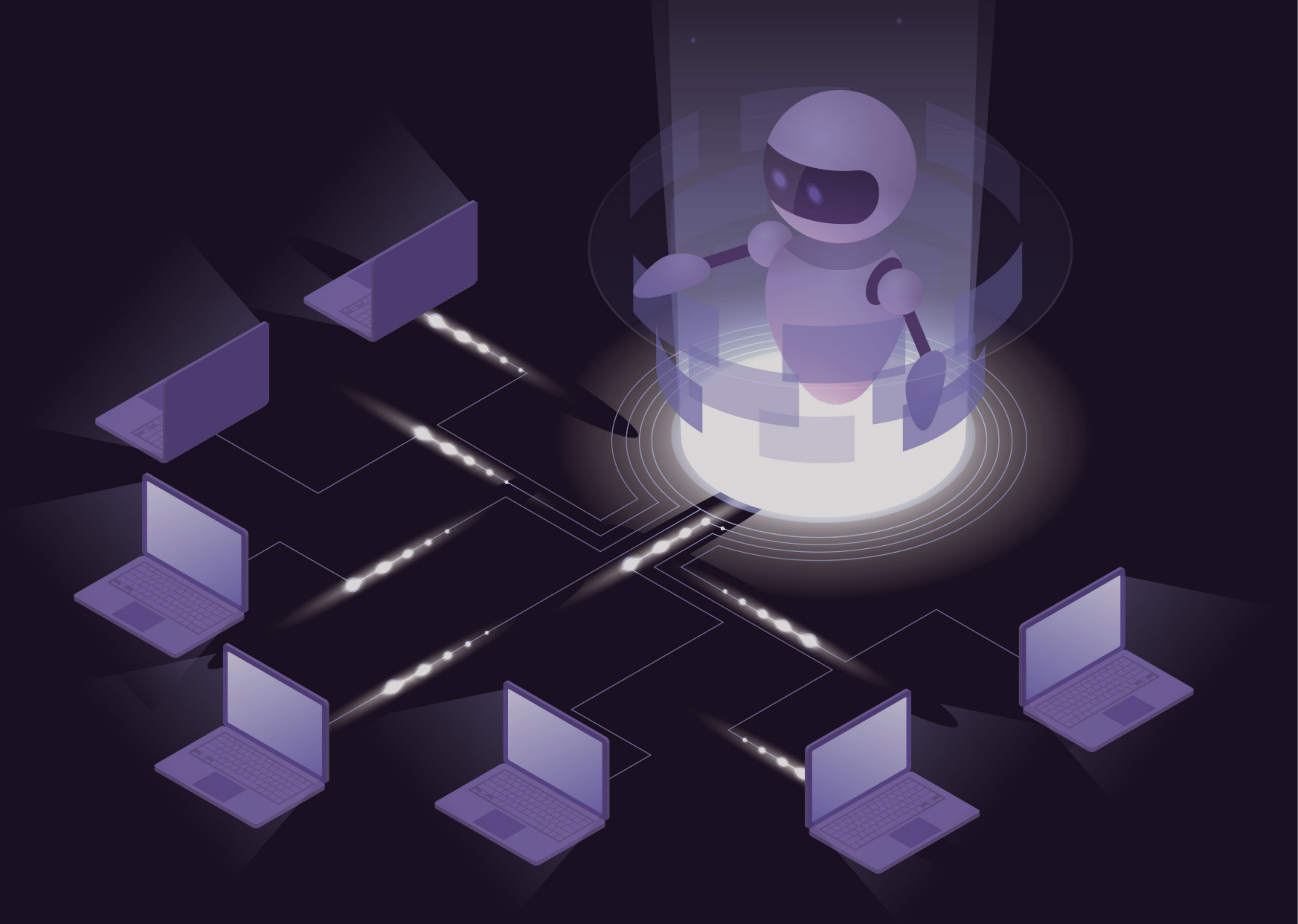
CYBOT™

Automated Investigation & Hunting Platform



Datasheet

Overview

activebytes innovations

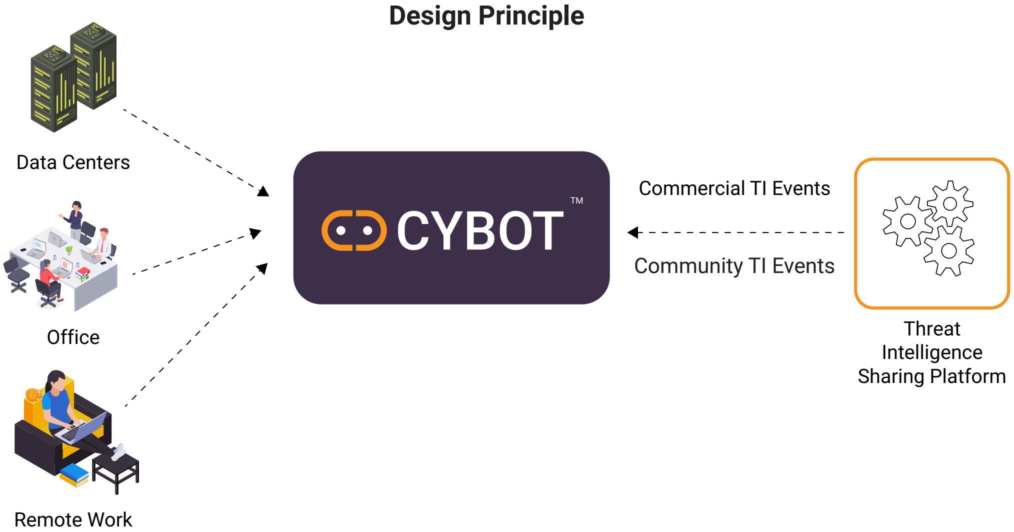
www.active-bytes.com

About the CYBOT

The working of the CYBOT is basically divided into three parts:

- First, the Analytics Platform with an analytics engine where the data from network sensors and endpoint sensors get collected. The data from log sources are contextualized ,structured & then displayed in user friendly dashboards for the analysts.
- Second part is the Threat Intelligence platform ,that collects feeds like IOCs and TTPs from community and commercial sources and integrate them with the Threat Hunting platform. This security intelligence, vulnerability & exploit intelligence feeds adds to the adaptive nature of the CYBOT automated playbooks ,thereby making it very effective in hunting & investigation.
- Third part is the Automated Threat Hunting platform that automatically & intelligently investigates the suspected observables from your enterprise logs in the analytics engine of analytics platform , correlates it with the known IOCs, patterns & intelligence feeds. After the automated investigation by intelligent playbooks, the result of the hunt is displayed in dashboards at granular level for the analysts. CYBOT is also designed with option to respond a threat by clicking a button. This saves time for analysts to perform other critical actions like neutralizing the adversary element that has breached your IT infrastructure security system.

Design Principle



Analytics

CYBOT Platform includes a Big Data Analytic Engine ,that handles huge amount of enterprise raw data which is beyond human capability ,with best-in-class analytics and processing capability. The logs collected from the endpoints, servers & network of the enterprise IT infrastructure is contextualized and formatted before undergoing automated analysis. Then it's displayed as Dashboards for analysts ,with information related to files, processes, hash, URL, network traffic, uncommon ports, IP etc. at granular level. Every data of suspicious nature undergoes further drill down automated investigation in Threat Hunting platform.

