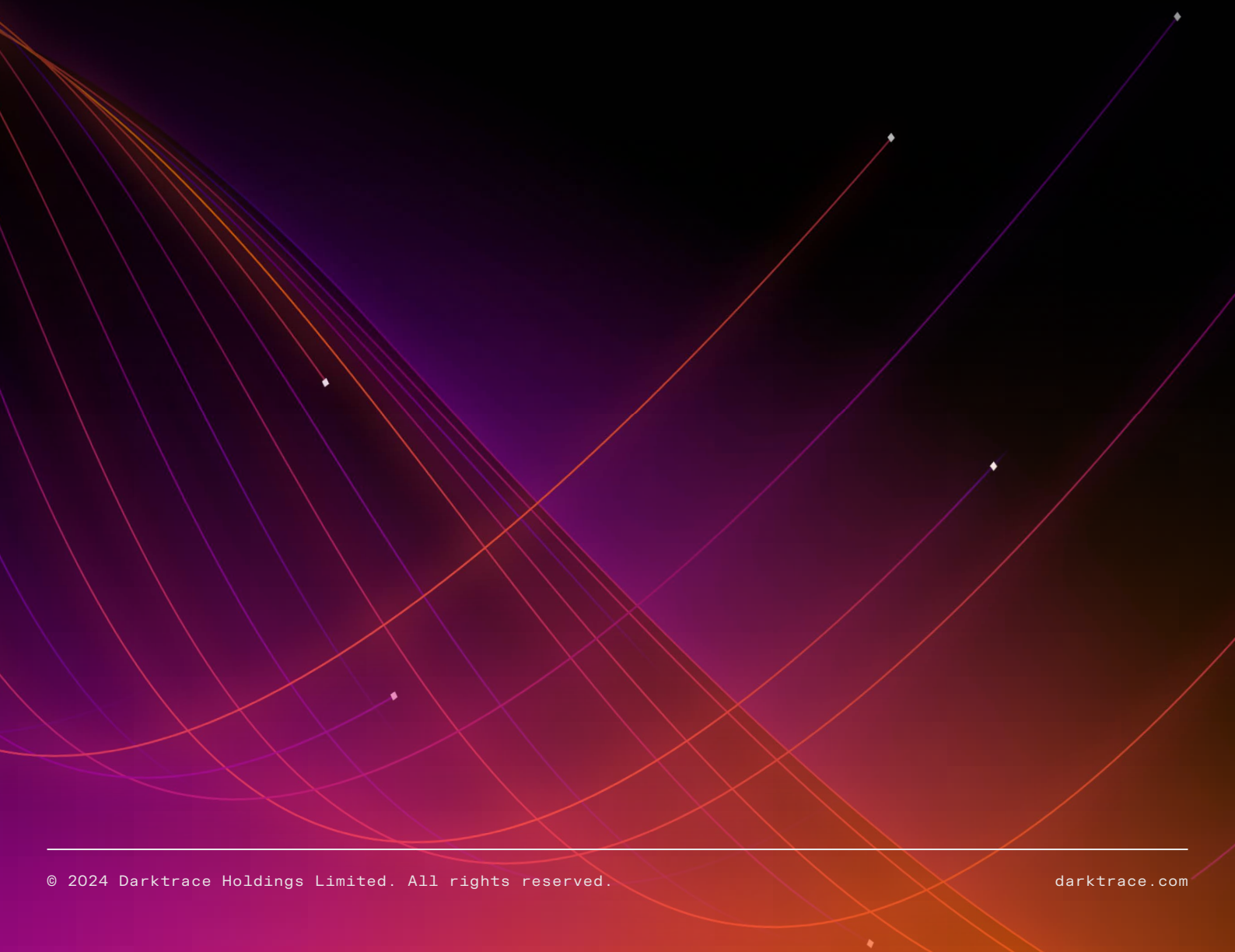
DARKTRACE

Analysts' Top Tips for Darktrace / NETWORK, Darktrace / CLOUD & Darktrace / OT

Customer Handbook



Contents

Read me first

Disclaimer

This document is intended to complement the foundational training and product guides available on the Customer Portal. It is strongly recommended that users complete this training before consulting this guide.

