IT Cybersecurity Act 2.0, Compliance

DARKTRACE

/ Introduction

The German IT security act 'IT-Sicherheitsgesetz 2.0' was reviewed in 2022 with the aim of sufficiently protecting the country's critical infrastructure (KRITIS). According to the changes, providers of critical infrastructure will be obliged to implement systems for recognizing cyber security attacks. By 1 May 2023 all providers of critical infrastructure will have to provide an update on the implementation of these systems according to the maturity scheme defined by the German Federal Office of Information Security.

This white paper outlines the support Darktrace provides to fulfil the MUSS, SOLL and KANN (must, should and can) criteria of the BSI Orientierungshilfe (Guidance for implementation of security systems in national critical infrastructure). Some of the criteria can be further fulfilled with the support of additional integrations and partners.

Built on a foundation of machine learning and AI algorithms, Darktrace technology analyzes complex, dynamic networks to detect indicators of threats against the 'pattern of life' that characterizes each network, device, and user.

By identifying unexpected anomalies in behavior, 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.

Darktrace software uses machine learning algorithms developed by mathematicians from the University of Cambridge to build an understanding of what is normal in the network. This approach is constantly evolving, learning in real time and adapting the results to complex, dynamic network. This allows the system to identify threats at the earliest stages and alert users accordingly.

Nowadays, providers of critical infrastructure rely on both IT and OT networks to deliver their services. The traditional air-gapped approach is slowly disappearing and the structure and operation of both networks are increasingly convergent. This exposes the OT network to more threats coming in from the IT network or the internet.

Darktrace can be implemented across the entire digital infrastructure and combine events from the OT and the IT network, showing them in one user interface.

Deploying Darktrace, security teams have a common solution, with 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). Darktrace's AI Analyst brings the benefits of a highly skilled cyber security analyst directly into your organization 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.

With a unified solution which is easy to implement Darktrace supports the providers of critical infrastructure to protect their critical environments in the ever-evolving threat landscape.

	Requirement	Darktrace
	Logging	
Planning	In the planning phase, based on the results of the risk analysis and considering the operator's critical processes, a step-by-step approach for the implementation of logging SHOULD be planned. The steps SHALL be chosen in such a way that adequate visibility is achieved within a reasonable time.	Darktrace is fully scalable. A single master appliance is sufficient to monitor several thousand devices in a network segment in a first step. If further network segments or locations are added, additional probe appliances can be connected to the existing master appliance. All network segments are considered and analyzed as one unit. If a single master appliance is no longer sufficient, several master appliances can be combined into one system via the so-called "unified view". the installation of additional probe appliances can be accomplished in a very short time.
	The operator SHALL collect, store and make available for evaluation all log and logging data necessary for effective attack detection at system or network level (see glossary according to § 2 paragraph 8 and 8a BSIG) in order to be able to detect and evaluate security-relevant events (SRE).	Darktrace fully analyzes all IP network traffic and extracts all relevant metadata using DPI. This is used to model and detect unusual events. All events in the IP network are logged and stored by the system. A later evaluation of any events is possible. Security-relevant events (SRE) are automatically recognised and evaluated (so-called "model breaches").
	Additional systems CAN be used for this purpose, so that not every single device has to record logging data for effective attack detection and thus the availability of the productive systems and thus the critical service can be guaranteed. The systems required for storage and their IT security precautions SHALL be considered at the planning stage. Since the logging may also contain data records that are relevant under data protection law, the legal handling of these MUST be included in the planning. If necessary, anonymization or pseudonymization of the protocol and logging data may be required.	Darktrace has visibility over all IP network traffic and evaluates it for attack detection. A copy of all IP network traffic is fed to the Darktrace system from central network components (e.g. switches, firewalls). Furthermore, Darktrace does not need access or agents on the production systems, so they are not burdened. Since the data traffic may also contain data records relevant to data protection, the Darktrace system provides a pseudonymization component that can be activated if required.
	As part of the planning process, all systems that are critical to maintaining the critical service SHALL be identified so that their log and logging data can be captured later.	Darktrace can automatically create an inventory of all existing systems in the network and classify them based on the data traffic in the network. Further, systems are grouped according to their similarity (clustering). This facilitates the identification of all critical systems. Furthermore, it is optionally possible to actively contact and identify the systems.
	If the existing systems are not able to provide adequate logging and logging data, the logging infrastructure SHOULD be adapted and/or supplemented by additional measures, software or systems to enable detection and response within the scope necessary according to the risk analysis.	If, for whatever reason, not all the data required for operation is available in the IP network traffic, this can be fed to the Darktrace system, e.g. via log files. In some cases, such as VDI, Darktrace host agents can also be used. However, the latter is rarely the case in the OT environment.

