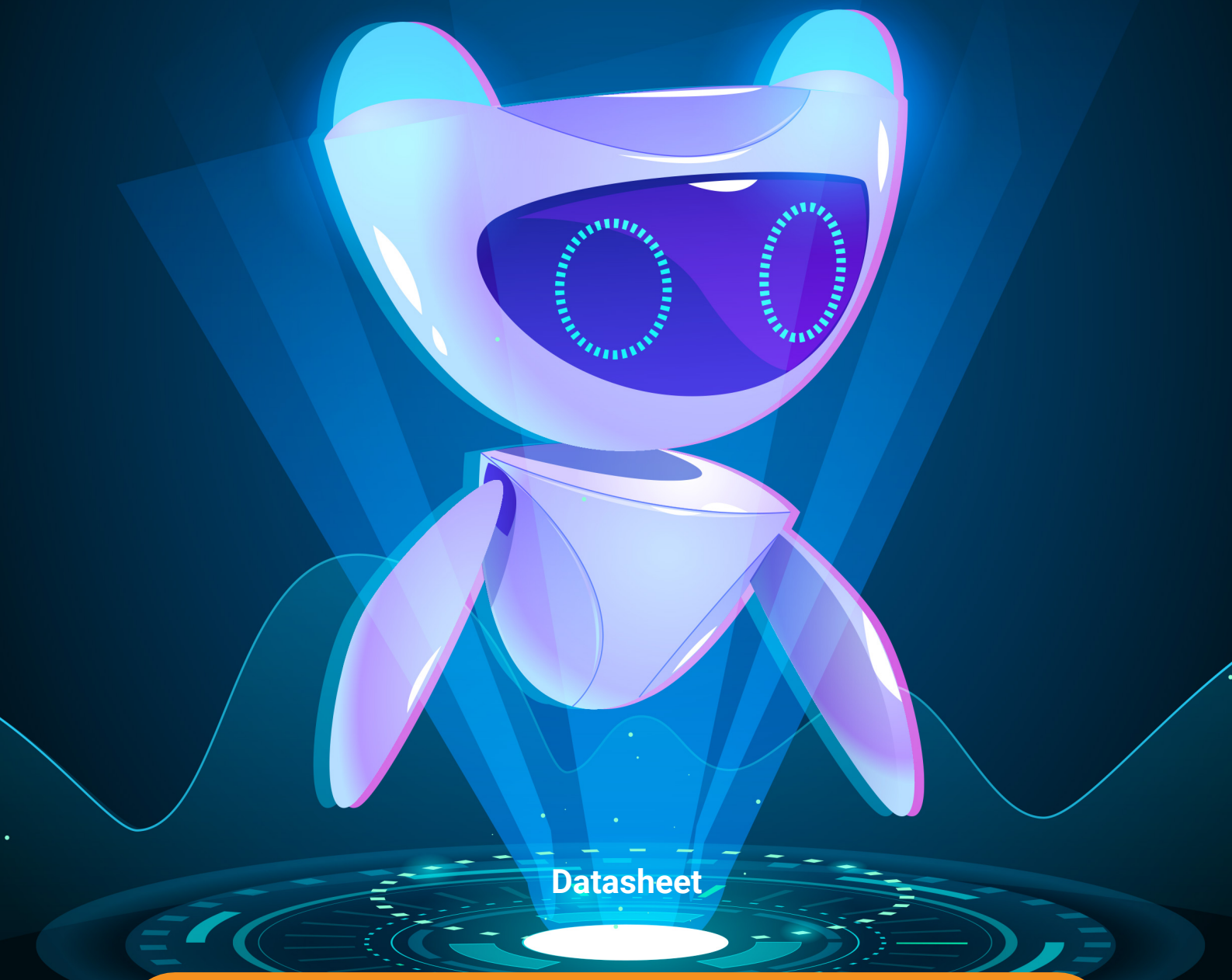
CYBOT™

Automated Investigation & Hunting Platform



Datasheet

Analytics Package

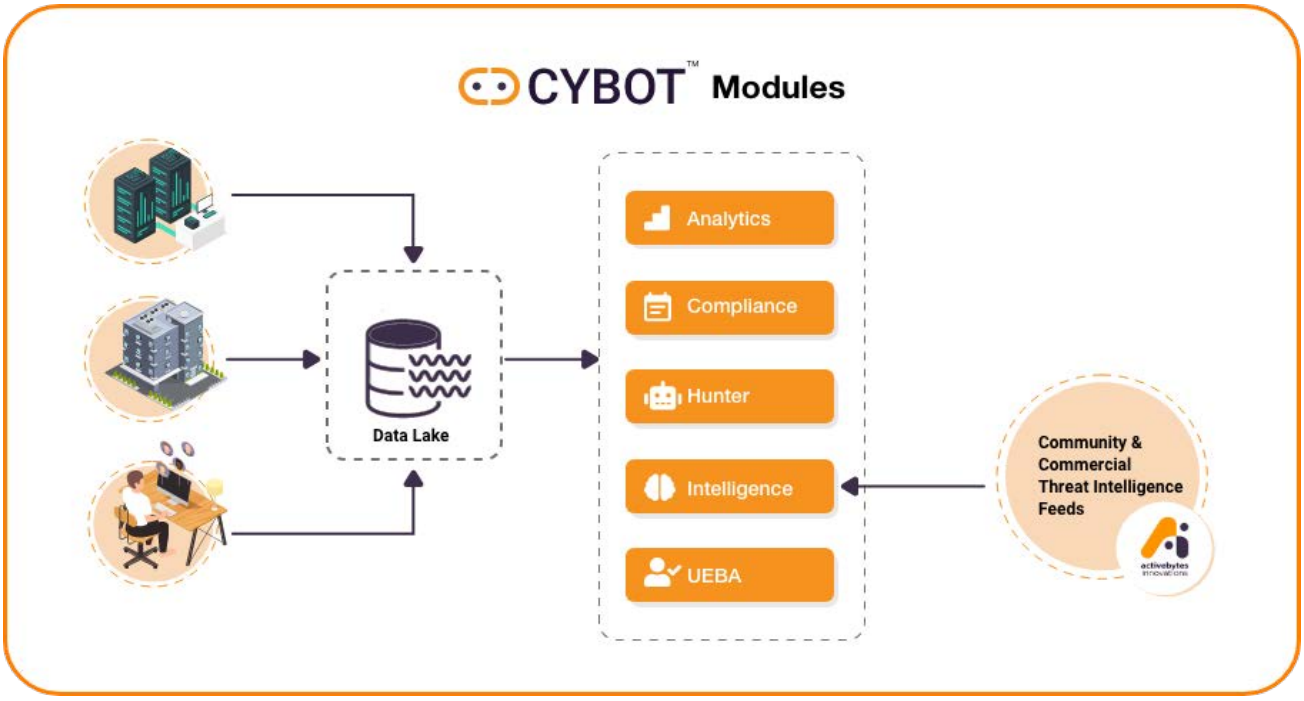
activebytes innovations

www.active-bytes.com

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™

Why CYBOT™ is Your Intelligent Analytical Threat Hunting Solution?

CYBOT™ Platform includes a Big Data Analytic Engine that handles huge data which is beyond human ability, with best-in-class analytics and processing capability. We've made hundreds of dashboards and alerts out of the box for both compliance and security analytics purposes. You will have additional access to our content library that we keep updating with new dashboards and alerts to continuously improve the hunting capability of the platform.