Failure to do so may result in changes to your deployment that could expose your organization to risks or vulnerabilities.

The information provided in this document is based on the assumption that users possess the requisite knowledge from the training. By using this guide without the appropriate training, you acknowledge that you may not fully understand the implications of your actions, which could potentially lead to security incidents.

The information provided in this document is for general guidance and informational purposes only. It does not constitute professional or legal advice.

Darktrace makes no representations or warranties regarding the accuracy, completeness, or reliability of the information contained in this document. Any reliance you place on such information is at your own risk. Darktrace disclaims any liability for any loss or damage arising from the use of the information provided in this document. It is advisable to consult with legal counsel regarding any applicable regulations or legal matters.

These guides may be updated from time-to-time and the latest version, available from the Customer Portal, should always be used.

1. Introduction

Darktrace enables security operations teams to experience a new approach to visibility that keeps machine pace with the threat landscape, surfacing what is most important to your team. Real-time detection and Autonomous Response frees up time for teams, enabling them to perform focused and directed threat investigation.

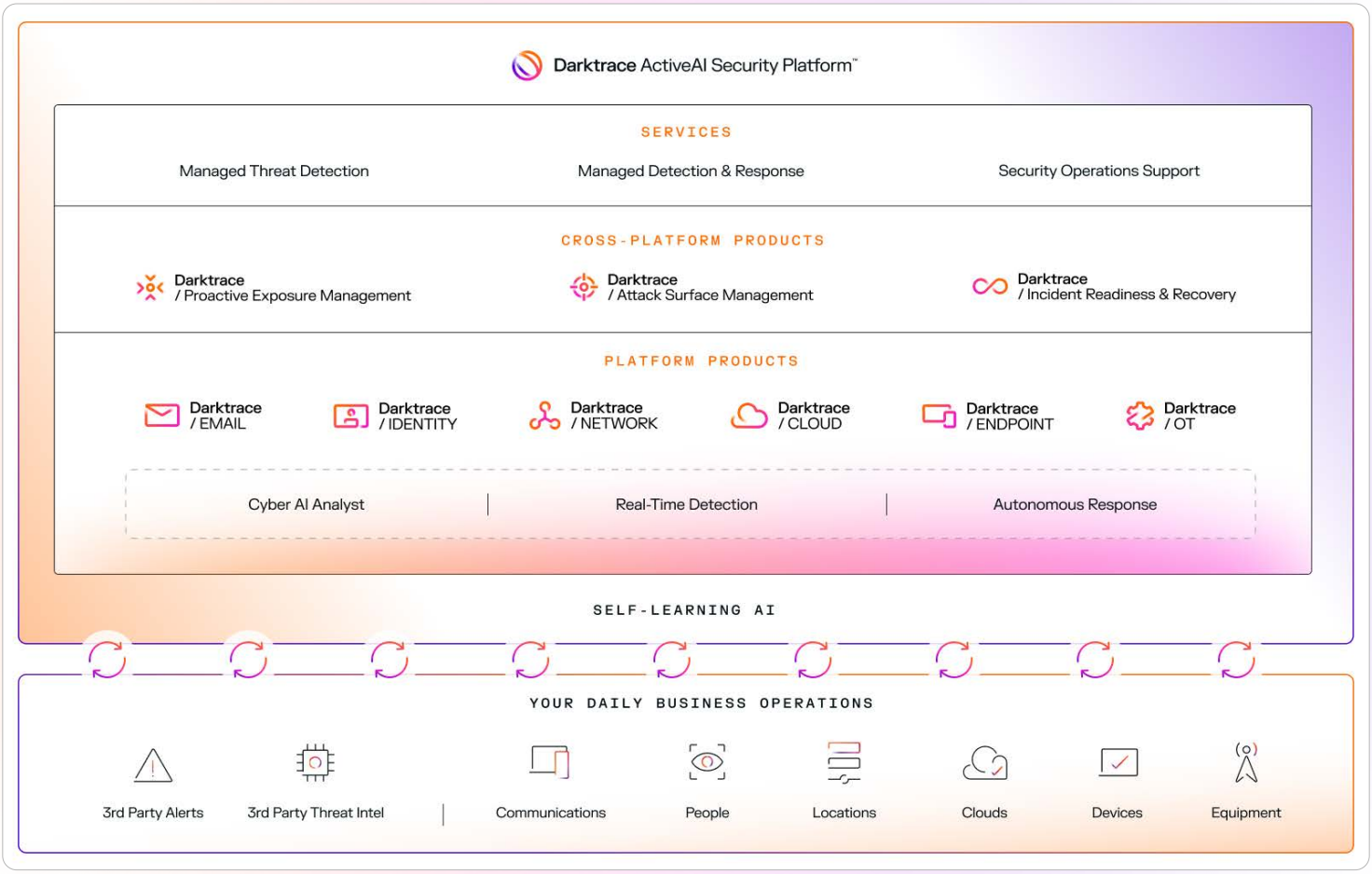
This documentation provides a comprehensive guide for implementing specific changes in your Darktrace / NETWORK, CLOUD and OT deployments that will improve workflows, increase efficiency and maximize value. Whether you are a seasoned professional or new to the field, these top tips will assist you in optimizing Darktrace. We also cover essential strategies to help you deploy changes swiftly and effectively.

