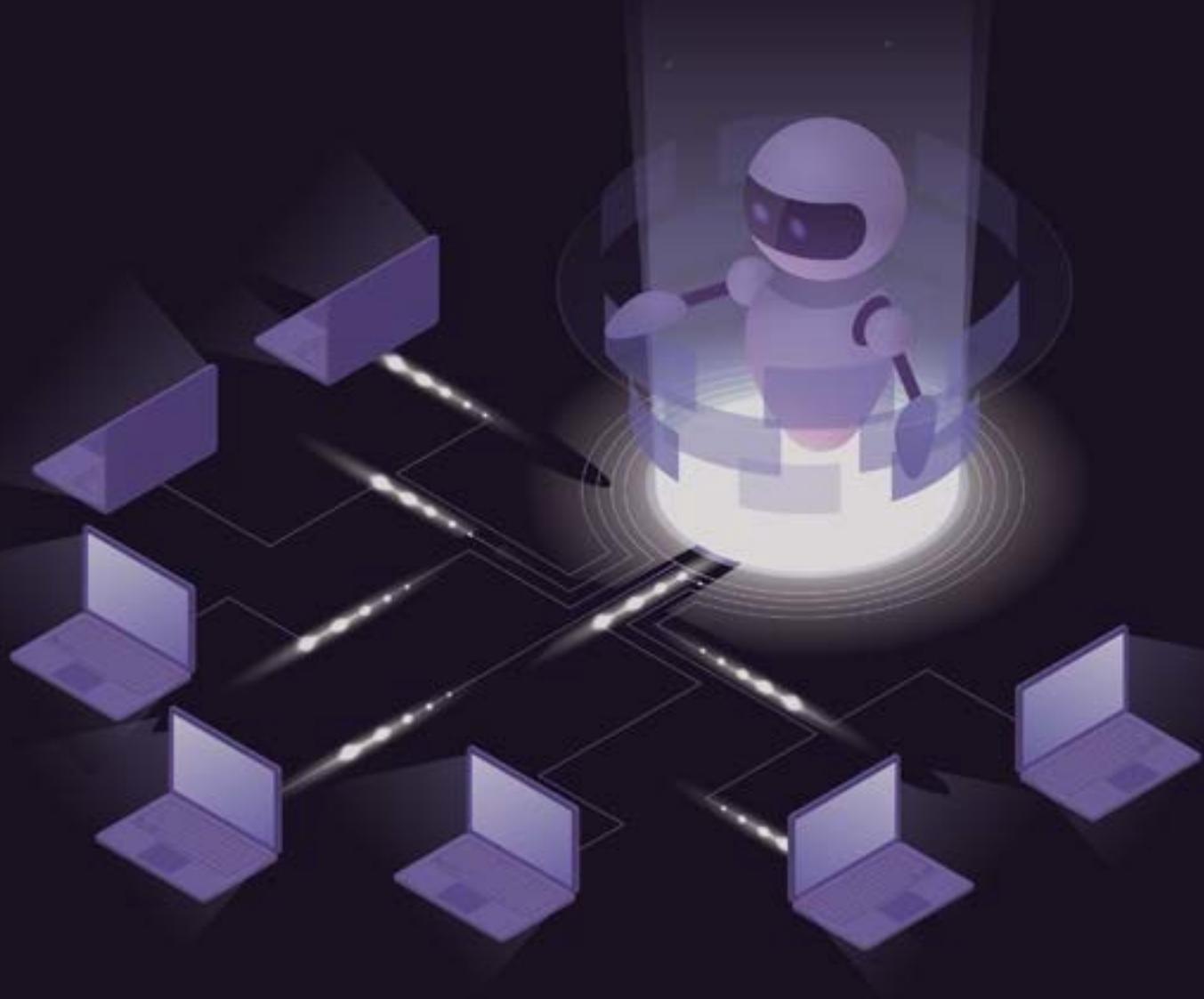




Automated Investigation & Hunting Platform



Datasheet

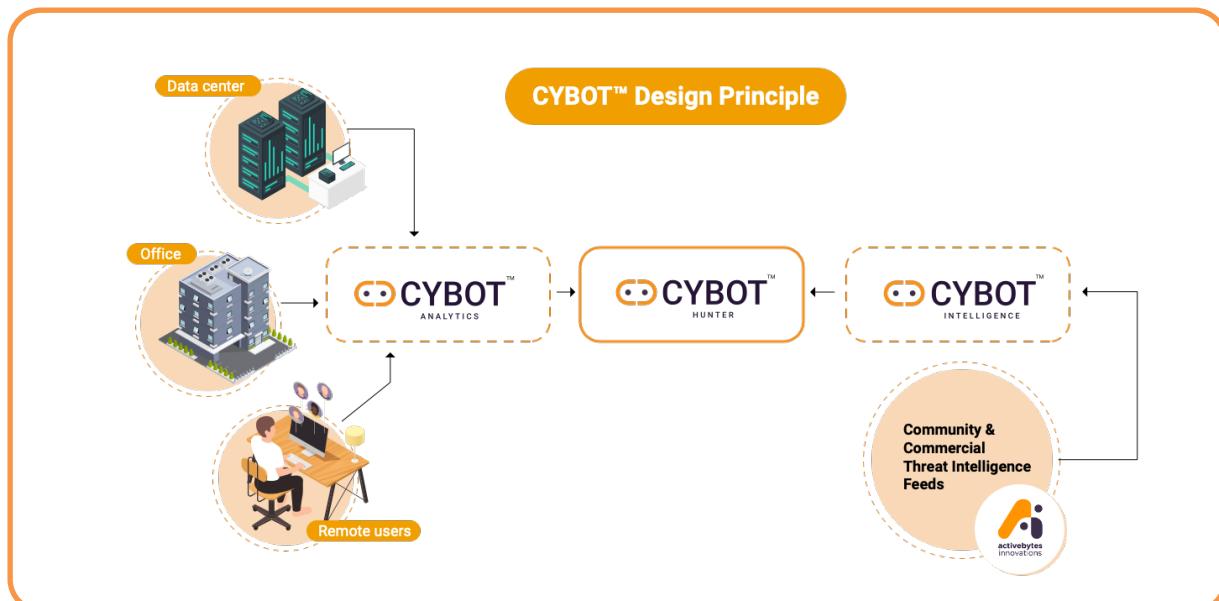
## Analytics Package



[www.active-bytes.com](http://www.active-bytes.com)

# About the CYBOT™

- CYBOT™ collects raw logs from the enterprise's network, remote users, servers and stores to its Analytical engine in a contextualized and secured way. The logs then undergo intelligent automatic analysis, thereby going the extra mile in threat hunting which a human cannot.
- CYBOT™ is designed to be adaptive to the latest adversary techniques and tactics by keeping in track with the threat intelligence events that it is programmed to receive from our trusted community sources and Activebytes dedicated threat intelligence team.