CYBOT™ protects your assets

Analytics

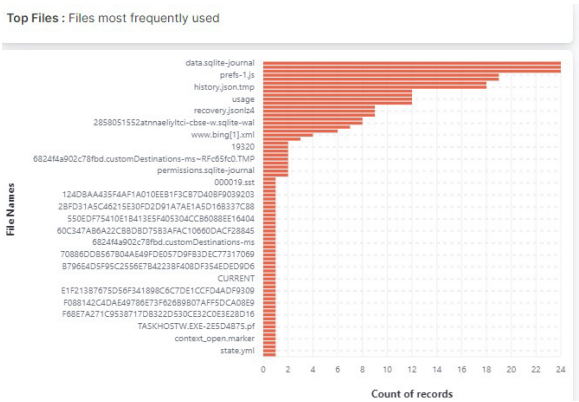
CYBOT™, with its advanced analytics design, performs quick profiling of raw data into useful information, analysis of this along with events patterns in the enterprise environment and helps in proactive handling of IOCs, thereby saving the enterprise IT infrastructure from a security breach. CYBOT™ is capable of early detection of even the new generation-based attack attempts with its huge pool of IOCs and pattern recognition capability. The observations that are available as dashboards and the panels with data at granular level allow analysts to quickly neutralize the threat element that breached their defence systems.

