Enhancing Darktrace Detection Capabilities: Cyberseer’s Deployment Strategy

1. Pre-Service Onboarding Workshop
2. Recommendations
3. Service Onboarding
4. Service Go-Live

1. Pre-Service Onboarding Workshop:

Cyberseer conducts a workshop session with the customer before the commencement of Cyberseer’s Darktrace SOC service. This workshop reviews the environment, optimises the current Darktrace deployment, and provides recommendations for performance enhancement. The ‘Pre-Service Onboarding Checks’ involves a thorough assessment of the Darktrace deployment status. Below are some of the checks carried out during the workshop.

High-level Checks:

- Identify any customer concerns regarding the Darktrace deployment.
- Ensure all probes deployed and operational.
- Ensure all sensors (vSensor, osSensor, cSensor) are deployed and operational.
- Confirm that licensed modules have been configured.
- Ensure required network traffic is present.
- Verify the expected number of subnets and assets have been observed within the environment.
- Ensure unidirectional traffic is within the acceptable limits.

2. Recommendations:

Cyberseer will provide recommendations to address the issues identified in the workshop. Cyberseer will highlight any recommendations that need to be addressed before proceeding with service onboarding.

Cyberseer will guide you through critical issues with Darktrace DETECT and RESPOND, including high-systems status alerts, workflows, configuration, and testing.

3. Service Onboarding:

This stage will commence after the completion of recommendations that need to be addressed before service onboarding. Cyberseer will work with the customer to gain access to the Darktrace environment. The recommendations identified during the "Pre-Service Onboarding Workshop" will be addressed during this stage.

High-level Tasks:

a. Obtain access to Darktrace environment.
b. Identify escalations and reporting channels.
c. Implement Cyberseer Custom Models and monitor their effectiveness.
d. Integrate Darktrace into Cyberseer ASPECT platform
e. Work with customer to address recommendations.
f. Craft custom Darktrace models to prioritise threat detection/response according to customer needs.
g. Update asset tagging to facilitate accurate asset categorisation for efficient monitoring and incident response.
h. Fine-tune Darktrace models to optimise their performance for threat detection.
i. Configure Darktrace Respond (if applicable) to operate in Human Confirmation mode during the initial learning period.
j. Define a change process with the customer. For example,
    - Tuning out-of-the box Darktrace models and Cyberseer models can be implemented using standard change, which doesn't require CAB approval.
    - Tuning of customer-specific models can be implemented using Normal change or Emergency changes, both requiring approval from the customer CAB or customer management.

During the service onboarding, there will be several catch-up calls to track the progress of the onboarding work.

4. Service Go-Live:

After all onboarding tasks have been completed, the service will go live. The analyst will use the pre-agreed escalation chain when a threat or risk is identified.

At this stage, Darktrace Respond (if applicable) will operate in autonomous mode, taking appropriate action based on model settings.