DARKTRACE INDUSTRIAL

WHITE PAPER

Darktrace and the UK NIS Directive

Introduction

The Network and Information Systems (NIS) Directive was enacted by the European Parliament[1] in 2016 with the goal of improving security in organisations that deliver vital services within all EU member states. These have been labelled Operators of Essential Services (OES).

The UK government is committed to implementing the NIS Directive and completed a public consultation in August 2017. The National Cyber Security Centre (NCSC) was chosen to provide the core expertise, and released fourteen high-level security principles and their explanations[2]. An initial Cyber Assessment Framework (CAF) was released in April 2018 and is periodically updated[3]. The Competent Authorities (CA) overseeing each industry sector are able to mandate a particular profile (a subset of the CAF that must be met) that each OES must comply with on or by a certain date. Over time, the sectors will largely converge towards the full CAF, although some specialised exclusions may remain.

This white paper demonstrates how OES-designated organisations can fulfil the obligations outlined in the NIS Directive through the implementation of Darktrace's Industrial Immune System.

Built on a foundation of machine learning and AI algorithms, the Industrial Immune System analyses complex network environments to detect indicators of threats against the 'pattern of life' that characterises each network, device, and user. By identifying unexpected anomalies in behaviour, Darktrace autonomously defends against all threat types – from advanced malware to insider threat and IoT hacks – as they emerge, at the earliest stage of the attack life cycle.

OES organisations that deploy the Industrial Immune System will be able to rapidly conform to significant fractions of the NIS Directive CAF.

> "Signature-based malware detection is dead. Cyber security needs to rely on machine learning-based artificial intelligence."
>
> **James Scott, Senior Fellow,**
> **Institute for Critical Infrastructure Technology**

Darktrace and NIS Compliance

Self-Learning Anomaly Detection in Industrial Control Systems

Security principle C.2 (Proactive Security Event Discovery) makes an anomaly detection solution mandatory on identified networks. Legacy approaches such as 'fingerprinting' or 'whitelisting' can flag simple changes, but typically fail to identify truly anomalous activity among the noise of normal network traffic and ongoing operational changes. In order to detect anomalies that meet the human definition of 'unusual', the 'normal' behaviour of the network must be understood to a degree that simple methods cannot achieve.

Darktrace's Industrial Immune System uses machine learning developed by mathematicians from the University of Cambridge to discern the complex 'pattern of life' for each device, user and network. From this rich and dynamic understanding of 'normal' which evolves along with the networks, it can highlight emerging anomalies that go unnoticed by legacy, rules-based approaches.

Implementing and actively using the Industrial Immune System will comply with the entirety of principle C.2. Security principle C.1 (Security Monitoring) is also mostly covered, although some indicators are either focused on internal policies (and therefore not affected by tools), or very strongly recommend higher-level information sharing within industry sectors.

> "There's no denying the benefit Darktrace delivers. It helps us stay ahead of emerging threats and better defend our key systems."
>
> **Martin Sloan,**
> **Global Head of Security, Drax**

Identified Networks

OES organisations rely on both their Operational Technology (OT) networks and their business Information Technology (IT) networks in order to deliver services. The structure and operation of both networks are increasingly convergent and interrelated for service delivery. For many OES, their critical systems will extend beyond their main definition of the OT network.

The Industrial Immune System is effective across the whole organisation, including OT and IT networks. Deploying Darktrace, security teams have a common solution, common capabilities and a common language for exchanging information. Modern control systems are not just significantly interconnected with typical IT, over time large parts of them have adopted IT hardware, software and services.

OT cyber security personnel have inherited all of these IT risks, compounded with the effects of using them in an environment they were not designed for (such as the need for totally reliable patching without frequent restarts). The Industrial Immune System is an industrial-specialised part of Darktrace's wider Cyber AI platform, and is equally capable within low-level OT networks, IT networks (and the high-level OT networks that use them), enterprise networks, the cloud, SaaS applications and more.