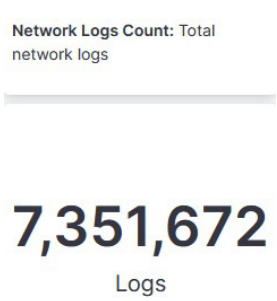
Some other features include

- Huge Data extraction from OS, system behaviour, communication between systems and to external IP addresses, common user behaviour
- Analysis of logs of OS binaries execution and registry changes
- Extraction of data related to file creation, deletion and modification activities, other system/ application logs

Advanced Analytics handles even the modern technology-based attack techniques

Data from the hosts and servers will be ingested to CYBOT™ and every manually hard to detect unusual logs, IOCs are subjected to detailed analysis.





Data from the network is ingested to CYBOT™ and any malicious attempt to damage or abuse the organization network infrastructure is quickly detected and notified.

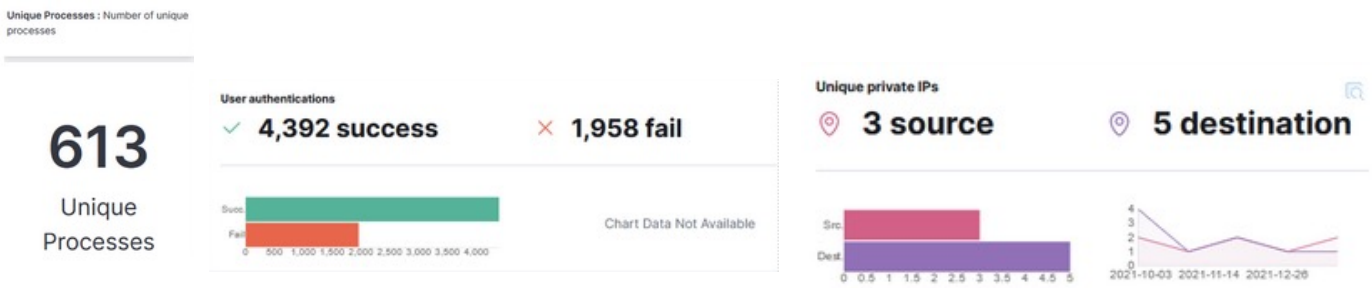
Some other features include

- Can extracts rich logs from the network and feed them to the data-lake.
- Capable of extracting domain lookups, communication logs irrespective of TCP/IP Protocols.
- Capture high fidelity transaction logs in the network and traffic across the network
- Capable of capturing file-content metadata, to and fro traffic from both internal and external critical systems.
- More capable to handle east-west traffic to detect and investigate new generation attacks.
- Capable of extracting and processing major Microsoft protocols used by active directories.
- Analytics engine supports industry-standard encryption for communication and necessary access controls, thereby keeping enterprise logs safeguarded.

The Analytics engine can analyze not only the known IOCs but also patterns from events. Thereby detects adversary acts like a user id or password abuse by correlating the user's typical behavioural pattern with the newly detected pattern.

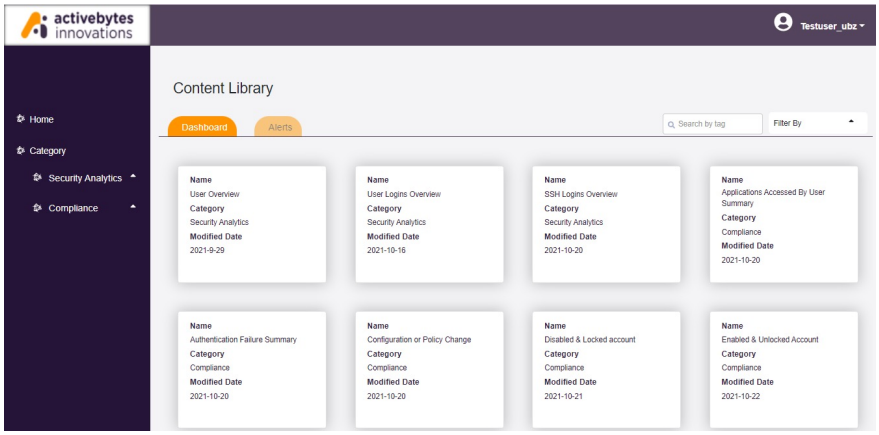
Analytics Dashboards and Use-case Alerts

