Threat Management Platform
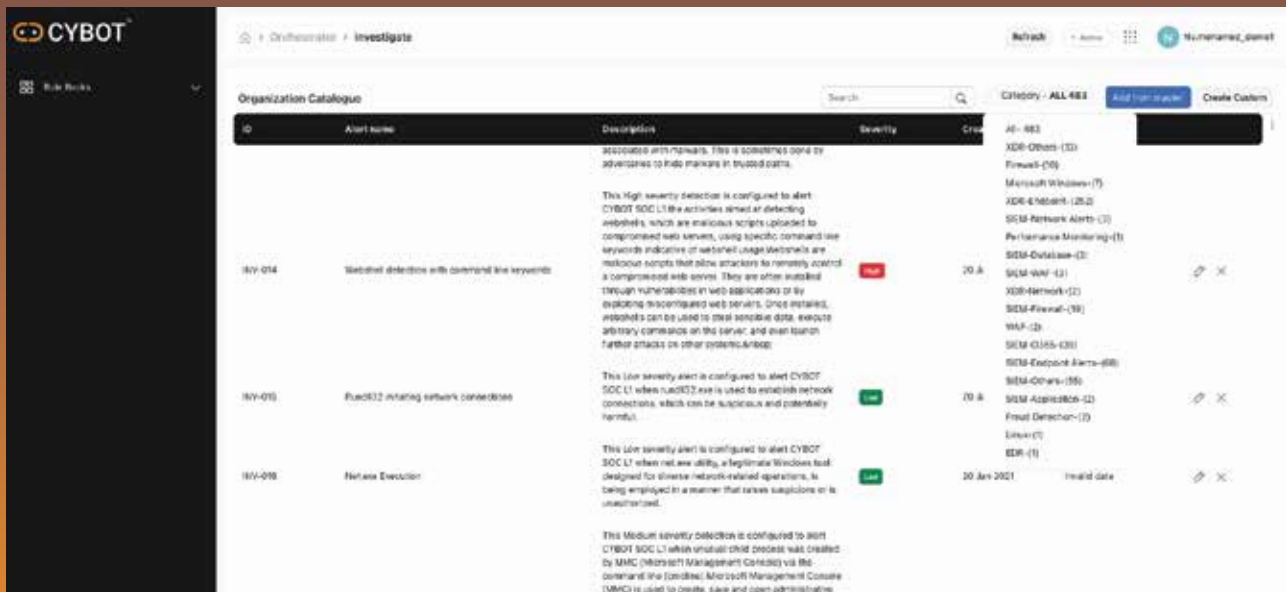
Components: Orchestrator

CYBOT ORCHESTRATOR

Introducing CYBOT Orchestrator, your advanced automation hub for streamlined cybersecurity investigations in the data lake. Seamlessly define, configure, and manage detections across CYBOT components, addressing SOC challenges.


With preloaded proprietary use cases and ongoing integration by our Detection team, Orchestrator provides a user-friendly interface for efficient security posture enhancement.

Its automation extends beyond traditional solutions, enabling continuous scanning for potential threats.