	Requirement	Darktrace
Planning	The amount of logging and logging data generated CAN be determined (and is strongly recommended) using a representative system per system group.	Different sizes of Darktrace hardware and virtual sensors are available depending on the traffic processing requirements. Metrics including number of modelled devices, ingested bandwidth, and connections per minute processed, are all considered in the sizing of sensors. Data from representative systems can be used to calculate the total data volumes for system groups, and consequently the processing requirements of the Darktrace deployment. Darktrace technical specialists will assist in these calculations using data provided by the prospective customer.
	The results of the planning phase SHALL be documented in a suitable form. The documentation SHALL include all network areas, the log and logging data sources, their relationships to each other and the data flow of the log and logging data in the application area.	Upon completing the scoping of the Darktrace deployment in the customer environment, Darktrace technical specialists can assist in creating deployment documentation indicating data capture points, data types, sensor placement, required communication channels, and integrations for data enrichment and workflow.
	An appropriate level of abstraction and detail should be chosen so that the effective use of SzA can be evaluated. To support this, in particular a grouping of similar system groups SHOULD take place within the documentation. Identical or very similar networks (e.g. different sites with the same network structure) may be grouped together. Furthermore, it SHALL be documented for each system or system group which events it logs.	Deployment documentation will indicate sensor placement and the data captured, or systems covered, by each sensor, and the Darktrace deployment as a whole. Similar networks will likely utilise similar Darktrace deployment architecture and data capture methods.
	A process SHALL be established to ensure that logging is adjusted accordingly in case of changes in the scope (Changes).	Darktrace DETECT gains a bespoke understanding of your digital environment, continuously analyzing your users, assets, devices and the complex relationships between them. Because DETECT learns 'on the job', it continues to adapt to your organization as it grows and changes – offering long-term protection against novel threats in an evolving threat landscape. As such, many changes in scope require no reconfiguration in Darktrace, however Darktrace's modular architecture allows for additional data capture points to be added easily if required.
Execution Establish centralised logging infrastructures:	All collected security-relevant log and logging data SHALL be stored at central locations for the respective network area. The number of central storage locations SHOULD be kept as low as possible and at least be oriented towards functional units so that the stored data can be easily accessed. The logging infrastructure SHALL be sufficiently dimensioned for this purpose. Sufficient technical, financial and human resources SHALL be available for this.	Darktrace utilises a primary appliance & secondary probe(s) appliance(s) architecture, in which one or more appliances/sensors configured as probes forward key metadata to a single primary appliance. A Darktrace probe appliance may be placed in the same location as the primary appliance to vertically increase raw packet capture capability, or at a separate location for geographically dispersed topologies. The primary appliance hosts the user interface that provides a single pane of glass through which data is accessed, and for an ordinary operator of the system, the existence of the primary/secondary configuration is invisible.The hardware and software that will be used to achieve a sufficiently dimensioned deployment will be carefully selected by the Darktrace team based on the technical information provided by the customer detailing the scale and throughputs expected at each capture point.