- CYBOT™ is capable of drilling down to the granular level of events which the security team can easily access and analyze, thereby prevent further damage from the adversary.
- Effective co-relation capabilities on specific data from the network and host data extractors and hence the advanced threats that go undetected by a human threat hunter are not missed.
- Faster reports and Dashboard generation for historical data helping in faster decision making.
- Enhanced visibility of user management activities across the infrastructure at Directory and Host level, thereby preventing abuse by insiders.
- 100+ Pre-built dashboards to review logs against compliance standards such as ISO27K, PCI-DSS, NIST
- Reports can be generated, and is available in technical and non-technical formats.
- Early detection of emerging threats gives sufficient time for analysts to defend the enterprise network.
- Major functions supported by APIs.
- Integrates with thecompany's baseline without affecting the network or IT architecture.
- Collects, analyze, and generate alerts on every quality IOCs, including Malicious files, URLs, Domains, IPs, Filenames/hashes, Malware families.



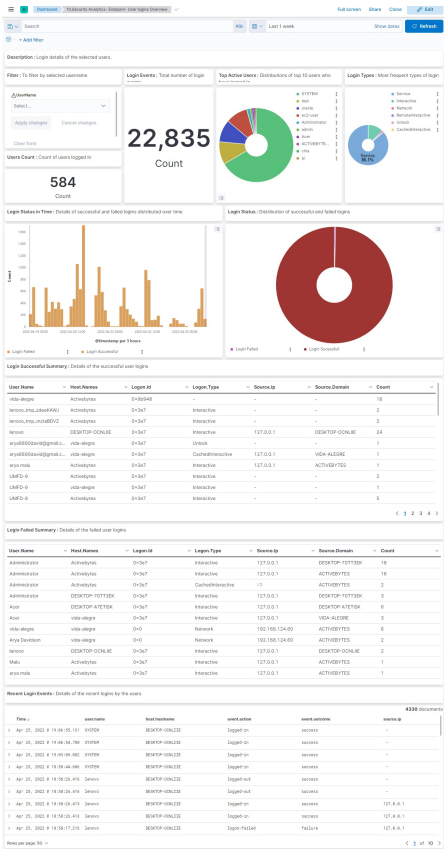
Additional access to our content-library portal where new Dashboards & Alerts are added

- Hundreds of Dashboards and Alerts for both compliance and security analytics. Hence covering a wide range of use cases with huge data, in a user-friendly manner.
- Faster understanding of huge data for analysts as automated analysis is performed on logs to the granular level. This saves time for analysts to focus on other critical tasks.
- Host and Network data visualization in a user-friendly manner. This makes understanding easier for non-technical personnel.
- Easy understanding of group management activities and enumerations on every data related to it.
- Co-relation Alert use-cases for new vulnerabilities and threats, make the platform gets updated with the latest adversary techniques.

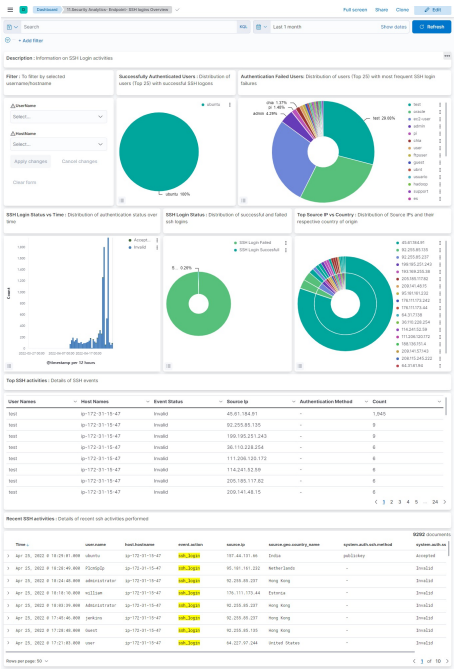


User friendly guides explaining the steps to access the platform, installation, content library, etc.