Additionally, if you are subscribed to the Security Operations Service (free trials are available via the Customer Portal), you may enquire on the suggestions below by creating a ticket, should you require further assistance. As every deployment is different, there is no one-size fits all approach.

Users should apply their understanding of their own network and security priorities to the suggestions herein. These suggestions are not a replacement for completing the free training available through the customer portal. Instead, they are compiled by Darktrace analysts for analysts, addressing the most common challenges observed in user deployments that can be easily prevented.

The Darktrace ActiveAI Security Platform

Darktrace delivers a proactive approach to cyber resilience in a single cyber security platform, providing pre-emptive visibility into security posture, real-time detection, and autonomous response to known and unknown threats. See the ActiveAI Security Platform solution brief for more information.



2. Darktrace Configurations

Starting off, we will cover deployment configurations that can enrich network data. These configurations will help to empower Darktrace learning, increase Autonomous Response capabilities, and improve workflow processes.

2.1. Label Subnets

Labeling key subnets is an important step to customizing your Darktrace deployment, and to streamline investigation. Labeling at least 50% of your total subnets enables quick identification of key assets. This facilitates easier prioritization during investigations and enables quicker responses to emerging threats.

For example, if you wish to exclude alerts from devices connected to a guest Wi-Fi network, you can use the "Exclude List" feature in a model, or by using the "Model Defeats" feature with the specific subnet label. During the investigation process, you can prioritize the triage of key subnets by filtering for the subnet label in the Threat Tray. Labeling larger subnets removes the need to memorize the purpose of each IP address range and allows for simpler subnet searching and selection in the Threat Visualizer.

For more information on how to add subnet labels, you may refer to this link:

Label Devices Subnets

2.2. Integrate Tools in your Existing Security Stacks

Quickly integrating new technologies into existing security defences is critical. Darktrace's technology is designed with an open architecture that integrates with your existing investments. These integrations include Telemetry Integrations (data enrichment into Darktrace), Threat Intelligence Integrations (additional threat hunting information), Workflow Integrations (to improve workflow processes) and Active Integrations (Autonomous Response Firewall Integrations).

For example:

Telemetry Integrations:

Log ingestion from platforms such as Microsoft Sentinel, Splunk, Netskope, and QRadar can add contextual information, supplement device tracking, enrich Darktrace with data to improve the quality of alerts, and increase's integration across your organization's digital estate. Please note that there are different tracking type templates for mapping. Telemetry data from third-party investigation tools can also be used to trigger Cyber AI Analyst investigations.