	Requirement	Darktrace
Provision of log and logging data for evaluation:	The collected log and logging data SHALL be filtered, normalised, aggregated and correlated. The log and logging data thus processed SHALL be made suitably available so that it can be analyzed. Temporary storage of the unprocessed log data MAY additionally support the detection process.	Darktrace is designed to collect and process log and logging data from a wide range of sources, including Network traffic in IT and OT environments, endpoints outside of the network, cloud environments and other external sources via syslog ingestion, or API integerations. The system filters, normalizes, aggregates, and correlates this data, making it easy for security analysts to quickly identify and investigate potential threats. All captured data is made readily available through user-friendly dashboards, to provide a comprehensive view of all network activity and enable the evaluation of anomalies, unwanted activities and suspicious behavior. Additionally, Darktrace supports temporary storage of unprocessed log data in the form of PCAPs to enable efficient threat investigation.
	To achieve adequate visibility of attacks, logging data sources SHOULD be tapped at the network level from the outside (network boundaries) to the inside (network areas).	Darktrace is able to detect attacks thanks to configurations of port/VLAN mirroring or TAPs. Darktrace seeks to gain visibility of all traffic passing through the relevant switch infrastructure, and can be deployed anywhere in the network from its boundary, to the internal network. This enables the system to monitor all devices (IT, OT, VoIP, IoT) traffic within a given network without the need to deploy directly onto each endpoint. Darktrace ingests, models and runs threat detection on all traffic types, including encrypted and unknown protocols.
	The system level (critical applications) SHOULD be developed starting from the central, critical systems, such as process control and automation technology and control systems. The prioritisation for the selection of logging data sources SHOULD be derived from the criticality of the systems.	Darktrace is deployed at a central point, in order to gain visibility of the most amount of data, but can also be deployed in other areas to ensure all critical systems such as process control and automation technology and control systems are covered. Darktrace is able to prioritize the most critical systems as the solution is always designed to meet specific security requirements.
	After successful implementation of logging, it SHALL be checked whether all planned logging data sources have been implemented according to the planning. If there are further legal or regulatory logging requirements specific to the industry, these SHALL also be implemented accordingly.	Following the successful implementation of logging, a full data check will be performed with the Darktrace team. This is performed to ensure that logging data sources established during the planning are correctly being ingested by the system. During this data check period, it will be checked that the correct scopes of the networks are being monitored, that the network traffic seen for these devices is complete and of high quality and that third party log sources determined during the planning are also being seen and enriching the data in the system. Further legal and regulatory logging requirements can also be determined during the planning, and verified during the data check process. Depending on these requirements, there is functionality to customize the implementation.

	Requirement	Darktrace
Detection		
Planning	When selecting and deploying detection measures, comprehensive and efficient coverage of the threat landscape SHALL be achieved. For this purpose, the results of the risk analysis as well as the size and structure of the company SHALL be included in the planning. A standardized method (e.g. MITRE ATT&CK or ATT&CK for ICS 6) MAY (and is recommended) be used to determine coverage. Depending on the size of the organization and the threat landscape, separate consideration of detection measures for the IT and OT environments MAY be required.	Darktrace has a fully modular deployment architecture that is entirely capable of scaling up and down to meet desired scope both in terms of the size and structure of your company, but also security needs (as defined by your risk analysis.) The scope of the deployment is always included in the planning to ensure that comprehensive and efficient coverage of the threat landscape is achieved. Darktrace's detection models for both IT and OT environments are preconfigured and mapped to ATT&CK frameworks, and may be directly utilized to determine coverage. Separate detection measures for IT and OT environments are already accounted for by the AI based detection models, but additional custom detection measures can also be configured as needed.
Execution	As a minimum requirement for detection, all basic requirements of DER.1 Detection of security incidents and the following requirements SHALL be met:	
Continuous monitoring and evaluation of log and logging data:	All log and logging data SHALL be continuously monitored and evaluated. This CAN be automated if immediate alerting of those responsible is ensured in case of relevant events. The examination of the event and, if necessary, the reaction SHALL take place within a short period of time according to the risk analysis. Employees or employees of service providers SHALL be appointed who are responsible for this.	Darktrace continuously monitors ingested data 24/7. Darktrace DETECT can then detect anomalous behaviour and generate alerts, the Darktrace AI Analyst can investigate and write reports on that behaviour, and Darktrace RESPOND can stop anomalous behaviour at machine speed. This is performed autonomously by the Darktrace AI, and users can view reports or investigate alerts further in the Darktrace UI. Darktrace can send alerts via the Darktrace Mobile App, Email Alerts, or a third party alerting integration. Additionally Darktrace can integrate with ticketing systems.
	If the responsible employees have to actively search for security-relevant events, e.g. when checking or testing IT systems, such tasks SHALL be documented in corresponding procedural instructions.	Darktrace provides a full audit trail of access and actions taken on Darktrace, including user audit logs. Whilst this audit trail is available natively within the Darktrace UI, audit logs may be also forwarded to external systems in Syslog format.
	Sufficient human resources SHALL be provided for the detection of security incidents.	The AI Analyst greatly speeds up the time to meaning of incidents by providing key information and a narrative of events. Darktrace is not responsible for reacting to incidents, but can assist with Darktrace specific information. Approved partners may be used to monitor Darktrace on behalf of the client, and optoinal services such as Ask the Expert and Proactive Threat Notification can supliment the native Darktrace alerts and account team.