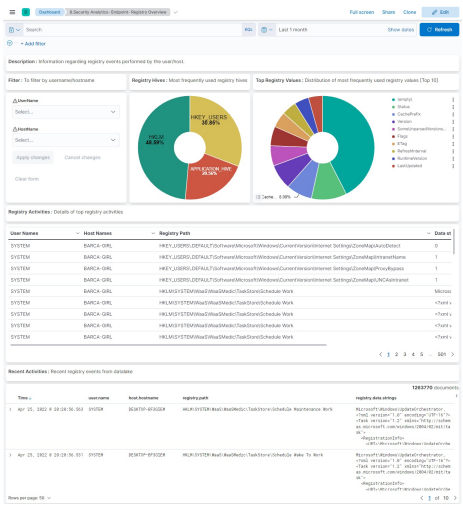
SAMPLE DASHBOARDS (Security & Compliance)



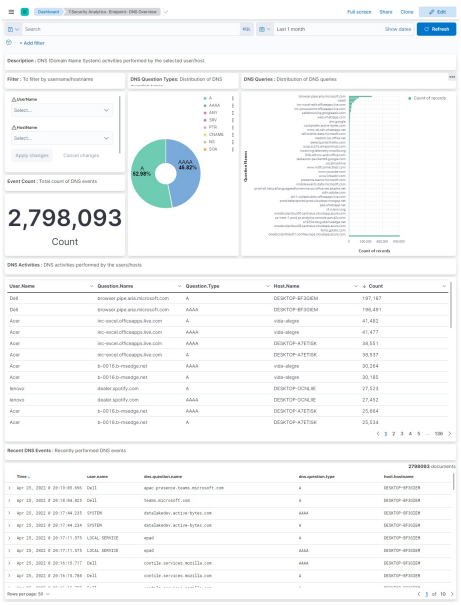
This security analytics dashboard displays login events performed by users in the organization,.



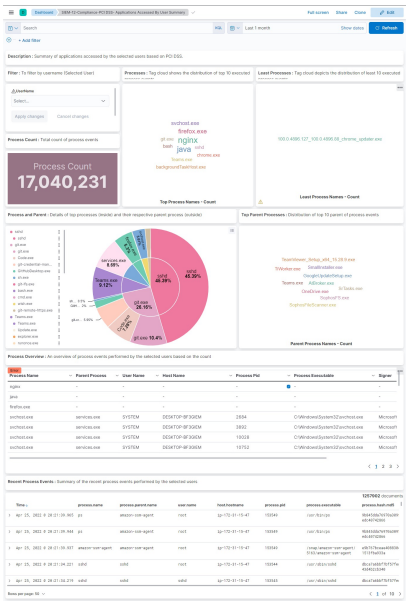
This security analytics dashboard displays information related to events SSH login events performed by users/hosts in the organization,.



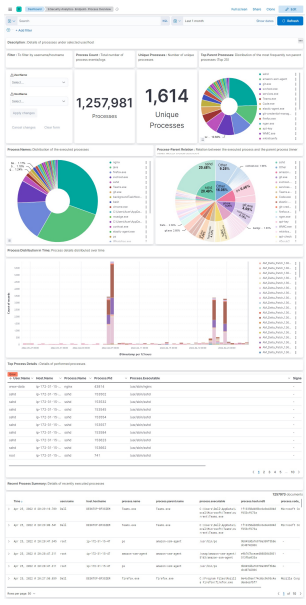
This security analytics dashboard displays registry events performed by users/hosts in the organization



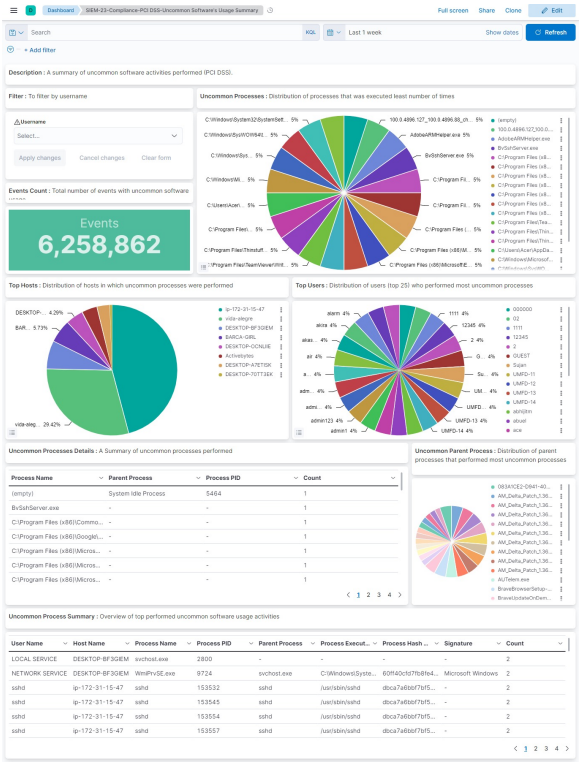
This security analytics dashboard shows the DNS (Domain Name System) activities performed by the selected user/host.