For more information on Telemetry Integrations, you may like to refer to these links:

Darktrace for Microsoft Sentinel

Ingesting syslog for enrichment

Cyber AI Analyst Triggered Investigation

Threat Intelligence Integrations:

These integrations can draw in additional contextual details from threat hunting information to enhance Darktrace analysis. Darktrace security integration models then supplement this enriched information with surrounding unusual activity. We also offer the free Darktrace Inoculation tool, where users can share and receive (anonymized) intelligence about unique, high-severity cyber threats discovered elsewhere across the Darktrace customer community.

For more information about Darktrace Inoculation, you may refer to these links:

Darktrace Inoculation

Introduction to TAXII config

Workflow Integrations:

SIEM, SOAR, Email, Mobile App etc. integrations are all available to help security teams manage Darktrace alerts using third-party tools. These integrations are useful for customers who use multiple tools and want all alerts to appear in a single pane.

Active Integrations:

Darktrace Autonomous Response can integrate with third-party firewalls to extend the reach of targeted Autonomous Response network blocking actions. These integrations can be configured and used independently of the native TCP reset capabilities utilized by Autonomous Response to block UDP traffic at firewall level.

2.3. Enrich via LDAP

Darktrace supports integration with LDAP servers such as Active Directory (e.g. Windows Server Active Directory & Entra Domain Services) for both authentication and enrichment. Providing details of an LDAP server for the Darktrace appliance to utilize will enrich user details in Darktrace / NETWORK by providing additional LDAP attributes for users. This also allows for the optional creation of LDAP group tags for use in modeling.

Having LDAP enrichment is particularly useful when it comes to investigating a device – by hovering over the selected device, you can view additional details, including users' email, phone, name, department and more. Another application of LDAP enrichment is the creation of user tags from LDAP groups. These tags are automatically assigned to users seen in the UI; they can then be referenced in Darktrace models to target devices associated with a LDAP user for model optimization. More information on tags can be found in the next section.

For more information about LDAP enrichment, you may refer to this link:

LDAP Enrichment

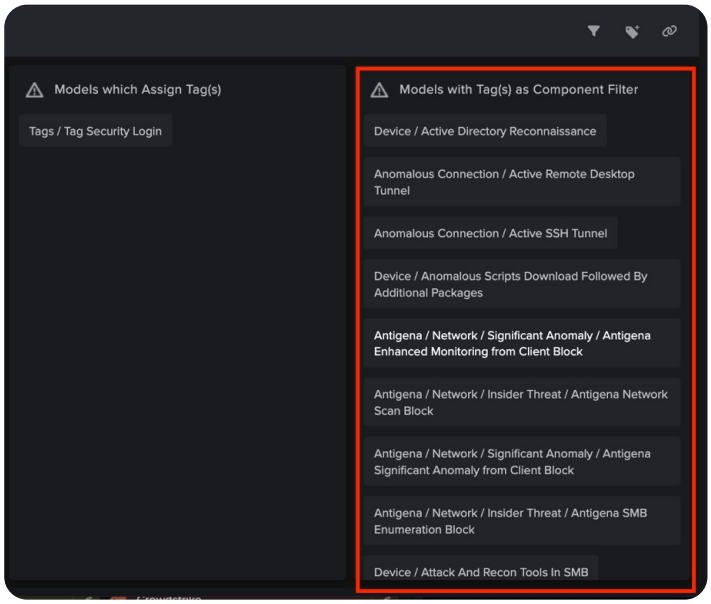


Figure 01: Examples of models that will be defeated when a device is tagged with the "Security Device" tag.

2.4. Tag Devices, Credentials and Users

Tags offer a robust labeling system for network devices, credentials and users detected on cloud platforms (e.g. Software-as-a-Service (SaaS) users). Tags can be used to identify important resources and can be referenced in models to control eligibility for Darktrace Autonomous Response, among other uses. However, tags should be used with care. When combined with model logic and defeats, they can suppress alerts. If not used carefully, this could result in the suppression of alerts for malicious activity.

