LogRhythm®

The Security Intelligence Company

NISD
Networking and Information Systems (NIS) Directive

Table of contents

The EU's Network and Information Systems (NIS) Directive entered into force in August 2016 with the aim of increasing the resilience of cybersecurity defences across Europe. The clock is now ticking with EU member states having until 9th May 2018 to transpose the NIS Directive into their own national laws.

The NIS Directive provides legal measures that will boost the overall level of cybersecurity in the EU, particularly for industries and organisations that provide services essential to everyday life and the security of a nation. These organisations will be required to report incidents to a regulatory authority and will face fines of up to £17m if breaches are down to failures in cybersecurity defences.

Specifically, the NIS Directive aims to safeguard the supply of essential services that rely heavily on IT, such as energy, transportation, water, banking, financial market infrastructures, healthcare, and digital infrastructure. Organisations in those sectors that are identified as operators of essential services (OESs) or digital service providers (DSPs) will be required to take appropriate security measures and comply with the incident notification requirements as set out by the NIS Directive.

Cybersecurity incidents affecting these suppliers of essential everyday services have the potential to cause significant damage to the economy, spread to other member states, or even cause loss of life. And the threat to OESs is increasing, with a wave of malware in 2017 specifically written to target operational technology (OT), supervisory control and data acquisition (SCADA), and industrial control systems (ICS). Take the Triton malware in December 2017, for example, which was designed to target and manipulate industrial safety systems by infecting a Windows computer that connects to an ICS.[1]

The NIS Directive will apply to all OESs and DSPs from 9th May 2018, but member states will then have a further six months until 9th November 2018 to formally identify all OESs and DSPs in their country that are essential to the supply of electricity, water, digital infrastructure, healthcare, and transport.

In light of these new security and incident reporting requirements under the NIS Directive, businesses are advised to do a full risk assessment of their cyber resiliency, particularly their ability to detect and respond to cyberthreats.

The NIS Directive and the GDPR

The NIS Directive has been designed to work alongside data protection legislation. It will be governed in line with the EU General Data Protection Regulation (GDPR), which has the power to impose significant penalties and fines on organisations that fail to comply.

The key distinction between the NIS Directive and the GDPR – apart from the organisations they apply to – is in the impact of incidents. The NIS Directive requires notification if an incident has a substantial impact on the provision of the operator's essential services. Under the GDPR, companies are required to report an incident if the risk is to the personal data of EU citizens.

It is up to individual EU member states to set their own rules on penalties under the NIS Directive and take all measures to ensure they are implemented.

The UK government has stated in a consultation paper on the implementation of the NIS Directive that the penalty regime should be similar to the GDPR because of the theoretically high impact of the loss of an essential service to human life or the economy.

The UK government published its response to the NIS Directive consultation in January 2018. It had initially proposed two separate bands of fines up to a maximum of the greater of £20m or four per cent of global turnover, similar to the GDPR. However, the government has now simplified this to one single band covering all contraventions under the NIS Directive, removing the percentage of global turnover element and reducing the maximum fine to £17m. It also said this maximum fine should be reserved for only the most severe cases.[2]

However, that does not remove the potential risk of "double jeopardy" and a company being subject to different penalties for the same incident under the NIS Directive and the GDPR. For example, the European Union Agency for Network and Information Security (ENISA) says that in some cases digital service providers (DSPs) that fall under the NIS Directive may also have to report the same incident to the authorities responsible for the GDPR.[3]

[1] Triton: hackers take out safety systems in 'watershed' attack on energy plant https://www.theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant

[2] Department for Digital, culture, Media & Sport: Security of Network and Information Systems Public Consultation (August 2017). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf

[3] Department for Digital, culture, Media & Sport: Security of Network and Information Systems Response to Public Consultation (January 2018) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf

What is the NIS Directive?

The first myth to put to bed is that Brexit might lead to the NIS Directive not applying to the UK. In this respect, the UK government has made it clear in the consultation paper that it intends to retain the strict reporting and penalty regimes of the GDPR and the NIS Directive following the UK's withdrawal from the EU.

In a statement of intent in August 2017 proposing a new Data Protection Bill, the UK government confirmed its intention to retain the GDPR, or an equivalent-level data protection regime, following the formal withdrawal from the EU after the Brexit transition period.

It is no surprise, therefore, that the UK government also confirmed in the NIS Directive consultation response in January 2018 that it intends for the NIS Directive's policy provisions to continue to apply in the UK following the withdrawal from the EU.