Darktrace's AI Analyst brings the benefits of a highly skilled cyber security analyst directly into your organisation, but operates at a scale and speed unmatched by humans. Rather than presenting a user with a single alert, the AI Analyst performs the follow-up investigation gathering and interpreting additional information and related alerts, then presents a far more advanced conclusion. The AI Analyst uses supervised machine learning trained over several years by Darktrace's own expert cyber analysts. As organisations move their OT and IT cyber security functions closer together, this world-leading technology supports both teams with the skills of the other, significantly reducing time to triage.

Real-Time Visibility

Security Principle B.1 establishes clearly that security processes must be "more than just a paper exercise". This is a significant departure from previous Information Security standards, which typically rely on documentation to demonstrate compliance. Darktrace's real-time visibility of the whole internal network, in combination with its comprehensive investigative tools, allows it to have relevance across all but one of the fourteen principles. To meet the spirit of the principle, all audit evidence should be viewable in real time to avoid the label of 'paper exercise'.

Darktrace's Threat Visualizer interface provides an unprecedented view into dynamic network activity across the most complex OT and IT networks. With the implementation of NIS, the ability to quickly investigate events through Darktrace's Threat Visualizer interface is essential as organisations will have limited time to discover and confirm the extent of an issue before they must report it.

How to Engage

As a self-learning technology, Darktrace's Industrial Immune System is extremely quick to deploy, and does not require a long roll-out project. Darktrace operates a no-fee Proof of Value (POV), where a Darktrace appliance is placed in a representative network location and over the course of a month the evaluator is able to see the value to their organisation, including visibility of the network in question and the discovery of threats or anomalies that would otherwise have gone unseen.

You can contact Darktrace to set up a meeting to learn more, and a much more detailed mapping between the capabilities of the Industrial Immune System and the full Cyber Assessment Framework will also be available to be shared and discussed.

Company Background

Darktrace is the world leader in cyber AI technology, with 3,000 customers worldwide and over 40 offices. Founded in 2013, Darktrace has a unique combination of expertise across the fields of mathematics, software and security intelligence. Named a finalist for the Royal Academy of Engineering's prestigious MacRobert Award in 2017 and 2019 and recognised as a 'Technology Pioneer' by the World Economic Forum, Darktrace's fundamental technology enables organisations to detect threats that would otherwise have gone unseen by traditional approaches and autonomously respond to developing threats in real time.

Principle Benefits

The following table sets out the relevance of Darktrace's Industrial Immune System to each outcome listed in Objective C of the Cyber Assessment Framework – Security Monitoring and Proactive Security Event Discovery. Comments on the other areas of the framework are also available.

Colour	Meaning
	Use of Darktrace's products and services results in a complete resolution of this Indicator.
	Darktrace completely meets the requirements of the Indicator itself, but other tools in use may mean the Indicator is not resolved for the organisation.
	Darktrace partially resolves the Indicator, but other tools and/or resources are also required.
	Darktrace provides support for the policies and policy components required by this Indicator.

C1: Security Modeling

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.

C1.a Monitoring coverage

Description	Indicator of Poor Practice	Relevance	Indicator of Good Practice	Relevance
The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function.	Data relating to the security and operation of your essential services is not collected.	Darktrace collects this data when given a copy of live network traffic from port mirrors or taps located in essential networks.	Monitoring is based on an understanding of your networks, common cyber-attack methods and what you need awareness of in order to detect potential security incidents that could affect your essential service (e.g. presence of malware, malicious emails, user policy violations).	Darktrace provides visualisation of your network and ensures complete coverage by ingesting all available network traffic. The standard model set is managed by Darktrace and covers known use cases plus the ability to detect novel attacks.
	You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential services, such as known malicious command and control signatures (e.g. because applying the indicator is difficult or your logging data is not sufficiently detailed).	Darktrace's standard model sets include high-confidence models that qualify as IoCs, and external lists of IoCs can be imported and used by models.	Your monitoring data provides sufficient detail to reliably detect security incidents that could affect your essential service.	Darktrace has proven its ability to detect real-world threats, both previously seen and novel, in all sorts of organisations and networks. Darktrace is happy to support any testing to support this during trials.
	You are not able to audit the activities of users in relation to your essential service.	Darktrace includes an activity audit log tied to user accounts which cannot be edited.	You easily detect the presence or absence of IoCs on your essential services, such as known malicious command and control signatures.	Darktrace's standard model sets include high-confidence models that qualify as IoCs, and external lists of IoCs can be imported and used by models.