Tags can be automatically applied as a model action, through LDAP groups (see earlier section), or manually via the UI or the "Device Admin" menu. For cloud environments, tags are applied to SaaS users automatically based on the SaaS platform the user is observed on. These tags on the user's profile allow for the identification of cloud environments and roles associated to that user - these tags are identified by "(CG)".

Tags can be used to exclude specific activity from triggering model alerts. For example, known network security devices performing port scanning in the internal environment will trigger multiple model alerts related to network scanning. If you do not want these security devices to alert on any kind of reconnaissance or lateral movement activity, you can add the "Security Device" tag to these devices. However, please note that adding the "Security Device" tag to a device will defeat many models. Figure 1 shows an example of the models that will be defeated when tagging with "Security Device" tag. You may also navigate Main Menu > Tags > "Security Device".

Another use case for the tagging feature is to enable heightened monitoring of high-risk users or devices. For example, you can use the "High Risk" or "Key User" tags for devices of departing or disgruntled employees, executives subject to spear phishing, or key assets.

For more information about tagging, you may refer to these links:

Commonly applied tags

Introduction to tags

Tags in Darktrace / IDENTITY console

2.5. Configure Autonomous Response

Darktrace Autonomous Response can take a range of proactive, measured, automated actions in response to real-time cyber threats. By understanding the 'pattern of life' of users and devices within the network, Darktrace Autonomous Response can act in a highly targeted manner, swiftly mitigating threats with high precision. This buys time for the internal security team to take remediating actions.

There are three different settings that you can configure Autonomous Response with:

- Full Human Confirmation Mode
- Partial Autonomous Mode
- Full Autonomous Mode

Firstly, new deployments of Darktrace Autonomous Response are initially kept in Human Confirmation mode for a short period. This allows Darktrace Autonomous Response to passively demonstrate the type of recommended actions it would take across your extended network. Secondly, partial autonomous mode is used by customers transitioning to full Autonomous Response mode. There are different ways to configure Autonomous Response to be in partial autonomous mode:

- **At the device level** – Autonomous Response for specific devices (e.g., devices where Autonomous Response can act without significant impact o business operations).
- **At the model level** – Autonomous Response for certain model alerts (e.g., External Threat, Significant Anomaly, Insider Threat, Compliance). If the concern is stopping specific high-risk events such as ransomware, Autonomous Response action can be configured to apply actions when specific model alerts trigger.
- **By time of day** – Autonomous Response can be configured for time periods outside of regular business hours/when security cover is not available.

Ultimately, the ideal end state is for Darktrace Autonomous Response to be in full autonomous mode 24/7, where Autonomous Response actions can be applied at machine speed, without waiting for user approval.

For more information about Autonomous Response modes, you may refer to this link:

Darktrace Autonomous Response deployment modes

3. Cyber AI Analyst

Combining human expertise with AI speed and scale, Cyber AI Analyst streamlines alert investigations and triage processes. This empowers Security Operations Centre (SOC) teams to focus on what matters, helping SOC leaders address the following challenges:

- Insufficient staff
- Team experiencing alert fatigue
- Limited time for daily or weekly investigation
- Attempting to engage in threat hunting, but do not know where to start

Cyber AI Analyst Incident Events are the best place to start when investigating alerts. Cyber AI Analyst Incident Events are only created for the most significant and high-priority activities observed by Darktrace. By incorporating Cyber AI Analyst into your investigation workflow in the Threat Visualizer, your team can concentrate on critical activity in your environment.

For more information about Cyber AI Analyst, you may refer to these links:

Cyber AI Analyst

Cyber AI Analyst investigation in the model alert log

Below are some tips and suggested changes that can be made in your environment to optimize your investigation workflow. Identifying and applying the features that may be the most applicable for your organization will ensure that your workflow is optimized.