The NIS Directive aims to boost the overall level of network and information system security in the EU. Under the directive, member states are required to:

- Put in place a national framework to support and promote the security of network and information systems, consisting of a National Cybersecurity Strategy, a Computer Security Incident Response Team (CSIRT), a Single Point of Contact (SPOC) and a national NIS competent authority (or authorities).
- Set up a Cooperation Group to support and facilitate strategic collaboration and the exchange of information among member states. Member states will also need to participate in a CSIRT Network to promote swift and effective operational cooperation on specific network and information system security incidents, as well as the sharing of information about risks.
- Ensure the framework for the security of network and information systems is applied effectively across sectors that are vital for the economy and society and that rely heavily on information networks. These include the energy, transport, water, healthcare and digital infrastructure sectors. Businesses in these sectors that are identified by member states as OESs will have to take appropriate and proportionate security measures to manage risks to their network and information systems and to notify serious incidents to the relevant authority. Key DSPs, such as search engines, cloud computing services, and online marketplaces, will also have to comply with the security and incident notification requirements established under the directive.

Some sectors, such as finance or civil nuclear, are exempt from certain aspects of the NIS Directive where there are provisions within their existing regulations, which are at least equivalent to those the NIS Directive specifies.

The UK's National Cyber Security Centre (NCSC) is providing technical support and guidance for the implementation of the NIS Directive. It has developed 14 principles for securing essential services and to guide cybersecurity decision-making.[4] The NIS cybersecurity principles define a set of top-level outcomes that describe good cybersecurity for OESs. These security principles are divided up across four objectives:

Objective A: Managing security risk

Appropriate organisational structures, policies and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.

- A.1 Governance
- A.2 Risk management
- A.3 Asset management
- A.4 Supply chain

Objective B: Protecting against cyberattack

Proportionate security measures in place to protect essential services and systems from cyberattack

- B.1 Service protection policies and processes
- B.2 Identity and access control
- B.3 Data security
- B.4 System security
- B.5 Resilient networks and systems
- B.6 Staff awareness and training

[4] NIS Directive: Top-level objectives https://www.ncsc.gov.uk/guidance/nis-directive-top-level-objectives

Objective C: Detecting cybersecurity events

Capabilities to ensure security defences remain effective and to detect cybersecurity events affecting, or with the potential to affect, essential services.

- C.1 Security monitoring
- C.2 Proactive security event discovery (anomaly detection)

Objective D: Minimising the impact of cybersecurity incidents

Capabilities to minimise the impacts of a cybersecurity incident on the delivery of essential services including the restoration of those services where necessary.

- D.1 Response and recovery planning
- D.2 Lessons learned (improvements)

A Cyber Assessment Framework (CAF) is due to be published by the NCSC by the end of April 2018.[5] This will provide guidance for assessing organisations falling under the NIS Directive against the 14 security principles as well as acceptable levels of security required under the directive.

Explanation on NISD Listings

Designated Competent Authorities (CAs) will be responsible for identifying the specific OESs and DSPs for their sector by November 2018. These CAs include the Secretaries of State for the relevant government departments and bodies such as the Drinking Water Inspectorate, Ofgem, the Health and Safety Executive, Ofcom, NHS Digital, the Civil Aviation Authority and the Information Commissioner's Office.

The essential services that will fall under the NIS Directive are listed in the UK government's consultation response paper on the directive. These essential services sectors include drinking water supply and distribution, electricity supply, transmission and distribution, oil production (upstream and downstream), gas supply, storage, transmission and distribution, healthcare, and air, maritime, rail, and road transport. The digital infrastructure sectors covered include top-level domain name registries, DNS service providers, and internet exchange point (IXP) operators.

[5] Incident notification for DSPs in the context of the NIS Directive https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/at_download/fullReport

The 14 NIS Directive security principles.[6]

Title	**A.1 Governance**
Principle	There are appropriate management policies and processes in place to govern the organisation's approach to the security of network and information systems.
Description	Effective security of network and information systems must be driven by organisational management and corresponding policies and practices. There should be clear governance structures in place with well-defined lines of responsibility and accountability for the security of network and information systems. There should be an individual(s) who holds overall responsibility and is accountable for security. This individual is empowered and accountable for decisions regarding how services are protected. For small organisations, the governance structure can be very simple.
How LogRhythm supports compliance	LogRhythm NextGen SIEM Platform provides visibility and security alerting against both security-specific scenarios, and compliance. Role-based access control (RBAC) allows defined users of the system to have access to differing views on the information coming into the platform.