Description	Indicator of Poor Practice	Relevance	Indicator of Good Practice	Relevance
The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function.	You do not capture any traffic crossing your network boundary including as a minimum IP connections.	A typical Darktrace deployment will naturally include capture of this data as a subset of the internal network activity.	You have timely access to the data you need to use with IoCs.	Darktrace's visibility and alerts are real-time and immediately accessible to workflows whether through the Threat Visualizer, email alerts, the Darktrace Mobile App or via export to a SIEM.
			Extensive monitoring of user activity in relation to essential services enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.	Darktrace relates activity to users through credentials where available, and through device tracking at all times. Its monitoring is extensive as it examines all network traffic in real time. Specific policy use-cases can be enacted as models with a long list of possible behaviours that can contribute.
			You have extensive monitoring coverage that includes host-based monitoring and network gateways.	Darktrace covers the internal network, incorporating boundary traffic as a subset of this. It does not monitor hosts directly.
			All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.	Darktrace's passive deployment methods mean that only access to network traffic is needed. Normal system provision will require no additional work, although entirely new networks should be designed to provide this data.

C1.b Securing logs

Description	Indicator of Poor Practice	Relevance	Indicator of Good Practice	Relevance
You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.	It is possible for logging data to be easily edited or deleted by unauthorised users or malicious attackers.	Darktrace's records cannot be edited or deleted (outside normal retention periods).	The integrity of logging data is protected or any modification is detected and attributed.	Darktrace's records cannot be edited or deleted (outside normal retention periods).
	There is no controlled list of who can view and query logging information.	Darktrace has individual user accounts with granular permissions, and can link to centralised authentication systems.	The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparative to those it is trying to identify. This includes protecting the service itself, and the data within it.	Darktrace views a passive duplicate of network data, so is not accessible to the threats it monitors. It can be used to identify or investigate network issues affecting logging.
	There is no monitoring of the access to logging data.	Darktrace includes an activity audit log tied to user accounts which cannot be edited.	Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered.	Darktrace's own records are never altered in this fashion.
	There is no policy for accessing logging data.	Darktrace provides strong controls around access and visibility, including role-based access control and LDAP integration, to support secure policies.	Logging datasets are synchronised, using an accurate common time source, so separate datasets can be correlated in different ways.	Darktrace acts as a single point of reference time source for relating all network events, as it recieves traffic in real time. It can be used to view and detect problems with network time synchronisation.
	Logging is not synchronised, using an accurate time source.	Darktrace acts as a single point of reference time source for relating all network events, as it receives traffic in real time.	Access to logging data is limited to those with business need and no others.	Darktrace has individual user accounts with granular permissions, and can link to centralised authentication systems.
			All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user.	Darktrace includes an activity audit log tied to user accounts which cannot be edited.
			Legitimate reasons for accessing logging data are given in use policies.	Darktrace offers an anonymisation mode where initial triage can be conducted without access to identifying data.