We've made hundreds of Dashboards and Alerts out of the box for both compliance and security analytics use cases. You will have access to our value-added provision of content-library where we update new dashboards & alerts use cases to continuously improve intelligent automated hunting capability of the CYBOT and thereby protect your infrastructure safety.

Know More About Datasheet of Analytics Platform

CYBOT Threat Intelligence

CYBOT has a Threat Intelligence Platform which continuously gets updated with knowledge of latest cyber security attacks, vulnerability & exploit intelligence and their details in the industry worldwide. This makes CYBOT adaptive and highly efficient in automated investigating & detection of hunts among the huge Logs by correlation.

The inputted Information from both commercial and community threat intelligence events, news and vulnerabilities is accessible in CYBOT platform to both technical and non-technical teams in the form of user-friendly dashboards, printouts and emails. This provides analysts and incident responders with effective intelligence. CYBOT is designed to avoid repeated investigation on identical observables including IOCs and patterns, thereby reducing false-positives and noise to the analysts. We extend our security specialist's hands for threat intelligence services like domain take down.

[Know More About Datasheet of CYBOTs Threat intelligence Platform](#)

CYBOT-Automated Threat hunting & Investigation

Raw data collected via sensors from servers, network and endpoints of the enterprise environment are fed into the Analytical engine and then stored in a unified, contextualized & secured format. CYBOT is designed to be intelligent & adaptive.

The platform is continuously updated with automated intelligent playbooks and intelligence information from security sources. The result from this automated hunts are displayed as dashboards and made available to be downloaded or taken as printouts. When the intelligent automation playbooks detect a threat, it executes end to end investigation, enrichment, and suggest incident response actions (can be quickly performed by security team via a preconfigured button placed next to suggestion section in the Dashboard) in case of an adversary intrusion. There are hundreds of playbooks, dashboards & Alerts use cases available in CYBOT and these use cases are are beyond capability of a human threat hunter.

[Know More About Datasheet of CYBOTs Threat Hunting platform]

activebytes
innovations

www.active-bytes.com / contact@active-bytes.com
+971 50 513 3973