3.1. Carrying out Cyber AI Analyst Investigation via Threat Visualizer

There are several features you may consider using to assist you in carrying out investigation on Cyber AI Analyst Incident Events, including:

- **Trigger Cyber AI Analyst Investigations:** When a Cyber AI Analyst investigation is manually triggered, it will conduct a close analysis of the activity for the device or user over approximately one hour, using the specified time as a focal point. It will then contextualize this behavior against historical activity and connectivity for the entity and its peers. For more information about triggering Cyber AI Analyst Investigations refer to this link here.
  - If a device is suspected of engaging in anomalous activity and you want to trigger an investigation bolstered by Cyber AI Analyst, it is recommended to use this function. Cyber AI Analyst will perform an investigation on the specific device during the specified time range.

- **Pre-Set Cyber AI Analyst Filter Options for Threat Tray:** Depending on the kind of alerts you wish to display on the threat tray, we have several filters that you can leverage:
  - **Behavior category visibility**
    Critical, Suspicious, Informational, Compliance
  - **Alert score range (severity ratings)**
    0 to 100%, with 100% representing the most critical incidents
  - **Time range**
    3 days, 7 days, 1 week, and customizable options
  - **Subnet**
    Filter for specific subnets that you wish to conduct further investigations

Filters for specific subnets that you wish to investigate further can be saved locally for both Cyber AI Analyst Incidents, Incident Events, and regular model alerts. If you conduct regular investigations via the Threat Visualizer, you can save your filter options so they are pre-loaded for future use, eliminating the need to manually select filter options each time. This will help optimize your team's investigation workflow.

Threat Tray Basic Filters

Threat Tray Categories

- **Generate A Cyber AI Analyst Report:** A downloadable PDF report can be generated from Cyber AI Analyst Incidents and Incident Events. For more information about generating a Cyber AI Analyst report refer to this link here.

3.2. Alerts via Integrations

Cyber AI Analyst Incidents may be sent to external platforms such as SIEMs. By incorporating Cyber AI Analyst in this manner, security teams can stay informed and take proactive or reactive measures against activities observed in your environment.

API Usage

The Darktrace API provides a method of accessing additional information about a particular alert or device object in the Darktrace system. HTTP GET requests are utilized to return formatted JSON data containing the requested information. The API can be an incredibly useful tool to integrate Darktrace with third-party SIEM or SOC environments, or for performing bulk actions on devices and model alerts.

For example, customers may want to perform bulk extraction of Cyber AI Analyst data, such as the number of Cyber AI Analyst scanning Incident Events observed over a specific period, the source IPs involved, destination IPs involved, etc., for documentation purposes. This information can be obtained using the Darktrace API.

For more information about the Darktrace API:

API Tokens

4. Model Alerts

Darktrace models are a series of logical statements and conditions which, if met, trigger an alert and/or action. Models are primarily used to identify and alert on anomalous and potentially malicious behavior. Output from the complex anomaly framework is available in accessible, building block format in the Model Editor. It can be combined with simple conditions and logical expressions to create tailored activity detection. Like Cyber AI Analyst, features like pre-set filter options for the threat tray, alerting via integrations and API usage can also be utilized for model alerts. Instead of highlighting similar features, we will focus on model alert investigation tips that are recommended to customers by our expert analysts.

4.1. Using Common Advanced Search Queries

Darktrace analyzes network traffic through Deep Packet Inspection; each connection is processed and logs containing key metadata about the connection are produced in Advanced Search. The Advanced Search interface provides searchable access to the detailed metadata logs produced by network traffic and event analysis over the past 28 days. When conducting a deep dive investigation into a particular activity, device or model alert, you may wish to use the Advanced Search feature to assist you.

For more information about Advanced Search:

Searching Advanced Search

If you are unsure how to build search queries for certain activities, Advanced Search provides a list of suggested queries you can utilize. Additionally, if you have queries that you use frequently, you can save them for future use.