- CYBOT™ intelligently and automatically hunts and investigates the threat leveraging Realtime Logs by performing correlation with TI IOCs received from even the dark sources, thereby detecting adversary attack patterns that a human can never pickup.
- Around the clock monitoring of logs and every unusual, suspected event is subjected to drill down the level of investigation. CYBOT™ is designed to provide automated options to respond along with suggestions and alerts to the security team. This will help analysts to deal with the adversaries that already intruded on the network.



[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

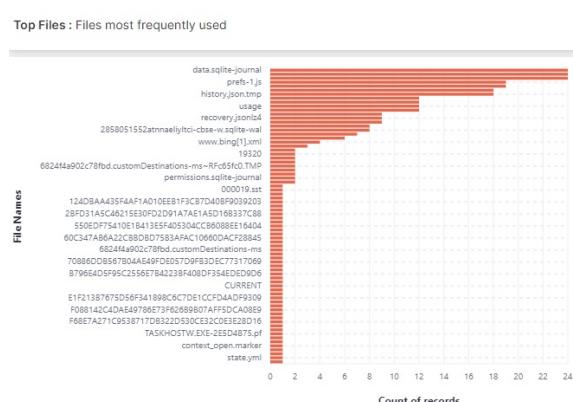
# Analytics

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.

**Network Logs Count:** Total network logs

**7,351,672**  
Logs



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.