	Requirement	Darktrace
Infrastructure for evaluating log and logging data and checking security-relevant events:	Malware detection systems SHALL be deployed and centrally managed. The network plan SHALL be used to determine which network segments need to be protected by additional detection systems. In particular, network-based intrusion detection systems (NIDS) SHALL be added to the transitions between internal and external networks defined in the network plan.	Yes to all. In accordance with any network plan supplied and conversations with the customer, Darktrace will have probes deployed in central areas where all traffic will be visible. This includes a SPAN on core switches on physical sites or installing Virtual Sensors as VMs within hypervisors or cloud environments (VNets/VPCs) to ingest virtual traffic. This will allow full detection of internal-internal and internal-external traffic, factoring in the customer's environment and topology to determine where these probes should be deployed
	In order for the log and logging data to be correlated and matched, they SHOULD all be synchronised in time. The collected event messages SHALL be checked regularly for anomalies. To ensure that security-relevant events can also be detected retrospectively, the signatures of the detection systems SHALL always be kept up to date.	The Darktrace platform integrates with NTP servers to ensure that logs are synchronized in time, which further allows the end user to navigate through captured data over time and correlate events holistically. Where deployed in a master/probe setup, time differences between Darktrace appliances will also generate alerts so that the end user can investigate and rectify. Based on ingested data and logs the Darktrace platform then performs real-time analysis of traffic, alerting to anomalies and abnormal behavior based on AI learning. As these detections are not based on rules or signatures, but rather deviations from normal behavior, the data underlying the alerting is always kept up to date by means of the continuously learning artificial intelligence.
Evaluation of information from external sources:	In order to gain new knowledge about security-relevant events for one's own information network, external sources SHALL be consulted. Since reports reach an institution through different channels, it SHALL be ensured that these reports are also recognised as relevant by the employees and forwarded to the right place. Information from reliable sources SHALL be evaluated as a matter of principle. All information provided SHALL be assessed as to whether it is relevant for the own information network. If this is the case, the information SHALL be escalated according to the security incident handling.	Darktrace can ingest external threat feeds in the form of STIX or TAXII notifications to understand known bad external IP/Domains. This feeds into the Darktrace learning allowing Darktrace to alert and potentially block these connections, preventing any users or malicious programs accessing the known bad external domain. Darktrace can also receive this data via Darktrace API calls - therefore if the data is in an incompatible format it could first be manipulated and passed to Darktrace to allow it to fit into the modelling and alerting on this. If other third party programs are used, and can export data to syslog, these can be sent to Darktrace in the form of custom data alert. These alerts can then be understood from an anomaly perspective, with Darktrace parsing and understanding these alerts to determine the relevant abnormality of their occurrence for the device or network as a whole. Darktrace customers can enable Darktrace Inoculation which serves to protect customers by identifying threats that are occurring across the Darktrace userbase, anonymising them, and analyzing connections in the specific client network to see if they are occurring in the local client environment as well.

