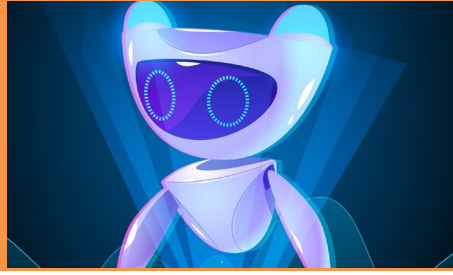
CYBOT™

Automated Investigation & Hunting Platform

## Datasheet: Compliance

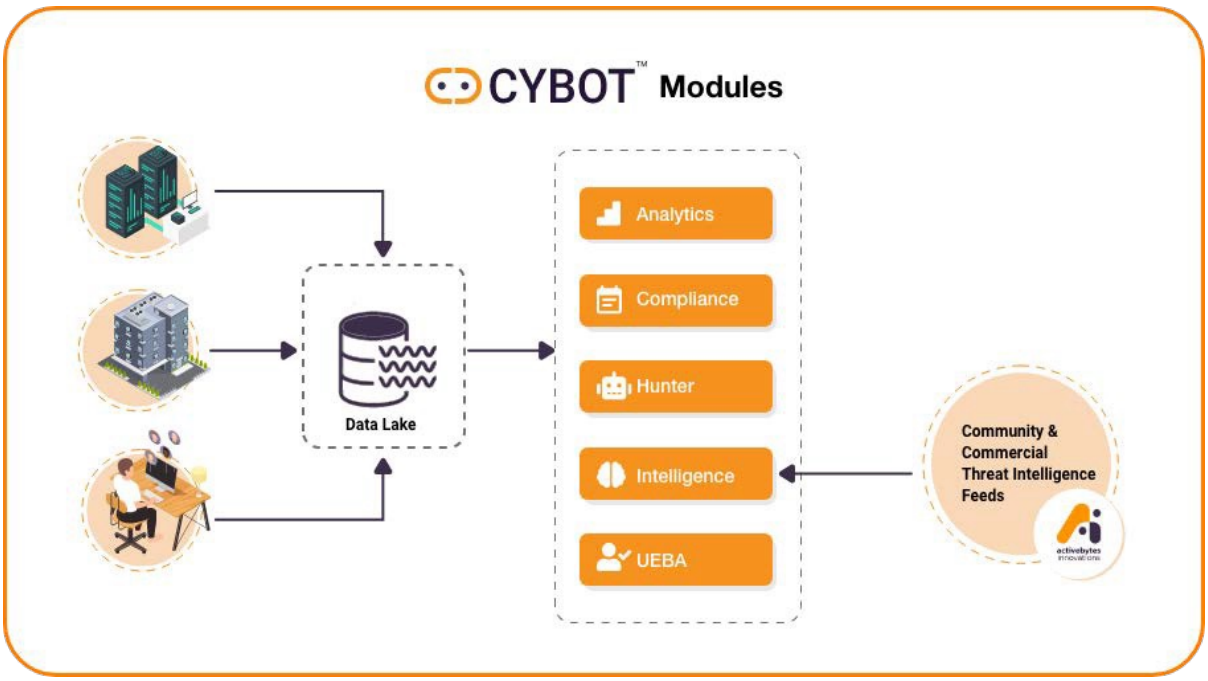


www.active-bytes.com / contact@active-bytes.com
+971 50 513 3973

# About the CYBOT™

**The working of CYBOT™ is basically divided into five 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 and then displayed in user-friendly dashboards for the analysts.
- The second part is the Threat Intelligence Platform, which collects feeds like IOCs and TTPs from community and commercial sources and integrates them with the Threat Hunting Platform. These security intelligence, vulnerability and exploit intelligence feeds add to the adaptive nature of CYBOT™ automated playbooks, thereby making them very effective in hunting and investigation.
- The third part is the Automated Threat Hunting Platform that automatically and intelligently investigates the suspected observables from your enterprise logs in the analytics engine of the analytics platform and correlates them with the known
- The fourth part is the UEBA module, designed to perform behavior analysis of user & hosts with machine learning algorithms. Data from the data lake is fed into the module for prediction of anomalies.
- The fifth part is the Compliance module designed to aid organizations and security teams to meet regulatory standards such as ISO 27001, PCI DSS & NIST through the built-in compliance dashboards and Active monitoring. The data from the data lake, that deviates from the required standard is triggered and displayed in detail. IOCs, patterns and intelligence feeds. After the automated investigation by intelligent playbooks, the result of the hunt is displayed in dashboards at the granular level for the analysts. CYBOT™ is also designed with an option to respond to 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.