Title	**A.2 Risk Management**
Principle	The organisation takes appropriate steps to identify, assess, and understand security risks to the network and information systems supporting the delivery of essential services. This includes an overall organisational approach to risk management.
Description	There is no single blueprint for cybersecurity; and therefore, organisations need to take steps to determine security risks that could affect the delivery of essential services and take measures to appropriately manage those risks. Threats can come from many sources, in and outside the organisation. A good understanding of the threat landscape and the vulnerabilities that may be exploited is essential to effectively identify and manage risks. Such information may come from sources including NCSC, information exchanges relevant to the organisation's sector, and reputable government, commercial, and open sources, all of which can inform the organisation's own risk assessment process. Organisations may contribute to the understanding of threats and vulnerabilities in their sector by participating in relevant information exchanges and liaising with authorities as appropriate. There should be a systematic process in place to ensure that identified risks are managed and the organisation has confidence mitigations are working effectively. Confidence can be gained through, for example, product assurance, monitoring, vulnerability testing, auditing, and supply chain security.
How LogRhythm supports compliance	In addition to the point-source security technologies an organisation should have in place – including strong firewalling, network segmentation, endpoint security, user account control and monitoring, and vulnerability assessment – overall visibility and correlation is paramount. Understanding a threat vector across multiple systems and vendors, while alerting and providing the ability to automatically remediate and mitigate a threat, drastically reduces the time to detect and time to respond.

Title	**A.3 Asset Management**
Principle	Everything that is required to deliver, maintain, or support networks for essential services is determined and understood. This includes data, people, and systems, as well as any supporting infrastructure (such as power or cooling).
Description	In order to manage security risks to the network and information systems of essential services, organisations require a clear understanding of service dependencies. This might include physical assets, software, data, essential staff, and utilities. These should all be clearly identified and recorded so that it is possible to understand what things are important to the delivery of the essential service and why.
How LogRhythm supports compliance	The LogRhythm NextGen SIEM Platform maintains an entity structure reflecting the host, network ranges, and user identities within an environment. Data seen from new systems/systems outside of this list can specifically be alerted against. This includes SCADA/ICS-specific equipment and protocols.

[6] The 14 NIS Directive security principles https://www.ncsc.gov.uk/index/guidance?f%5B0%5D=field_topics%253Aname%3ANIS%20Directive

Title	A.4 Supply Chain
Principle	The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third-party services are used.
Description	If an organisation relies on third parties (such as outsourced or cloud-based technology services), it remains accountable for the protection of any essential service. This means that there should be confidence that all relevant security requirements are met regardless of whether the organisation or a third-party delivers the service. For many organisations, it will make good sense to use third-party technology services. Where these are used, it is important that contractual agreements provide provisions for the protection of things upon which the essential service depends.
How LogRhythm supports compliance	LogRhythm can take in data from cloud services, and monitor connections out to outsourcing/third-party organisations that interact with the monitored environment. Unauthorised access to the environment, or unusual activity, to/from the external sources, can be monitored for on a geolocation or time basis.

Title	B.1 Service protection policies and processes
Principle	The organisation defines, implements, communicates, and enforces appropriate policies and processes that direct the overall approach to securing systems and data that support delivery of essential services.
Description	The organisation's approach to securing network and information systems that support essential services should be defined in a set of comprehensive security policies with associated processes. It is essential that these policies and processes are more than just a paper exercise and steps must be taken to ensure that the policies and processes are well described, communicated, and effectively implemented. Policies and processes should be written with the intended recipient community in mind. For example, the message or direction communicated to IT staff will be different from that communicated to senior managers. There should be mechanisms in place to validate the implementation and effectiveness of policies and processes where these are relied upon for the security of the essential service. Such mechanisms should also support an organisational ability to enforce compliance with policies and processes when necessary. To be effective, service protection policies and processes need to be realistic, i.e. based on a clear understanding of the way people act and make decisions in the workplace, particularly in relation to security. If they are developed without this understanding, there is a significant risk that service protection policies and processes will be routinely circumvented, as people use work-arounds and short cuts to achieve their work objectives.
How LogRhythm supports compliance	The LogRhythm NextGen SIEM Platform can alert against a deviation from standard policies, with variance on alert severity and potential remediate action based on the risk profile, entities impacted, users involved, and systems accessed. LogRhythm's SmartResponse™ technology can alert end users if they deviate from policy and procedure. It can also perform fully automated or analyst-validated actions on associated technologies to prevent further access or potential damage. For example, a user account could be disabled when attempted file access or encryption is observed.