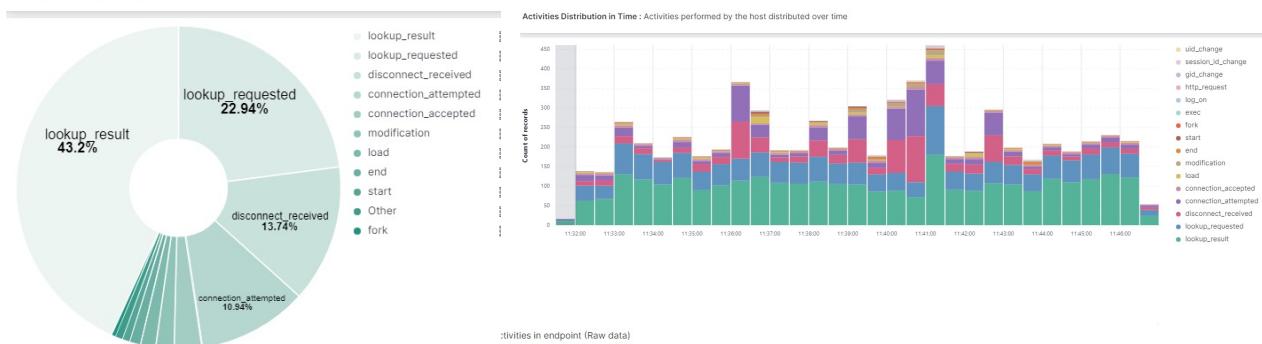
## Some other features include

- Can extract 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.

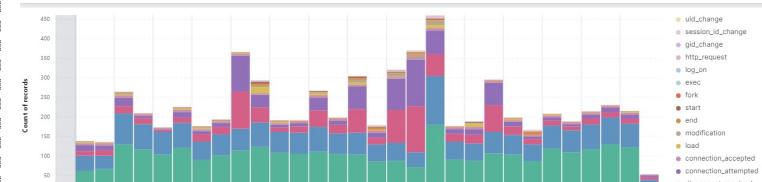


The Analytics engine can analyze not only the known IOCs but also patterns from events. Thereby detects adversary acts like a user id or password abuse by correlating the user's typical behavioural pattern with the newly detected pattern.

Event Actions : Distribution of the event actions



Activities Distribution in Time : Activities performed by the host distributed over time



Activities in endpoint (Raw data)

| Time                          | Document                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| > Apr 25, 2022 @ 11:38:39.290 | event.category: network #timestamp: Apr 25, 2022 @ 11:38:39.290 agent.id: c4df7206-f3bf-4aeb-957b-2121620f5a56 agent.type: endpoint agent.version: 7.15.1 data_stream.dataset: endpoint.events.network data_stream.namespace: default data_stream.type: logs dns.Ext.options: 4294967295 dns.question.name: b-0016.b-msedge.net dns.question.type: AAAA ecs.version: 1.11.0 elastic.agent.id: c4df7206-f3bf-4aeb-957b-2121620f5a56 event.action: lookup_result event.agent_id_status: verified event.created: Apr 25, 2022 @ 11:38:39.290 event.dataset: endpoint.events.network event.id: K2y10Btcr846504****001 event.ingested: Apr 25, 2022 @ 11:38:44.000 event.kind: event |
| > Apr 25, 2022 @ 11:38:39.289 | event.category: network #timestamp: Apr 25, 2022 @ 11:38:39.289 agent.id: c4df7206-f3bf-4aeb-957b-2121620f5a56 agent.type: endpoint agent.version: 7.15.1 data_stream.dataset: endpoint.events.network data_stream.namespace: default data_stream.type: logs dns.Ext.options: 4294967295 dns.question.name: inc-word-edit.officeapps.live.com dns.question.type: AAAA ecs.version: 1.11.0 elastic.agent.id: c4df7206-f3bf-4aeb-957b-2121620f5a56 event.action: lookup_result event.agent_id_status: verified event.created: Apr 25, 2022 @ 11:38:39.289 event.dataset: endpoint.events.network event.id: K2y10Btcr846504****001 event.ingested: Apr 25, 2022 @ 11:38:44.000     |
| > Apr 25, 2022 @ 11:38:39.289 | event.category: network #timestamp: Apr 25, 2022 @ 11:38:39.289 agent.id: c4df7206-f3bf-4aeb-957b-2121620f5a56 agent.type: endpoint agent.version: 7.15.1 data_stream.dataset: endpoint.events.network data_stream.namespace: default data_stream.type: logs dns.Ext.options: 4294967295 dns.question.name: b-0016.b-msedge.net dns.question.type: A ecs.version: 1.11.0 elastic.agent.id: c4df7206-f3bf-4aeb-957b-2121620f5a56 event.action: lookup_result event.agent_id_status: verified event.created: Apr 25, 2022 @ 11:38:39.289 event.dataset: endpoint.events.network event.id: K2y10Btcr846504****001 event.ingested: Apr 25, 2022 @ 11:38:44.000                      |