Click here to get an overview of the working of CYBOT ™

## CYBOT™ Compliance

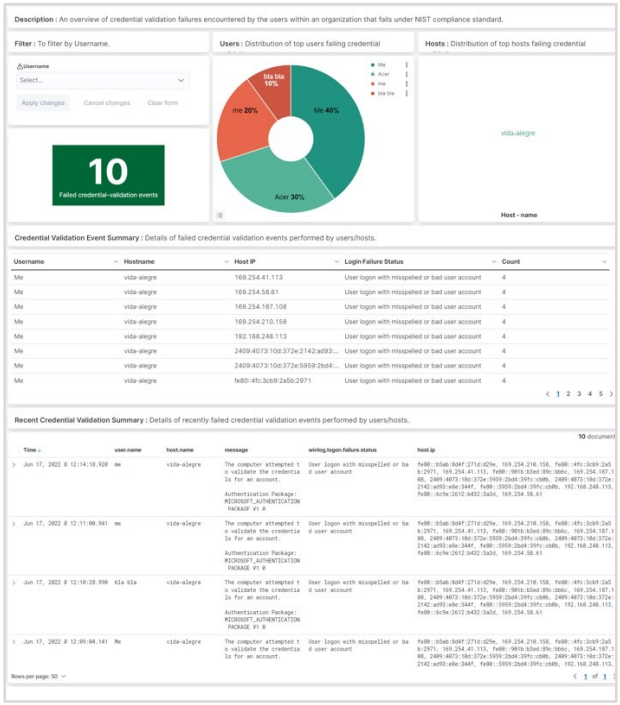
We have designed a compliance module in CYBOT solution, with an aim to aid organizations and security teams to meet regulatory standards such as ISO 27001, PCI DSS & NIST. The alerts and dashboards in the module are based on controls requirement. The enterprise data from data lake relevant to compliance controls is visually displayed in an accessible, user-friendly interface that provides actionable insights, and allows administrators to prioritize and respond to the most serious threats first. A compliant company culture establishes an organization's trustworthiness, integrity, and maturity in the industry landscape

CYBOT compliance package consists of **compliance Dashboards** and **Active monitoring**

## Dashboard for compliance

There are more than hundreds of dashboards designed based on compliance standards PCI DSS, NIST & ISO 27001


This dashboard shows an overview of rejected network connections encountered by the endpoints within an organization that falls under NIST compliance standards.




This dashboard gives an overview of credential validation failures encountered by the users within an organization that falls under NIST compliance standard.

[click here to view full list of ISO 27001 dashboard compliance]

[click here to view full list of PCI DSS dashboard compliance]

[click here to view full list of NIST dashboard compliance]



activebytes innovations

## Active Monitoring

Active monitoring are alerts designed to trigger in an organisation based on the compliance regulatory standards like NIST, PCI DSS & ISO 27001

- ✓ When active monitoring is triggered the security team will see (Fig 1), showing the details of an alert triggered, along with its compliance mapping control number.

