DARKTRACE

Product Data Sheet

Using the Threat Visualizer: A Practical Guide

Founded on the idea that organizations require a greater insight into what truly happens inside their enterprise networks, the Visualizer focusses on simple, interactive storytelling and is suitable for organizations of any stage of information security maturity. Operators can explore their digital environments without limits, and discover unexpected behaviors which are presented in the context of the actual systems and users within the enterprise.

Darktrace's Threat Visualizer is a unique interface that provides a genuine insight into activity within an organization's entire network and any emerging threats, in real time. Leveraging the Threat Visualizer lets you see what is happening in your enterprise globally, by visually representing all network activity, both external and internal, between all machines and users. This works at a high level, flagging diverse threats and anomalies for the analyst's attention, and at a more granular level, allowing you to drill down and view specific clusters of activity, subnets and host events.

Easy to use, can be used by anyone

The Threat Visualizer is easy for staff members of any skill level or background to adopt, requiring just half a day of training. The platform has been designed and built to enable anyone, from forensic security experts, to business executives and junior members of the IT team who are still developing their corporate IT skills and security awareness.

The Threat Visualizer can be operated in two ways. Firstly, by investigating alerts presented in the threat tray by the Enterprise Immune System. Your analyst can then determine what reactive action should be taken.

Secondly, you can drive the Visualizer from an investigation perspective, by zooming in to examine specific users or devices. A number of Darktrace customers have further enabled their HR professionals to access the Threat Visualizer for the purposes of investigating disciplinary cases for staff members or third parties.

Just ½ day of training

Darktrace training courses are provided for all customers and are focused on the operators that will be analyzing and investigating incidents. The training course also includes a short module covering system administration and audit aspects of the Enterprise Immune System. Darktrace training courses are held on your premises, using your own deployed Enterprise Immune System, ensuring that training is tailored to the context of your enterprise environment. Darktrace trainers provide user manuals and other resources for further learning or reference during the courses.

Use your team more effectively

No additional resources are needed in addition to the Darktrace appliance. The Threat Visualizer can be accessed from any device via a web browser, and is touch-pad friendly. The platform surfaces abnormalities within the customer's network into a threat tray, from which threats are triaged using four key tools: the device event log, graphing function, advanced search and packet capture analysis. These tools allow your team to stop writing rules and focus on investigating threats.

Lifetime access to experts

Every customer will have access to a dedicated cyber analyst, who will oversee the deployment of the Darktrace appliance and training. Weekly Threat Intelligence Reports (TIR), which concisely summarize your network activity each week and categorize any potential threats detected, are provided by either your security team, an outsourced managed service provider, or a Darktrace analyst. Threats are classified into four distinct categories depending on their gravity and potential impact.

Many customers maintain an on-going mentoring relationship with their assigned Darktrace cyber analyst or subject matter expert, which may range from a weekly interaction through to occasional interaction based on the customer's requirements.