Summary of applications accessed by the selected users for PCI-DSS compliance.

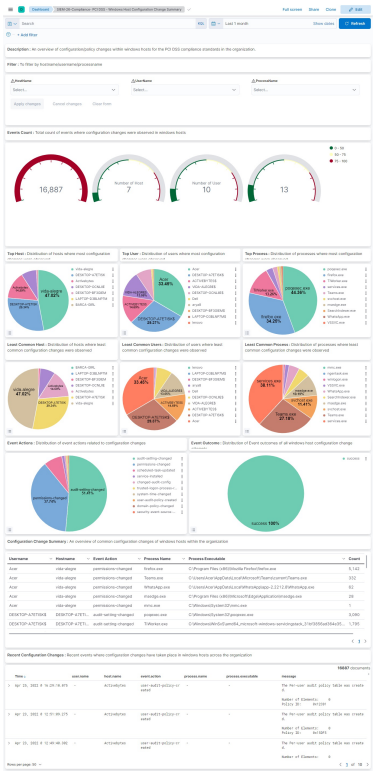


This security analytics dashboard gives details of processes under selected user/host.

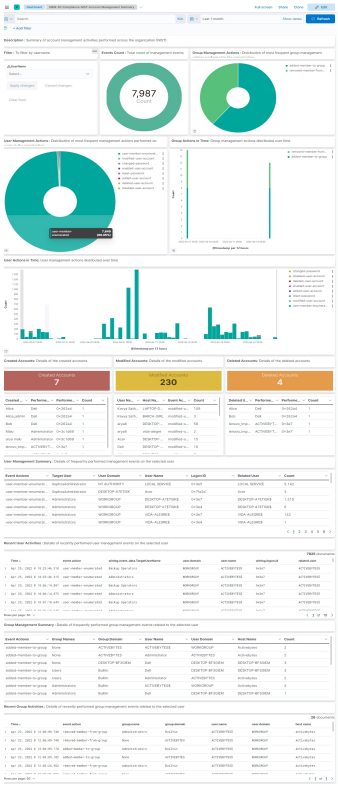


Summary of uncommon software activities performed for PCI- DSS compliance.

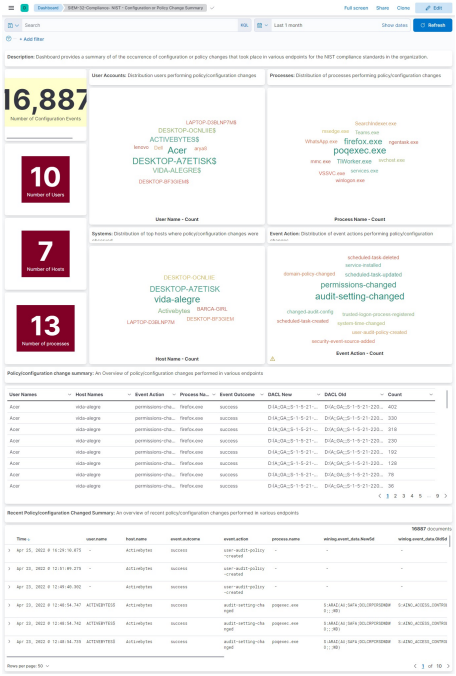
An overview of windows firewall policy modification events for the PCI DSS compliance standards in the organization.