Title	B.2 Identity and access control
Principle	The organisation understands, documents, and controls access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services should be appropriately verified, authenticated, and authorised.
Description	Users, devices, and systems should be appropriately authenticated and authorised before access to data or services is granted. For highly privileged access it might be appropriate to include approaches such as two-factor or hardware authentication. Unauthorised individuals should be prevented from accessing data or services at all points within the system. This includes system users without the appropriate permissions, unauthorised individuals attempting to interact with any online service presentation, or individuals with unauthorised access to user devices (e.g., if a user device were lost or stolen).
How LogRhythm supports compliance	User-auditing and User and Entity Behaviour Analytics (UEBA) are core aspects of the LogRhythm NextGen SIEM Platform. With CloudAI and standalone UEBA functionality available, advanced trending/alerting against user activity is also possible, with automatic baselining and the application of supervised and unsupervised machine-learning techniques.

Title	B.3 Data Security
Principle	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause disruption to essential services. Such protection extends to the means by which authorised users, devices, and systems access critical data necessary for the delivery of essential services. It also covers information that would assist an attacker, such as design details of networks and information systems.
Description	The protection in place for data that supports the delivery of essential services must be matched to the risks associated with that data. As a minimum, unauthorised access to sensitive information should be prevented (protecting data confidentiality). This may mean, for example, protecting data stored on mobile devices that could be lost or stolen. Data protection may also need to include measures such as the sanitisation of data storage devices and/or media before sending for maintenance or disposal. Protect data in accordance with the risks to essential services posed by compromises of data integrity and/or availability. In addition to effective data access control measures, other relevant security measures might include maintaining up-to-date offline backup copies of data, combined with the ability to detect data integrity failures where necessary. Software and/or hardware used to access critical data may also require protection. It is important to ensure that data supporting the delivery of essential services is protected in transit. This could be by physically protecting the network infrastructure, or using cryptographic means to ensure data is not inappropriately viewed or interfered with. Duplicating network infrastructure to prevent data flows being easily blocked provides data availability. Some types of information managed by an OES would, if acquired by an attacker, significantly assist in the planning and execution of a disruptive attack. Such information could be, for example, detailed network and system designs, security measures, or certain staff details. These should be identified and appropriately protected.
How LogRhythm supports compliance	This capability can be supported with the included File Integrity Monitoring functionality available using LogRhythm System Monitor Agents. In addition to the integration with existing file integrity monitoring and data policies services, data access and movement can be tightly monitored and controlled.

Title	B.4 System security
Principle	Network and information systems and technology critical for the delivery of essential services are protected from cyberattack. An organisational understanding of risk to essential services informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.
Description	There is a range of protective security measures that an organisation can use to minimise the opportunities for an attacker to compromise the security of networks and information systems supporting the delivery of essential services. Not all such measures will necessarily be applicable in all circumstances – each organisation should determine and implement the protective security measures that are most effective in limiting those opportunities for attackers associated with the greatest risks to essential services. Opportunities for attackers to compromise networks and information systems, also known as vulnerabilities, arise through flaws, features, and user error. Organisations should ensure that all three types of vulnerability are considered when selecting and implementing protective security measures. Organisations should protect networks and information systems from attacks that seek to exploit software vulnerabilities (flaws in software). For example, software should be supported and up-to-date with security patches applied. Where this is not possible, other security measures should be in place to fully mitigate the software vulnerability risk. Limiting functionality (e.g. disabling services that are not required) and careful configuration will contribute to managing potential vulnerabilities arising from features in hardware and software. Some common user errors, such as leaving an organisation-issued laptop unattended in a public place, inadvertently revealing security-related information to an attacker (possibly as a result of social engineering) etc. can provide opportunities for attackers. Staff training and awareness on cybersecurity should be designed to minimise such occurrences (see B.6 Staff Training and Awareness).
How LogRhythm supports compliance	Using the LogRhythm NetMon, automatic application and protocol identification can be achieved. In addition, packet capture capability based on underlying traffic contents (SmartCapture) is also possible. Lastly, using the built-in Deep Packet Inspection engine, alerting/capture based on specific individual packet contents can be integrated with the LogRhythm NextGen SIEM Platform, or directly output.