C1.c Generating alerts

Description	Indicator of Poor Practice	Relevance	Indicator of Good Practice	Relevance
Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.	Alerts from third party security software are not investigated e.g. Anti-Virus (AV) providers.	Darktrace provides extensive capabilities for investigating alerts, whether produced internally or by a third party.	Logging data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.	Darktrace's primary data source is a complete copy of all internal network traffic. This is an extremely rich data source compared to traditional logging.
	Logs are distributed across devices with no easy way to access them other than manual login or physical action.	Darktrace's real-time visibility of the entire network naturally avoids this issue.	A wide range of signatures and indicators of compromise are used for investigations of suspicious activity and alerts.	Darktrace can make use of external IoCs. It does not work with signatures as a fundamental method, but its models look for a very wide range of known and even unknown signs of compromise through unusual activity.
	The resolution of alerts to a network asset or system is not performed.	Darktrace provides extensive capabilities for investigating alerts, whether produced internally or by a third party.	Alerts can be easily resolved to network assets using knowledge of networks and systems.	Darktrace provides extensive capabilities for investigating alerts to network assets, whether produced internally or by a third party, enabling their resolution.
	Security alerts relating to essential services are not prioritised.	Darktrace's alerts are easily sorted by multiple means, and it is very quick to set up flagging policies that do not require manual updating.	Security alerts relating to all essential services are prioritised and this information is used to support incident management.	Darktrace produces prioritised alerts. This forms part of workflows supporting incident management, that also include analyst commenting and report building. Darktrace offers live analysis services that further support triage and escalation decisions.
	Logs are reviewed infrequently.	Darktrace's machine learning continuously reviews its ingested data to produce alerts, and its Threat Visualizer gives access to the context around them such as log-type information. Normal use of Darktrace to investigate alerts avoids this issue.	Logs are reviewed almost continuously, in real time.	Darktrace's machine learning continuously reviews its ingested data to produce alerts.
			Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.	Darktrace is happy to support any testing to support this during trials and beyond.

C1.d Identifying security incidents

Description	Indicator of Poor Practice	Relevance	Indicator of Good Practice	Relevance
You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.	Your organisation has no sources of threat intelligence.	Darktrace Community services provide threat intelligence, as do all support plans that include access to Darktrace's Analyst team.	You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong antivirus providers, sector and community-based infoshare).	Darktrace provides different support plans and other professional and Community services. It does not recommend or enforce the use of other intelligence feeds.
	You do not apply intelligence updates (e.g. AV signature updates, other threat signatures or IoCs) in a timely way, after receiving them.	Darktrace can be used to act on automated IoC updates, but it is not an AV engine. It can be used to confirm the reporting and updating behaviours of devices that should be operating AV products.	You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.	Darktrace can be used to act on automated IoC updates, but it is not an AV engine. It can be used to confirm the reporting and updating behaviours of devices that should be operating AV products.
	You do not receive signature updates for all protective technologies (such as AV and IDS) or other software in use.	Darktrace fundamentally does not operate on signatures. Its closest equivalent for this outcome is its standard model deck, which is maintained within software updates as a minimum. It cannot confirm the correctness of signature updates to other tools.	You receive signature updates for all your protective technologies (e.g. AV, IDS).	Darktrace fundamentally does not operate on signatures. Its closest equivalent for this outcome is its standard model deck, which is maintained within software updates as a minimum. It cannot confirm the correctness of signature updates to other tools.
	You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	Darktrace Community promotes sharing of feedback and intelligence, including automatic sharing through Inoculation.	You can track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, government agencies).	Darktrace Community allows and promotes sharing of feedback and intelligence, including automatic sharing through Inoculation.

