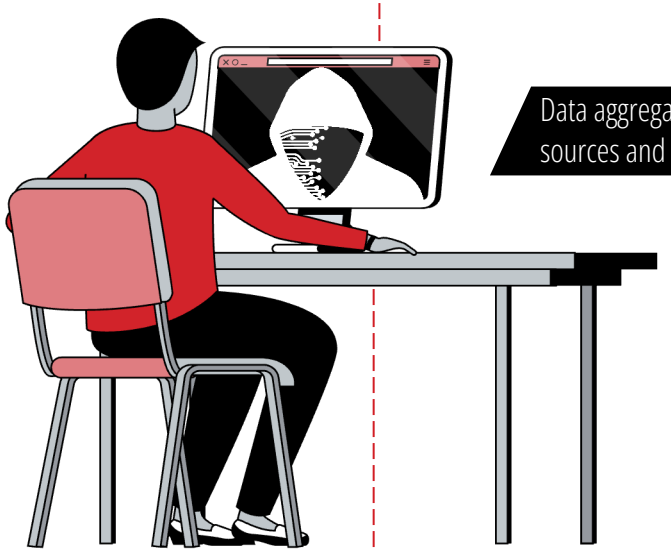
Choose R.E.D. to Protect!

RIEDEL Enterprise Defense is our proven **managed** service approach in the security sector. Customers receive a security setup tailored to their needs, which essentially includes the following areas:

- ✓ (D)DoS Protection
- ✓ Next Generation Firewalls
- ✓ SD-WAN
- ✓ SASE
- ✓ SIEM & SOC
- ✓ XDR (EDR+NDR)
- ✓ SOAR

With pleasure we explain to you in detail what is behind the individual areas and how it all works.
Just give us a call!

All components are managed by our own security team from a single source (24/7) and can be used separately or in combination with existing network solutions from RIEDEL Networks.



Data aggregation and analysis from internal and external sources and tools for threat detection and defense

Allianz für Cyber-Sicherheit

Our security suite contains a lot of information, tools and functions that are also used by attackers (crackers, colloquially known as hackers). In the cybersecurity, the group of attackers is known as the RED team. Our solution includes common functions and processes used by classic defense teams (BLUE), but is enhanced by explicit insights from existing attack modules, thus offering more comprehensive protection.

RIEDEL

RIEDEL Enterprise Defense

Governance, risk & compliance – where the fun stops

Classification sections

RIEDEL Enterprise Defense has the following standard classification sections and subsections that you can access to review the information generated by the events.

Cybersecurity - find the optimal solution!
Governance, risk, compliance

Security Information Management

• Security Events • Integrity monitoring • Office 365 • Amazon AWS • Google Cloud Platform • Github

Threat Detection and Response

• Vulnerabilities • Mitre ATT&CK • VirusTotal • Docker listener

Auditing and Policy monitoring

• Policy monitoring • System auditing • Security configuration assessment • OpenSCAP • CIS-CAT

Regulatory Compliance

• PCI DSS • NIST 800-53 • TSC • GDPR • HIPAA

RIEDEL

Why RIEDEL Networks?

Choose R.E.D. to protect

Detection rate
≥ 99,00%
to MITRE ATT&CK

24x7 Operations

We ensure continuous global business operations with experienced technicians in the NOC & SOC who are available around the clock.

All data & systems are hosted in
Germany

Unlimited scalable

Modular and resilient architecture with managed Kubernetes and Elastic, as well as automatic scaling.

Availability
99,999% SLA
For system and backbone

Fair pricing

No incalculable calculation, not according to volume (per Mbps) and not by events per second (EPS).

Allianz für Cyber-Sicherheit

We are
ACS - Member
of the BSI

Preventive support

Prevent all dangers. Anticipate problems, minimize disruptions and improve your operational performance.

Every 10 sec
in real time
the endpoint reports to the SIEM

RIEDEL

Get in Touch

October 18th is coming sooner than you think!

RIEDEL Networks GmbH & Co. KG

RN-sales@riedel.net

+49 (0) 6033 9169 100

Not convinced? We would be pleased to send you our "Cyber Security lazy excuses quartet".

Then we'll talk again.

Supervisory authority: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Tulpenfeld 4, 53113 Bonn, Reg-Nr. 12/158

RIEDEL