Title	B.5 Resilient networks and systems
Principle	The organisation builds resilience against cyberattack and system failure into the design, implementation, operation, and management of systems that support the delivery of essential services.
Description	Organisations should ensure that systems are well maintained and administered through life. The devices and interfaces that are used for administration are frequently targeted, so they should be well-protected. Spear phishing remains a common method used to compromise management accounts. Preventing the use of management accounts for routine activities such as email and web browsing significantly limits the ability for a hacker to compromise such accounts.
How LogRhythm supports compliance	Privileged Account Monitoring is a core part of the LogRhythm NextGen SIEM Platform. In addition, peripheral services such as the LogRhythm Phishing Intelligence Engine (PIE) integrate with mail systems to combat the primary vector of account compromise, account detail acquisition via phishing emails.

Title	B.6 Staff awareness and training
Principle	Staff have appropriate awareness, knowledge, and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the delivery of essential services.
Description	Staff are central to any organisation's ability to operate securely. OESs should ensure their employees have the information, knowledge, and skills they need to support the security of networks and information systems. To be effective any security awareness and training programme needs to recognise and be tailored to reflect the way people really work with security in an organisation, as part of creating a positive security culture.
How LogRhythm supports compliance	LogRhythm has integration with a number of staff awareness/training and situational technologies that can provide real-time intelligence and context back into the SIEM. This enables broader and layered intelligence around risk for specific individuals.

Title	C.1 Security monitoring
Principle	The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.
Description	An effective monitoring strategy is required so that actual or attempted security breaches are discovered and there are appropriate processes in place to respond. Good monitoring is more than simply the collection of logs. It is also the use of appropriate tools and skilled analysis to identify indicators of compromise in a timely manner so that corrective action can be taken. This principle also indicates the need to provide effective and ongoing operational security. As time goes on, new vulnerabilities are discovered, support arrangements for software and services change, and functional needs and uses for technology change. Security is a continuous activity, and the effectiveness of the security measures in place should be reviewed and maintained throughout the delivery and operational lifecycle of a system or service.
How LogRhythm supports compliance	Log management and collection is the first phase of integration within the LogRhythm NextGen SIEM Platform. Data enrichment and contextualisation makes the data orders of magnitude more useful and provides detailed insight. This contextualised data is then made available to the correlation engine for baselining, trending, and statistical analysis. With the LogRhythm Emerging Threats feed, new malware families and methods are available automatically for detection within the system.

Title	C.2 Anomaly detection
Principle	The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployed).
Description	Some cyberattackers will go to great lengths to avoid detection via standard security monitoring tools such as antivirus software, or signature-based intrusion detection systems, which give a direct indication of compromise. Other, less direct, security event indicators may provide additional opportunities for detecting attacks that could result in disruption to essential services. Examples of less direct indicators could include the following: • Deviations from normal interaction with systems (e.g. user activity outside normal working hours). • Unusual patterns of network traffic (e.g. unexpectedly high traffic volumes, or traffic of an unexpected type etc). • 'Tell-tale' signs of attack, such as attempts to laterally move across networks, or running privilege escalation software. • The retrieval of large numbers of essential service design documents It is not possible to give a generic list of suitable indicators because their usefulness in detecting malicious activity will vary considerably, depending on how a typical attacker's actions might reveal themselves in relation to the normal operation of an organisation's networks and information systems. Opportunities for exploiting these less direct security event indicators to improve network and information system security should be proactively investigated, assessed, and implemented when feasible (e.g. technically possible, cost effective, etc). Successful attack detection by means of less direct security event indicators may depend on identifying combinations of network events that match likely attacker behaviour, and will therefore require an analysis and assessment capability to determine the security significance of detected events. Wherever possible, network and information systems supporting the delivery of essential services should be designed with proactive security event discovery in mind.
How LogRhythm supports compliance	Using the built-in trending and baselining capabilities within the LogRhythm NextGen SIEM Platform and CloudAI components, "normal" behaviour can be determined automatically. Deviations from this can be defined as a percentage deviation, time deviation, geolocation deviation, etc. Peer-group analysis can also help determine the change in a user or host's activity from other "similar" users. This can be determined without requiring user input.