CYBOT Orchestrator: your practical solution for creating, managing, and fortifying defenses against evolving adversary tactics.
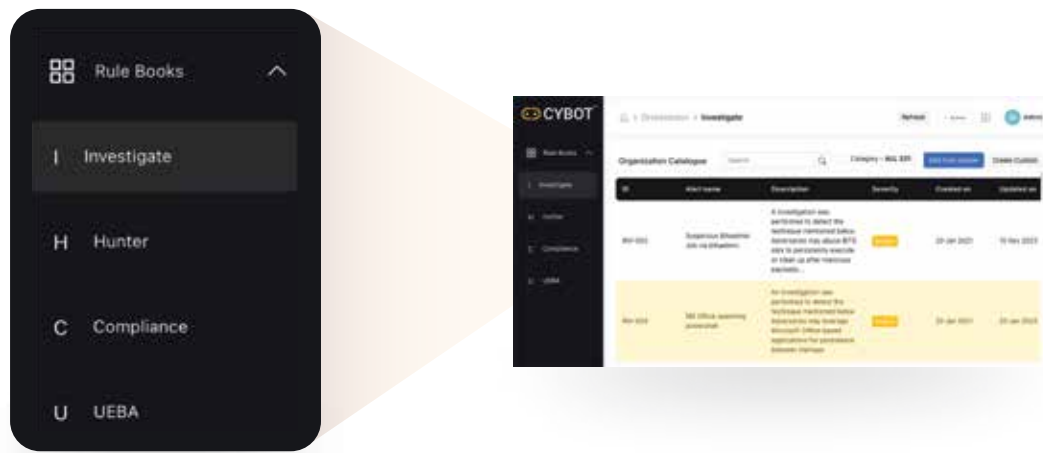
✓ Unlock precision and control in your cybersecurity strategy with CYBOT Orchestrator's intuitive navigation menu. Choose your rule book components effortlessly and take command of your use cases.

**Navigate, create, and manage seamlessly — CYBOT Orchestrator empowers you at every click.**

✓ Explore the **Investigate** components for seamless management of deployed cases, delve into the **Hunter** components for specialized use cases, and ensure **compliance** with ease in the dedicated Compliance components.
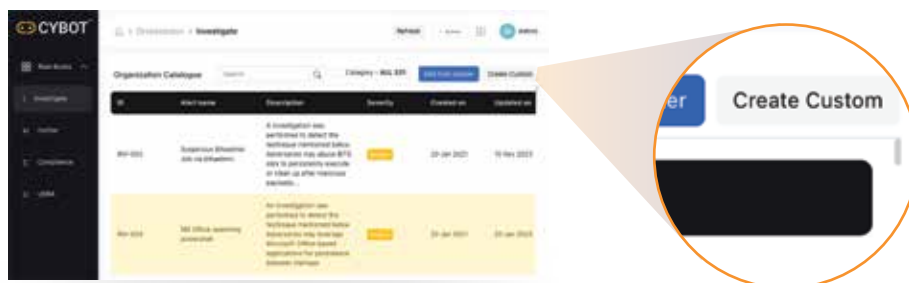
✓ CYBOT Orchestrator offers a unique **Create Custom** feature, allowing administrators to craft and deploy use cases tailored to organizational requirements.

✓ Unlike traditional SIEMs, CYBOT goes beyond by enabling the selection of specific automated investigations to run alongside detections.