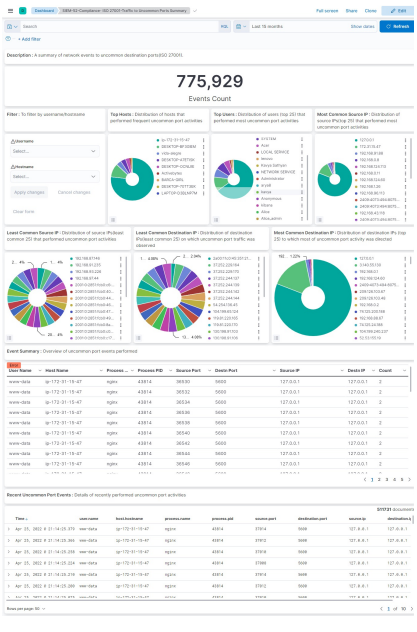
An overview of configuration/policy changes in windows hosts for the PCI DSS compliance standards in the organization.



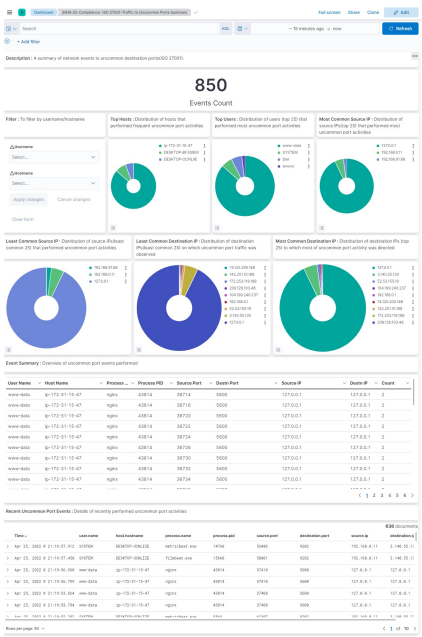
Summary of account management activities performed across the organization for NIST compliance.



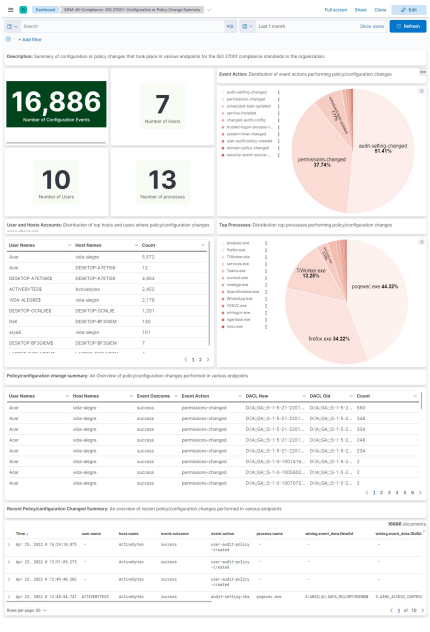
Summary of configuration or policy changes occurred in various endpoints for the NIST compliance standards in the organization.



Summary of Internet traffic activities performed, ISO 27001 compliance



A summary of network events to uncommon destination ports, ISO 27001



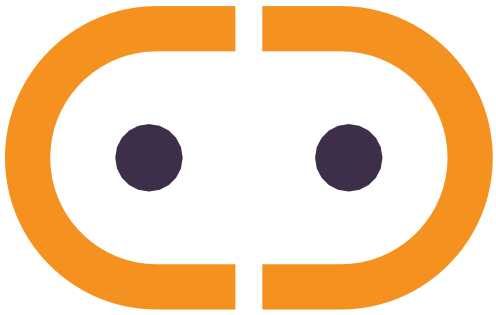
An overview of configuration/policy changes within windows hosts for the ISO 27001 compliance standards in the organization.