Title	D.1 Response and recovery planning
Principle	There are well-defined and tested incident-management processes in place, that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities are in place that are designed to contain or limit the impact of compromise.
Description	Incidents will invariably happen. When they do happen, organisations should be prepared to deal with those incidents and, as far as possible, have mechanisms in place that minimise the impact on the essential service. The particular mechanisms required should be determined as part of the organisation's overall risk-management approach. Examples might include things such as DDoS protection, protected power supply, critical system redundancy, rate-limiting access to data or service commands, critical data backup or manual failover processes.
How LogRhythm supports compliance	Using the built-in Case Management functionality, incidents detected within an environment can quickly be escalated to help reduce time to detect and respond. Adding collaborating team members and automatically recording metrics around detection and response times allows a team to iteratively improve their case handling. The automatic remediation and mitigation component of the LogRhythm NextGen SIEM Platform, known as SmartResponse, allows interaction with other systems within an environment, quickly disabling an account, quarantining a host, changing network configuration, reaching to an endpoint to pull additional forensic data, or testing file samples against external threat intelligence services to determine malicious intent for example.

Title	D.2 Improvements (Lessons learned)
Principle	When an incident occurs, steps must be taken to understand the root cause of that incident and ensure appropriate remediating action is taken.
Description	If an incident does occur, it is important the organisation learns lessons as to why it happened and, where appropriate, takes steps to prevent the same issue from reoccurring. The aim should be to address the root cause or seek to identify systemic problems, rather than fix a very narrow issue. For example to address the organisations overall patch management process rather than to just apply a specific missing patch.
How LogRhythm supports compliance	The LogRhythm NextGen SIEM Platform utilises a leading indexing technology with the availability of clustered indexing nodes to provide incredibly fast drill-down on alerts and alarms generated. This gives SOC team members and analysts direct access to the underlying information, with the additional ability to pivot around data and track back to the root-cause events and entry point to an environment. Remediation capability using the LogRhythm SmartResponse functionality allows the immediate, fully automated modification of systems found to be misconfigured to address any potential gaps.

Summary

In the face of growing cyberthreats against critical national infrastructure, the NIS Directive is a wake-up call to all organisations in those sectors. When the NIS Directive becomes part of UK law in May 2018, companies that provide essential services that underpin everyday life and the economy – such as water, electricity, gas, transport, digital infrastructure, and healthcare – face fines of up to £17m for failures in cybersecurity that leave them vulnerable to attack.

By November 2018, the organisations that fall under the NIS Directive as OESs and DSPs will be confirmed and published. In the meantime, the UK government has outlined the key sectors that will be covered and guidance has been published by the NCSC to help OESs adhere to the security principles outlined in the Directive.

In the event of an incident that interferes with the delivery of an essential service, an OES will be required to report it in a timely manner to the designated regulator for that sector. The OES will then be assessed on whether the appropriate cybersecurity measures were in place. If failures are found, then the OES could face legally binding orders to improve security and a fine of up to £17m for the most serious cases.

In light of these new security and incident reporting requirements under the NIS Directive, businesses are advised to do a full risk assessment of their cyber resiliency and their ability to detect and respond to cyberthreats.

LogRhythm helps organisations assess their current security capabilities and associated level of risk to build a roadmap to improve their security and become more resilient to incoming threats.

Authors

Mark Baker

Director of CNI and enterprise clients,
UK and Ireland
LogRhythm

Adam Brady

Senior OT Engineer
LogRhythm

LogRhythm Industrial

- LogRhythm-specific SCADA labs
- LogRhythm CNI intelligence: real-time use cases specifically for the requirements of the NIS Directive and OT-based technologies
- Specific pre-packed professional services for streamlined implementation in line with the NISD (including security cleared pre- and post-delivery consultants)
- Specific NISD packaged analytics, reports, SpartResponse™ remediation plugins and DPI rules
- Validated MSSP/SIs partners specifically tailored for NISD and CPNI

Why LogRhythm?

- LogRhythm has experience across the globe with CNI-specific requirements, including best practices for previous compliance mandates including NERC CIP
- LogRhythm has patented technology around NextGen SIEM, UEBA and accuracy in data time stamps using TrueTime
- LogRhythm's strategic vendor alliances include real-time correlation and response capabilities to minimise detection and response times

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organisations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralising damaging cyberthreats. The LogRhythm platform combines user and entity behaviour analytics (UEBA), network traffic and behaviour analytics (NTBA) and security automation and orchestration (SAO) in a single end-to-end solution.

LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations centre (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.

LogRhythm®

The Security Intelligence Company

Security. Made Smarter.

Contact us

UK: **+44 (0)1628 918 330**
Germany: **+49 89 919292 - 200**
Middle East & North Africa: **+971 55 6422224**
europe@logrhythm.com | **www.logrhythm.com**

LogRhythm, Clarion House, Norreys Drive, Maidenhead, SL6 4FL, United Kingdom.