✓ This technical flexibility ensures a proactive and customized response to emerging threats, enhancing our cybersecurity capabilities beyond conventional solutions.
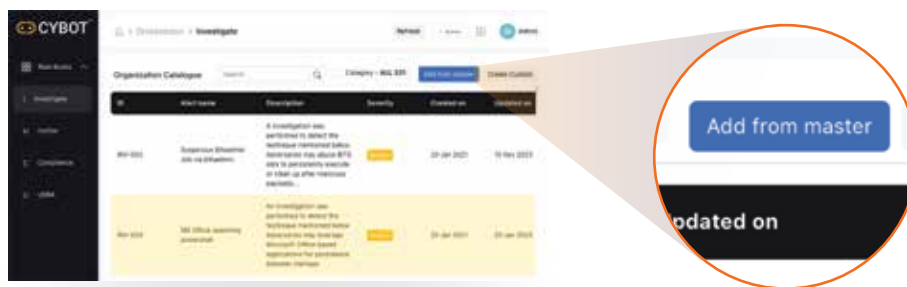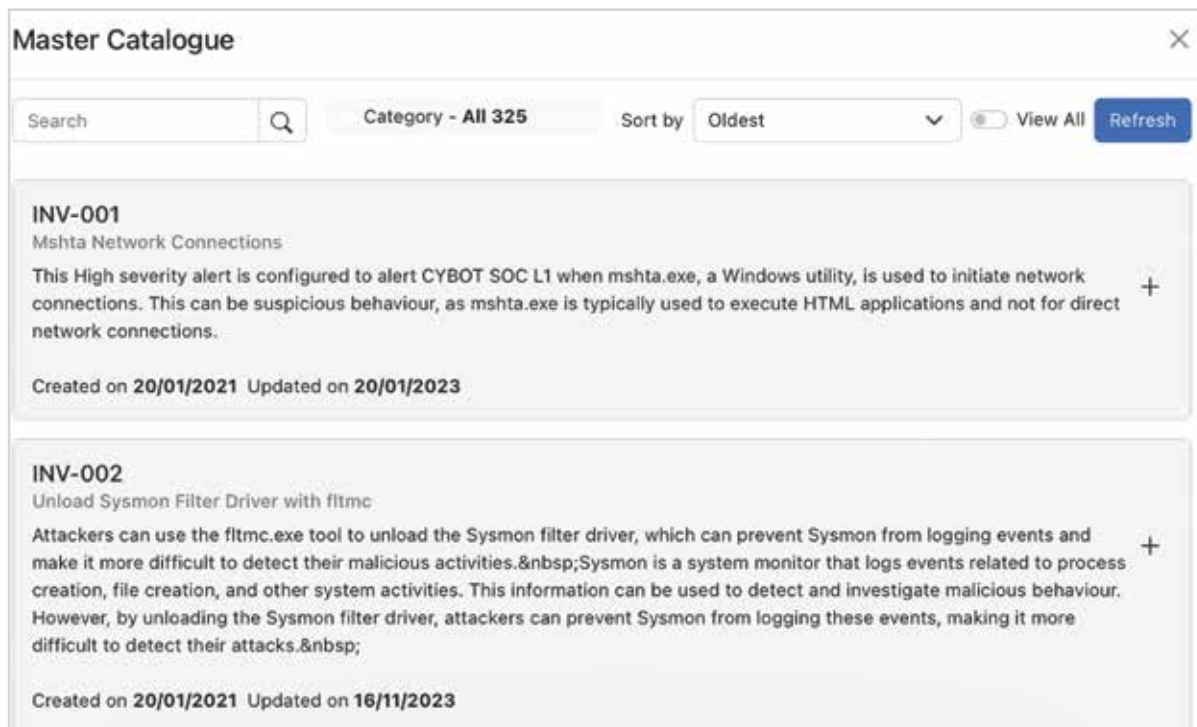
✓ Simplify your workload with CYBOT Orchestrator – our Detection Engineering team takes charge of new threat identification.

✓ When they pinpoint a new ATP activity or attack vector, a corresponding use case is promptly added to the **master repository**.

✓ Admins can effortlessly access the master library, adding required use cases to their environment without the need for manual creation. It's that straightforward.

Master Catalogue ✕

Search 🔍   Category - All 325   Sort by Oldest ⌄   ⬤ View All Refresh

INV-001
Mshta Network Connections

This High severity alert is configured to alert CYBOT SOC L1 when mshta.exe, a Windows utility, is used to initiate network connections. This can be suspicious behaviour, as mshta.exe is typically used to execute HTML applications and not for direct network connections.

Created on **20/01/2021** Updated on **20/01/2023**

+

INV-002
Unload Sysmon Filter Driver with fltmc

Attackers can use the fltmc.exe tool to unload the Sysmon filter driver, which can prevent Sysmon from logging events and make it more difficult to detect their malicious activities. Sysmon is a system monitor that logs events related to process creation, file creation, and other system activities. This information can be used to detect and investigate malicious behaviour. However, by unloading the Sysmon filter driver, attackers can prevent Sysmon from logging these events, making it more difficult to detect their attacks.

Created on **20/01/2021** Updated on **16/11/2023**

+

Notice

Copyright

Trademarks

Contact Us

ActiveBytes Innovations

Sharjah Media City, Sharjah, UAE, Dubai, UAE +971 505676727
www.active-bytes.com