Vulnerability Disclosure Policy

Initial Scope

Darktrace's Vulnerability Disclosure Program covers the following products:

- Darktrace Appliances

  Remote access only, ensure you have permission from the appliance's owner before testing.

  Exploits that require physical access to the appliance will not be accepted. The appliances are designed to be kept in secure data centers.

- Darktrace Sensors (V, C, and OS)

While Darktrace has developed a number of other products, we ask that all security researchers submit vulnerability reports only for the stated product list. Researchers who submit a vulnerability report to us will be given full credit on our website once the submission has been accepted and validated by our product security team.

Legal Posture

Darktrace Holdings Ltd will not engage in legal action against individuals who submit vulnerability reports through our Vulnerability Reporting Disclosure Program. We only accept reports for the currently listed products. We agree not to pursue legal action against individuals who:

- Engage in testing of systems/research without harming Darktrace or its customers.
- Engage in vulnerability testing within the scope of our Vulnerability Disclosure Program and avoid testing against anything out of scope.
- Test on products without affecting customers or receive permission/ consent from customers before engaging in vulnerability testing against their devices/software, etc.
- Adhere to the laws of their location and the location of Darktrace Holdings Ltd or its affiliates (United Kingdom). For example, violating laws that would only result in a claim by Darktrace Holdings Ltd based in the United Kingdom may be acceptable as Darktrace Holdings Ltd is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.
- Refrain from disclosing vulnerability details to the public before the expiry of the mutually agreed-upon timeframe.

How to Submit a Vulnerability Report

To submit a vulnerability report to Darktrace Holdings Ltd's security team, please make initial contact by email: vulnerability-disclosure@darktrace[.]com. We can use standard SMIME or other secure methods later when gathering the full details.

Preference, Prioritization, and Acceptance Criteria

We will use the following criteria to prioritize and triage submissions. What we would like to see from you:

- Well-written reports in English will have a higher chance of resolution.
- Reports that include proof-of-concept code equip us to better triage.
- Reports that include only crash dumps or other automated tool output may

receive lower priority.

- Reports that include products not on the initial scope list may receive lower priority.
- Please include how you found the bug, the impact, and any potential remediation.
- Please include any plans or intentions for public disclosure.

What you can expect from us:

- A timely response to your email (within 2 business days).
- After triage, we will send an expected timeline and commit to being as transparent as possible about the remediation timeline as well as on issues or challenges that may extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- Credit after the vulnerability has been validated and fixed.

If we are unable to resolve communication issues or other problems, Darktrace Holdings Ltd may bring in a neutral third party (such as NCSC) to assist in determining how best to handle the vulnerability.

Version

This document Version 2.0 was created on 28 April 2021. We update or review this policy annually. Any updates will be noted in the version notes below.

Original version created on 01 March 2021. Darktrace Limited changed to Darktrace Holdings Ltd.