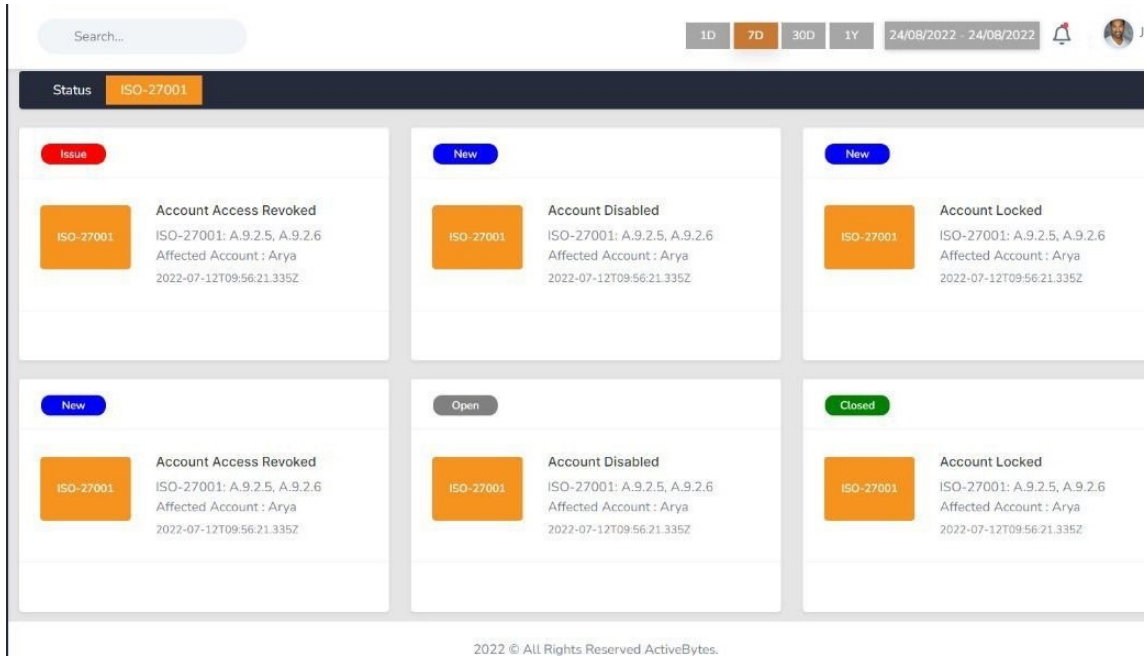



Fig 1

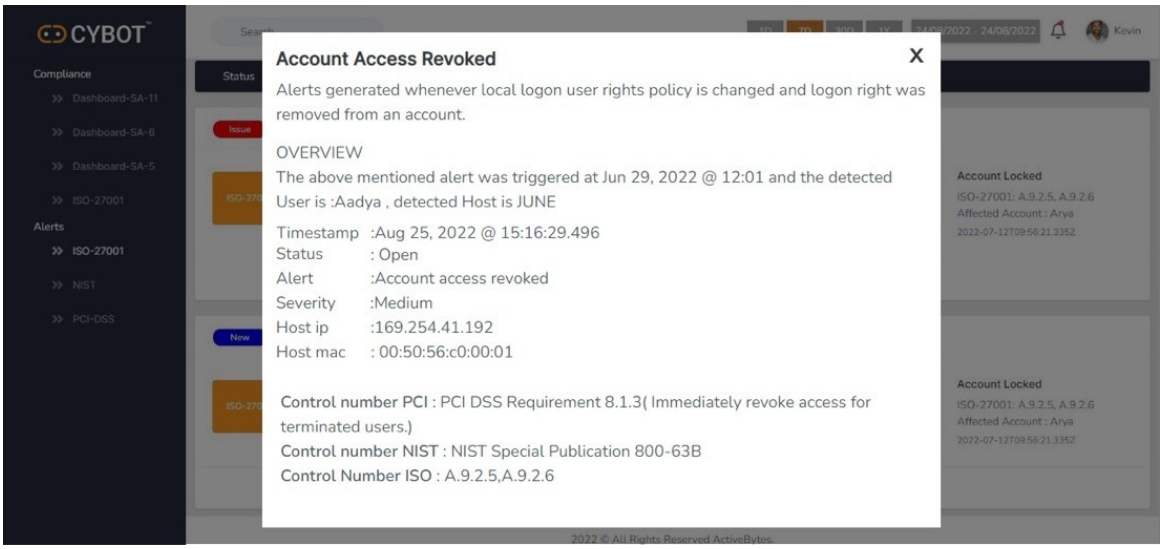



Fig 2

- ✓ The pop-up window (fig 2) shows the content of an Active compliance module, along with a description of the triggered event, details regarding that event, and Control numbers that map it to the compliance standards

click here to view full list of PCI-DSS, NIST, ISO 27001 Alert compliance