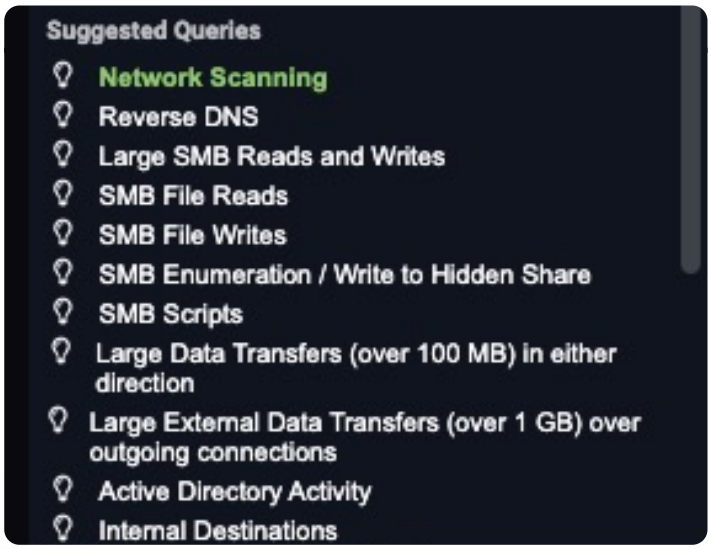


Figure 02: Advanced Search Suggested Queries

Figure 03: Example of an Advanced Search Query

4.2. Additional Darktrace Features

Alert fatigue is a known issue in the cyber security industry, with many customers asking if Darktrace has features to 'blacklist' and/or 'whitelist' endpoints in their environment. Darktrace, as an anomaly-based detection platform, does not rely on rules and signatures for detections. All alerts in your environment are self-regulating, meaning there is no need for end users to constantly address every false positive alert. This reduces the frequency with which the security detection engineering team has to manage false positives.

Nevertheless, Darktrace does have features that can be used in place of a typical 'blacklist' and 'whitelist.' Some of these features include:

- **Trusted Domains:** Domains added to Trusted Domains will be considered by Darktrace as 0% rare. This feature ensures that models relying on domain and endpoint rarity will not alert on activities involving common domains such as "google[.]com". For more information about Trusted Domains refer to this link here.
- **Watched Domains:** Watched Domains are endpoints of concern, flagged due to past compromise, anomalous behavior, or compliance violations. They will trigger a model alert and optional Darktrace Autonomous Response if devices are observed connecting to them. Domains can be added manually, through the API (/intelfeed), or via configured STIX/TAXII intelligence feeds. For more information about Trusted Domains refer to this link here.
- **Model Defeats List:** Specific conditions which prevent a model from breaching - they are distinct from the model logic and will not be overwritten when the model receives updates. Model Defeats are a very useful tool when it comes to optimizing a model. It is recommended to only optimize models for activity that has been confirmed as legitimate and no longer requires alerts. Before implementing any defeats or negative components, ensure that you have identified and understood the risks first. For more information about Trusted Domains refer to this link here.
- **Report Scheduler:** The Report Scheduler allows Darktrace Cyber AI Insights, Executive Threat Reports, Operational Reports and Incident Readiness Reports to be generated automatically and sent to recipients via email. It can now also send a notification when a scheduled report (daily, weekly, monthly, quarterly or yearly) is ready. This feature provides a link to download the report (requires authentication). For more information about Trusted Domains refer to this link here.

These reports are particularly useful for reporting to management and executives, as well as for taking a broader view of your threat environment. They provide an overview of activity in your deployment, overview of user's engagement, the value provided by Darktrace, and more.

You are also able to customize the content (subnet filter, behavior categories filter, etc.) that you wish to include in the report.

5. The Darktrace Mobile App

The Darktrace Mobile App provides a streamlined Threat Visualizer experience for on-the-go investigation and response.

The application allows security teams to quickly investigate suspicious activities and approve, extend or clear any associated Autonomous Response actions. Security teams can be notified of critical alerts and respond to them wherever they are.

For more information about the Darktrace Mobile App, refer to this link here.