	Requirement	Darktrace
Evaluation of the log and logging data by specialised personnel:	Staff members or staff members of service providers SHALL be specifically assigned to analyze all log and logging data. The evaluation of log and logging data SHOULD be given a higher priority than their other tasks. Therefore, it is recommended that this be their predominant task. These personnel SHOULD receive specialised advanced training and qualifications. A group of persons SHALL be appointed to be responsible for the issue of log and logging data evaluation.	All data received within Darktrace is made available for logging purposes within the UI. Raw network traffic, as well as telemetry information that is sent to Darktrace and is parsed is logged and can be reviewed within Advanced Search. Data is also processed and analyzed to understand typical behavior of users and devices, with anomalous activity being raised for security attention in the form of model breaches and AI Analyst incidents. This data can be accessed within the Threat Visualizer. Logs can be queried within Advanced Search for users to look for specific activity or patterns as needed. Each appliance in the deployment also highlights details of what is fed into the appliance. Alerts are raised for the health of the appliances to allow for continuous logging and performance monitoring. Users responsible for analyzing log and logging data can be receive specialised training for administration of the Darktrace platform. Darktrace Threat Visualizer Administration training is available for all relevant users on the Darktrace Customer Portal.
Central detection and real-time checks of event messages:	Central components SHALL be used to detect and evaluate security-relevant events. Central automated analyzes with software tools SHALL be used to record all log and logging data occurring in the system environment, to relate them to each other and to make security-relevant events visible. All log and logging data supplied SHALL be fully visible and evaluable in the log administration. The data SHALL be continuously evaluated.	Darktrace ensures central components are used to detect and evaluate security-relevant events using a single pane of glass to view activity within an environment. A deployment setup will feature either a Primary-Secondary appliance configuration, where secondary probes are used to capture traffic from a variety of physically disperse capture points, with centralized learning performed on the Primary, or using a Unified View, which is made up of multiple deployed appliances, allowing deployments to scale. Central automated analysis within the system is performed at the primary appliance level, allowing data from different probes to be correlated, and relevant security alerts to be raised. In Unified View environments model breaches are triggered on the masters themselves, with the Darktrace Cyber AI Analyst running on the Unified View able to correlate information together for cyber security events and incidents. Data and logs within Darktrace are fully visible and can be queried and evaluated using the Threat Visualizer. The Darktrace Advanced Search can be used to filter for specific activity or connections for purpose of threat hunting or log administration. Data coming into Darktrace is continuously monitored, with model breaches triggering on anomalous activity when a user or device's pattern of activity deviates from the normal activity performed. Data streams can be reviewed in a continuous fashion via device event logs, which can display real-time data as it is ingested and parsed by the capture engine. Details of these connections can be further investigated and analysed in Advanced Search.

	Requirement	Darktrace
Central detection and real-time checks of event messages:	Central components SHALL be used to detect and evaluate security-relevant events. Central automated analyzes with software tools SHALL be used to record all log and logging data occurring in the system environment, to relate them to each other and to make security-relevant events visible. All log and logging data supplied SHALL be fully visible and evaluable in the log administration. The data SHALL be continuously evaluated.	The Darktrace platform continuously monitors activity within the environment, understanding normal user and device behavior. This allows Darktrace to detect anomalous activity and raise alerts in the form of model breaches to highlight changes in behaviour. Upon a model breach, the Cyber AI Analyst will investigate activity of the user or device to understand whether a security incident needs to be raised, with relevant details provided for further investigation if an AI Analyst incident is raised. Model breaches and AI Analyst incidents will trigger with a severity score (0-100) to highlight the urgency of the incident, and can also be classified based on the criticality of the behaviour (Critical, Suspicious, Compliance or Informational). Model breaches and AI Analyst incidents are available for users to triage. A minimum score or behaviour can be set for users to investigate activity based on their focus. Alerts are raised within Darktrace directly, or can be sent to trigger in external systems (such as SIEMs or SOARs) for the purpose of workflow. A minimum score and behaviour can be specified to ensure desired alerts are sent to the systems. Within the Darktrace UI users are provided with workflow mechanisms, such as Acknowledging alerts and incidents after completing an investigation, as well as Commenting on alerts and incidents to highlight their findings and any relevant details. The system managers are able to regularly review the activity within the UI to understand the alerting and analysis being performed, and can adjust the alerting thresholds to other systems if needed. During investigation, or for the purpose of auditing, users can review logs on a regular basis to understand previous activity triggered on a user, device, or entire environment using Advanced Search to understand a holistic view of a device over a long period of time. Additionally, reporting can be set up to provide a summary of security alerts and incidents in an environment over a specified period of time.

