User and Entity Behaviour Analytics (UEBA)

Alexander M. Hendren

Nova Scotia Community College, Cyber Security

ISEC1005

Assignment 4

December 10th, 2024

	Product Name	Company Name	Price	Monitors on-prem assets?	Monitors Assets in cloud?	Diverse DATA Source/types?	Ease of setup? (1 = hard, 10 = easy)	Visualization and Alerts?	Scalability
Darktrace UEBA	Darktrace UEBA	Darktrace	Expensive	Yes	Yes	Yes	8/10	Advanced capabilities	Very Scalable
Varonis UEBA	Varonis UEBA	Varonis	Mid End	Yes	Yes	Yes	8/10	Advanced capabilities	Very Scalable
SonicWall UEBA	SonicWALL UEBA	SonicWall	Cheap	Yes	Yes	Yes	6/10	Moderate capabilities	Scalable

After looking over three separate UEBA products, I would recommend ABC Corp uses Darktrace UEBA. Comparing Darktrace UEBA, Varonis UEBA and SonicWall UEBA, I have determined that Darktrace is superior in scalability, visualization and alerts, and ease of setup.

Darktrace is the most expensive UEBA, followed by Varonis and then SonicWall. Because of ABC Corps needs, the more expensive UEBA is justified, as it provides AI detection which the other UEBA's do not. All these UEBA's offer on premise and cloud monitoring, as well as diverse data sources. Darktrace and Varonis are both very easy to setup, while SonicWall can be harder to setup in a large atmosphere. Darktrace and Varonis both offer advanced alerts, but Darktrace is a little bit better as it is powered by AI. SonicWall provides basic alerts but is no where near as in depth as Varonis and Darktrace. Varonis and Darktrace both offer great scalability to larger networks and growing networks.