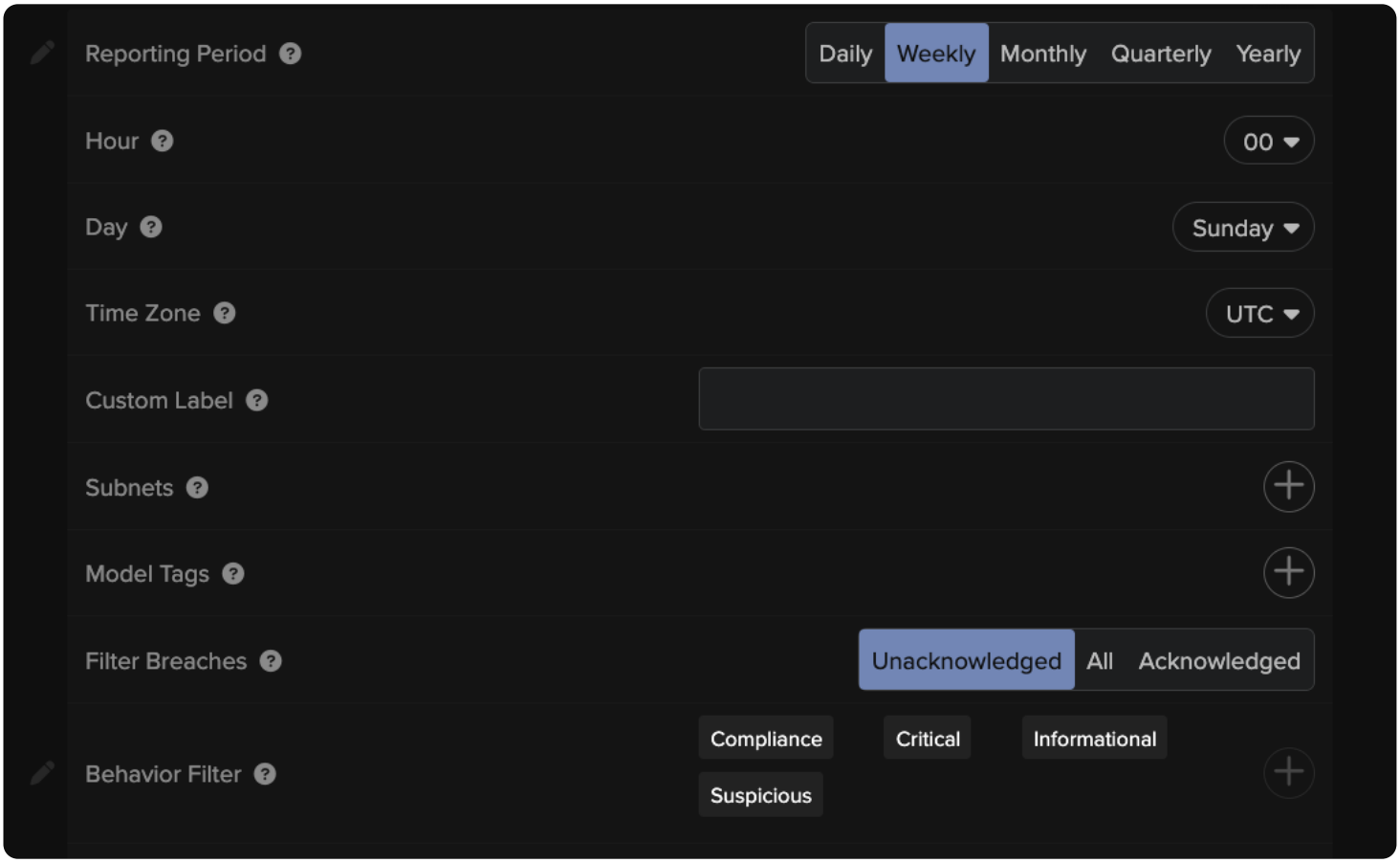


Figure 04: An image of Report Scheduling Configurations.

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,400+ employees who protect nearly 10,000 customers globally. To learn more, visit http://www.darktrace.com.

North America: +1 (415) 229 9100 Europe: +44 (0) 1223 394 100 Asia-Pacific: +65 6804 5010 Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com