List of few Dashboards from the hundreds of available use-cases
Dashboard and report to analyse Account Management Summary
Dashboard and report to analyse Authentication Failure Summary
Dashboard and report to analyse Default Act Auth/Access Failure Summary
Dashboard and report to analyse Default Act Auth/Access Success Summary
Dashboard and report to analyse Default Act Management Summary
Dashboard and report to analyse Disabled & Locked Account Summary
Dashboard and report to analyse Enabled & Unlocked Account Summary
Dashboard and report to analyse Priv Act Auth/Accs Failure Summary
Dashboard and report to analyse Priv Act Auth/Accs Success Summary
Dashboard and report to analyse Priv Act Management Summary
PCI DSS Compliance
Dashboard and report to analyse Host Configuration Change Summary
Dashboard and report to analyse Applications Accessed By User Summary
Dashboard and report to analyse Authentication Failure Summary
Dashboard and report to analyse Configuration or Policy Change Summary
Dashboard and report to analyse Data Transfer Summary
Dashboard and report to analyse Disabled & Locked Account Summary
Dashboard and report to analyse Enabled & Unlocked Account Summary
Dashboard and report to analyse File Integrity Monitor Log Summary
Dashboard and report to analyse Accounts Modification Summary
Dashboard and report to analyse Traffic to internet Summary
Dashboard and report to analyse Traffic to uncommon ports Summary
Dashboard and report to analyse Windows Firewall Change Summary
Dashboard and report to analyse User Privilege Escalation (SU & SUDO)
Dashboard and report to analyse Rejected Connection to Network
Dashboard and report to analyse Uncommon softwares usage summary
Dashboard and report to analyse Use of Non-Encrypted Protocols
Dashboard and report to analyse File Monitoring Event-File Changes
Dashboard and report to analyse Software Installed Summary
Dashboard and report to analyse Windows Host Configuration Change Summary
Dashboard and report to analyse User Privilege Escalation (Windows) Summary
Dashboard and report to analyse Account Management Summary

NIST Compliance
Dashboard and report to analyse Host Configuration Change Summary
Dashboard and report to analyse User Privilege Escalation (SU & SUDO)
Dashboard and report to analyse Applications Accessed By User Summary
Dashboard and report to analyse Account Management Summary
Dashboard and report to analyse Authentication Failure Summary
Dashboard and report to analyse Configuration or Policy Change Summary Dashboard and report to analyse Data Transfer Summary
Dashboard and report to analyse Disabled & Locked Account Summary
Dashboard and report to analyse Enabled & Unlocked Account Summary
Dashboard and report to analyse File Integrity Monitor Log Summary
Dashboard and report to analyse Accounts Modification Summary
Dashboard and report to analyse Traffic to internet Summary
Dashboard and report to analyse Traffic to uncommon ports Summary
Dashboard and report to analyse Windows Firewall Change Summary
Dashboard and report to analyse User Privilege Escalation (Windows) Summary
Dashboard and report to analyse Rejected Connection to Network
Dashboard and report to analyse Uncommon softwares usage summary
Dashboard and report to analyse Use of Non-Encrypted Protocols
Dashboard and report to analyse File Monitoring Event-File Changes
Dashboard and report to analyse Software Installed Summary
Dashboard and report to analyse Windows Host Configuration Change Summary
ISO 27001 Compliance
Dashboard and report to analyse Host Configuration Change Summary
Dashboard and report to analyse Account Management Summary
Dashboard and report to analyse Authentication Failure Summary
Dashboard and report to analyse Configuration or Policy Change Summary
Dashboard and report to analyse Data Transfer Summary
Dashboard and report to analyse Disabled & Locked Account Summary
Dashboard and report to analyse Enabled & Unlocked Account Summary
Dashboard and report to analyse File Integrity Monitor Log Summary
Dashboard and report to analyse Accounts Modification Summary
Dashboard and report to analyse Traffic to internet Summary
Dashboard and report to analyse Traffic to uncommon ports Summary
Dashboard and report to analyse Windows Firewall Change Summary
Dashboard and report to analyse Applications Accessed By User Summary
Dashboard and report to analyse Rejected Connection to Network

Dashboard and report to analyse Uncommon softwares usage summary
Dashboard and report to analyse File Monitoring Event-File Changes
Dashboard and report to analyse Use of Non-Encrypted Protocols
Dashboard and report to analyse Software Installed Summary
Dashboard and report to analyse Windows Host Configuration Change Summary
Dashboard and report to analyse User Privilege Escalation (Windows) Summary
Dashboard and report to analyse User Privilege Escalation (SU & SUDO)

List of few Aerts from the hundreds of available use-cases
Account Access Revoked
Account Disabled Rule
Account Locked Rule
Configuration or Policy Change
Data Destruction Rule
Non-Admin Linux Rule
Non-Admin Windows Rule
Windows Firewall Change
Privilege account Access Failure Rule
Privileged Account Authentication Failure Rule
Priv Group Access Granted Rule
Recent Disable Acct + Acs Fail
Recent Disable Acct + Acs Success
System Time Change
Time Sync Error
Default Account Access Failure Rule
Default Account Auth Failure Rule
Data Loss Prevention Rule



activebytes innovations

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