	Requirement	Darktrace
Central detection and real-time checks of event messages:	If defined threshold values are exceeded, an alarm SHALL be triggered automatically. The responsible personnel7 SHALL ensure that, in case of an alarm, a qualified and appropriate response is initiated after professional assessment and within a short period of time according to the risk analysis. The system managers SHALL regularly audit and adjust the analysis parameters, if required. In addition, already reviewed log and logging data SHALL be automatically examined on a regular basis with regard to security-relevant events.	The Darktrace platform continuously monitors activity within the environment, understanding a user and devices normal behavior. This allows Darktrace to detect anomalous activity and raise alerts in the form of model breaches to highlight changes in behavior. Upon a model breach, the Cyber AI Analyst will investigate activity of the user or device to understand whether a security incident needs to be raised, with relevant details provided for further investigation if an AI Analyst incident is raised. Model breaches and AI Analyst incidents will trigger with a severity score (0-100) to highlight the urgency of the incident, and can also be classified based on the criticality of the behavior (Critical, Suspicious, Compliance or Informational). Model breaches and AI Analyst incidents are available for users to triage. A minimum score or behavior can be set for users to investigate activity based on their focus. Alerts are raised within Darktrace directly, or can be sent to trigger in external systems (such as SIEMs or SOARs) for the purpose of workflow. A minimum score and behavior can be specified to ensure desired alerts are sent to the systems. Within the Darktrace UI, users are provided with workflow mechanisms, such as Acknowledging alerts and incidents after completing investigation, as well as Commenting on alerts and incidents, to highlight their findings and any relevant details. The system managers are able to regularly review the activity within the UI to understand the alerting and analysis being performed, and can adjust the alerting thresholds to other systems if needed. During investigation, or for the purpose of auditing, users can review logs on a regular basis to understand previous activity triggered on a user or a device, or within the environment using Advanced Search, to understand a holistic view of a device over a long period of time. Additionally, reporting can be set up to provide a summary of security alerts and incidents in an environment over a specified period of time.
	As a key prerequisite for effective detection, information on current attack patterns for technical vulnerabilities SHALL be obtained continuously for the systems used in the area of application. For this purpose, reports from manufacturers (hardware and software), authorities, the media and other relevant bodies SHALL be continuously reviewed and incorporated into documented vulnerability management processes.	Darktrace's PREVENT provides security teams with the information to continuously harden their systems by providing visibility of weaknesses on both their internet facing assets and the assets within the network. Attack Surface Management checks for known vulnerabilities and potential misconfigurations that can be exploited to gain access to the internal network. Additionally, Darktrace Newsroom will extract reports from vendors, media, and news sources to quickly understand the impact of new critical vulnerabilities and highlight affected assets.

	Requirement	Darktrace
Central detection and real-time checks of event messages:	When implementing detection mechanisms, a calibration SHOULD be performed initially to determine which safety-related events (SREs) occur in the normal state (baselining). This SHOULD be done by assessing whether this normal state is acceptable in terms of the number of false positives or whether changes need to be made. The calibration SHOULD be performed again in case of changes within the scope or the threat situation.	Darktrace's self-learning AI uses continuous learning to adapt to changes as the network evolves. As a result, Darktrace does not require a fixed baselining period to define a normal state. The system allows for tuning of models to speed up the learning process if required. This can be achieved by adding assets or domains to allow lists or adding defeats to individual models. This tuning process can be performed as needed at any point after installation.
	SREs SHALL be reviewed and assessed to determine whether they are indicative of a security incident (qualified SRE). The systems used for attack detection should allow for automated qualification of SREs in clearly identifiable cases. Only qualified SREs SHOULD trigger the process of response. The qualification SHOULD be carried out manually by defined responsible persons in automated cases that cannot be clearly assigned. Based on the findings of the qualification, the detection mechanisms SHALL be readjusted.	Darktrace alerts are automatically classified as: "Critical", "Suspicious", "Informational" and "Compliance". This will be based on the unusual strength of the activity and the possible impact it could have on the environment e.g. a fast moving ransomware would be considered critical. These assignments can also be adjusted by increasing or decreasing the priorities of assets and the underlying detection model.
	If there are further legal or regulatory requirements specific to the industry, these MUST also be implemented accordingly.	Darktrace Cyber AI Loop provides visibility over an organization's entire digital estate, including internal and external data, simultaneously. This allows Darktrace to be used to support legal and regulatory requirements and identify where these have not been fulfilled correctly.