C1.e Monitoring tools and skills

Description	Indicator of Poor Practice	Relevance	Indicator of Good Practice	Relevance
Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential functions they need to protect.	There are no staff who perform a monitoring function.	Darktrace can provide many relevant support and professional services, including a 24/7 SOC monitoring service and training.	You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.	Darktrace can provide many relevant support and professional services, including a 24/7 SOC monitoring service and training.
	Monitoring staff do not have the correct specialist skills.	Darktrace can provide many relevant support and professional services, including a 24/7 SOC monitoring service and training.	Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.	Darktrace can provide many relevant support and professional services, including a 24/7 SOC monitoring service and training.
	Monitoring staff are not capable of reporting against governance requirements.	Darktrace's real-time alerting is compatible with all requirements. Its monitoring services have different response times and can likely match a customer's requirement.	Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external.	Darktrace's real-time alerting is compatible with all requirements. Its monitoring services have different response times and can likely match a customer's requirement.
	Monitoring staff lack the skills to successfully perform any part of the defined workflow.	Darktrace can provide many relevant support and professional services, including a 24/7 SOC monitoring service and training.	Monitoring staff are empowered to look beyond fixed workflows to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.	Darktrace's Threat Visualizer enables investigation of alerts triggered by non-standard threats, from high-level to extremely low-level. It is continuously developed by Darktrace's own Analyst team who encounter such threats routinely.
	Monitoring tools are only able to make use of a fraction of logging data being collected.	Darktrace examines all of the network data that is copied to it. It cannot however ensure that other tools in use do not have this issue.	Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.	Darktrace examines all of the network data that is copied to it. It cannot however ensure that other tools in use do not have weaknesses in this area.
	Monitoring tools cannot be configured to make use of new logging streams, as they come online.	Darktrace natively responds to all new copied traffic inputs as they are added. It cannot however ensure that other tools in use do not have this issue.	Monitoring staff and tools are able to drive and shape new log data collection and can make wide use of it.	Darktrace natively responds to all new copied traffic inputs as they are added. It cannot however ensure that other tools in use do not have this issue.
	Monitoring staff have a lack of awareness of the essential services the organisation provides, what assets relate to those services and hence the importance of the logging.	Darktrace automatically assigns device types and pulls passive identification from the network traffic it monitors e.g. DHCP hostnames. It also allows naming, tagging and priority settings. These can be set up using models to be part automated.	Monitoring staff are aware of essential services and related assets and can identify and prioritise alerts or investigations that relate to them.	Darktrace's alerts are easily sorted by multiple means, and it is very quick to set up flagging policies that do not require manual updating. Minimal customisation can add individual business priorities to the alerting.

C2 Proactive Security Event Discovery

The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployable).

C2.a System abnormalities for attack detection

Description	Indicator of Poor Practice	Relevance	Indicator of Good Practice	Relevance
You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.	Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity.	Darktrace's machine learning has an evolving, deep understanding of the whole network and all devices and users on it derived from its very rich network data source.	Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity.	Darktrace's machine learning has an evolving, deep understanding of the whole network and all devices and users on it derived from its very rich network data source.
	You have no established understanding of what abnormalities to look for that might signify malicious activities.	Darktrace alerts on abnormalities and provides the context around them and ability to investigate them that the security team need. A solid foundation for prioritisation is established by the standard model deck maintained by Darktrace's expert Analyst team.	System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.	Darktrace alerts on abnormalities and provides the context around them and ability to investigate them that the security team need. A solid foundation for prioritisation is established by the standard model deck maintained by Darktrace's expert Analyst team.
			The system abnormalities you search for consider the nature of attacks likely to impact on the networks and information systems supporting the delivery of essential services.	Darktrace's standard model deck, maintained by its expert Analyst team, achieves this through prioritisation of alerts. This can be customised further with minimal effort.
			You regularly update the descriptions of the system abnormalities that you search for to reflect changes to your networks and information systems and current threat intelligence.	Darktrace's standard model deck is maintained by its expert Analyst team and included in software updates as a minimum.

C2.b Proactive attack discovery

Description	Indicator of Poor Practice	Relevance	Indicator of Good Practice	Relevance
You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.	You do not routinely search for system abnormalities indicative of malicious activity.	Darktrace continuously examines real-time network data for indications of potential malicious activity.	You routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting your essential service, generating alerts based on the results of such searches.	Darktrace continuously examines real-time network data for indications of potential malicious activity and produces prioritised alerts.
			You have justified confidence in the effectiveness of your searches for system abnormalities.	Use of Darktrace, or use of Darktrace's threat notification or report services, will provide ongoing evidence of effectiveness.

References

Available at these URLs.

[1] EU legislation underpinning the NIS Directive
https://publications.europa.eu/en/publication-detail/-/publication/d2912aca-4d75-11e6-89bd-01aa75ed71a1/language-en

[2] NCSC explanations of the required high-level security objectives and principles
https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance

[3] The latest Cyber Assessment Framework
https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

About Darktrace

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 3,000 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1000 employees and headquarters in San Francisco and Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.

Contact Us

North America: +1 (415) 229 9100

Latin America: +55 (11) 97242 2011

Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

info@darktraceindustrial.com

darktraceindustrial.com