	Requirement	Darktrace
Respond		
	As a minimum response requirement, all basic requirements of DER.2.1 Security Incident Handling SHALL be met for all possible security incidents that are or could be related to attacks. The standard requirements of DER.2.1 Security Incident Handling SHALL also be implemented for all possible security incidents that are or could be related to attacks.	Darktrace is best-in-class for detecting and responding (therefore preventing) to both known and unknown, novel threats - whether these orgiinate from within or outside your organization - and across all data sets you may use. In this way, the use of Darktrace software, should greatly mitigate the risk that a security incident occurs. However, should such an incident arise, the Darktrace software provides total forensic analysis which will save a company's analyst team time and help get the organization back to fully functional asap. Alongside this human analysis, Darktrace also provides an AI-driven Analyst function which autonomously investigates every potential security incident, hugely scaling a human analyst team and reducing their time to understanding of an event. If required, this would also greatly reduce such a team's time to reporting such an incident to the relevant internal or external authority
Automatic reaction to safety-relevant events:	In case of a security incident, the deployed detection systems SHALL automatically report the incident and respond with appropriate protective measures in networks where the automatic response does not endanger the critical service. In networks where the critical service is not endangered by the implementation, it SHALL be possible to automatically intervene in the data stream to prevent a possible security incident. If an automatic reaction is not possible, manual processes SHALL ensure that the possible security incident is prevented.	Darktrace will not only alert should it see a security related behavioral anomaly, but the Response mechanism will suggest a possible blocking action to stop the behavior as well that is appropriate and proportional to the detected incident. The response mechanism can be configured in human confirmation mode, allowing administrators control over the suggested blocks before allowing the system to block or autonomous mode, meaning the sytem will automatically block according to the suggested remediation but still give administrators the ability to override. Automatic response is possible for all cases, however additionally Darktrace allows for manual blocks to be taken as well. Darktrace's unique AI based learning also ensures that the blocks we suggest or apply are very precise and does not block business systems but only the specific traffic darktrace is flagging as behviouraly anomolous, ensuring that critical services are unaffected.
	The exclusion of networks or network segments from an automatic reaction or the intervention in the data stream SHALL be conclusively justified.	Darktrace allows administrators of the system to select the subnets and device types that the autonomous response system is allowed to apply to. Using the tagging system customers can exclude certain highly sensitive areas of the network from any potential interruption from the Darktrace Response feature.
	Identified security incidents allegedly related to attacks SHALL be addressed.	Darktrace will learn the bahaviour of devices on the network. Should these devices start behaving strangely we will initially alert on the behavior if there is a possible security relation to the behavior. Should the behavior continue the Darktrace Response capability will also step in to attempt to block the strange behavior. Darktrace can also integrate in SIEM solutions to help customers surface critical alerts to dashboards the SOC team might have built, we also have a mobile application that allows administrators quick mobile access to darktrace alerts and Responce blocks.

	Requirement	Darktrace
Automatic reaction to safety-relevant events:	In the case of malfunctions and security incidents, especially in the alleged context of attacks, it SHALL be checked whether these meet the criteria of the reporting obligation according to § 8b paragraph 3 BSIG or §11 paragraph 1c EnWG and whether a report to the BSI is necessary.	In the event of a security incident, Darktrace DETECT and RESPOND will provide visibility and autnomous response in order to attempt to prevent such an incident. Should the need arise to analyze an incident as to determine whether the incident meets a reporting obligation, Darktrace is able to fully contextualise the incident in a number of ways. The security team can trigger an AI Analyst investigation on the incident/device to get a summary of unusual activity in report format. Full connection details and metadata can be exported for the given incident/device, providing the specifics of each connection. Partial packet captures can be downloaded with respect to the connections involved. Leveraging Darktrace DETECT, the security team can make an informed decision as to whether the incident needs to be reported, in relation to the relevant BSIG and EnWG acts.
	The systems used for attack detection SHOULD be able to take automated measures to avoid and eliminate attack-related faults, provided that the underlying SRE is clearly qualifiable. It SHALL be ensured that exclusively automated measures cannot lead to a relevant impairment of the operator's critical service.	Darktrace continuously analyzes all devices and IPs on the network, and establishes a pattern of life for these individual devices, as well as the network as a whole. Unusual and/or malicious activity is detected as devices deviate from normal activity. Darktrace alerts on these events and attacks, and is able to autonomously respond in a proportionate manner, in order to neutralise the attack. Importantly, Darktrace has an understanding of 'normal', and thus is able to respond to attacks, without impairing normal business operations or affecting any critical services.
	The deployed SCA SHOULD also support a non-automated qualification and handling of events.	The Darktrace response mechanism can be fully controlled by administrators in terms of what behaviors should be automatically blocked. This can be controlled by on a behaviorly deviation bases and a time basis. Furthermore, manual respond actions and blocks can be triggered by the security team.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,400 organizations globally from advanced cyber-threats.

Scan to LEARN MORE

DARKTRACE

Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011
info@darktrace.com
darktrace.com