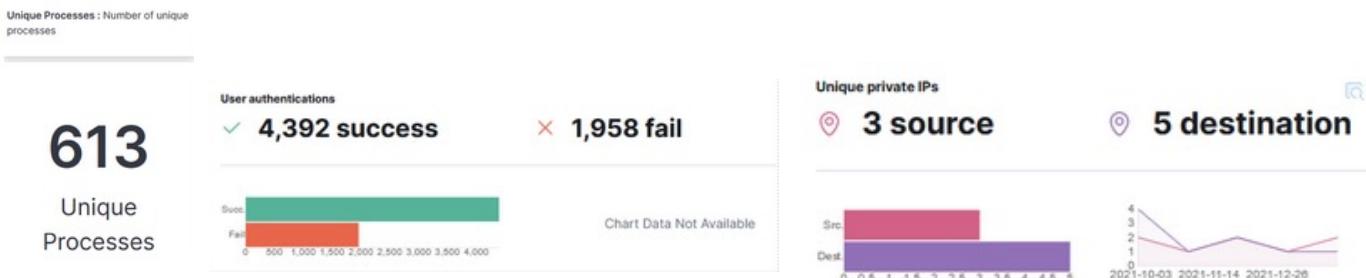
Rows per page: 50 >

3716 documents

1 of 10 >

# 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 the company'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.

The screenshot shows the 'Content Library' section of the platform. It displays a grid of eight cards, each representing a different report or overview:

- User Overview**: Modified Date 2021-9-29
- User Logins Overview**: Modified Date 2021-10-16
- SSH Logins Overview**: Modified Date 2021-10-20
- Applications Accessed By User Summary**: Modified Date 2021-10-20
- Authentication Failure Summary**: Modified Date 2021-10-20
- Configuration or Policy Change**: Modified Date 2021-10-20
- Disabled & Locked account**: Modified Date 2021-10-21
- Enabled & Unlocked Account**: Modified Date 2021-10-22



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

## SAMPLE DASHBOARDS (Security & Compliance)

**Logins Overview Dashboard:**

- Key Metrics:** Total number of logins (22,835), Count of users logged in (584).
- Visualizations:** Donut chart of Top Active Users (Distribution of top 50 users who have logged in) and Logon Types (Most frequent types of login).
- Data Tables:** Logins Status vs Time (Details of successful and failed logins distributed over time) and Logon Success Summary (Details of the successful user logins).

**Registry Events Dashboard:**

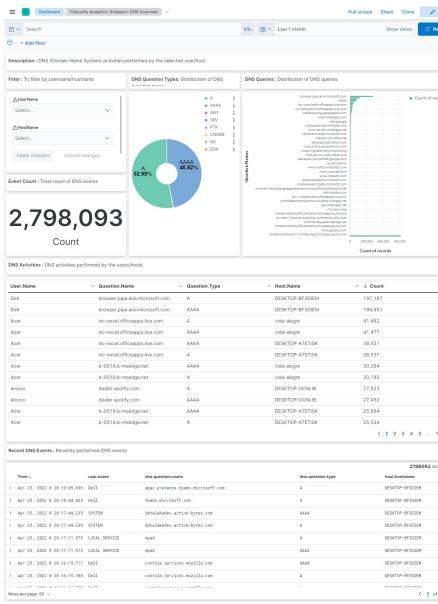
- Key Metrics:** SuccessFully Authenticated Users (Distribution of users (Top 20) with successful logins) and Authentication Failed Users (Distribution of users (Top 20) with failed login attempts).
- Visualizations:** Donut chart of Registry Events (Top Registry Events) and Registry Status vs Time (Distribution of authentication status over time).
- Data Tables:** Registry Activities (Details of top registry activities) and Recent Activities (Recent registry events from database).

**SSH Login Events Dashboard:**

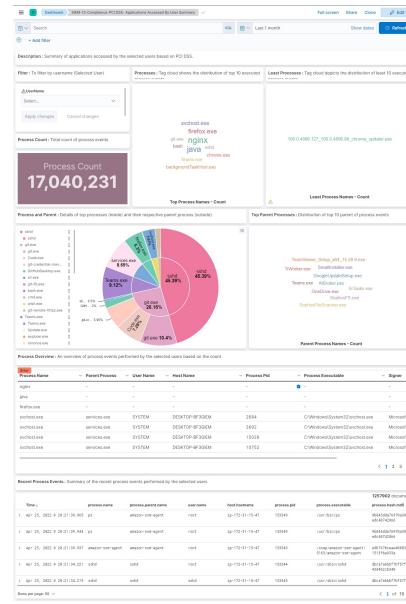
- Key Metrics:** SSH Login Status (Distribution of successful and failed logins).
- Visualizations:** Donut chart of Top Source IP vs Country (Distribution of source IP's and their respective country).
- Data Tables:** Recent SSH Activities (Recent SSH activities performed) and Recent Logon Events (Details of the recent logins by the users).

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

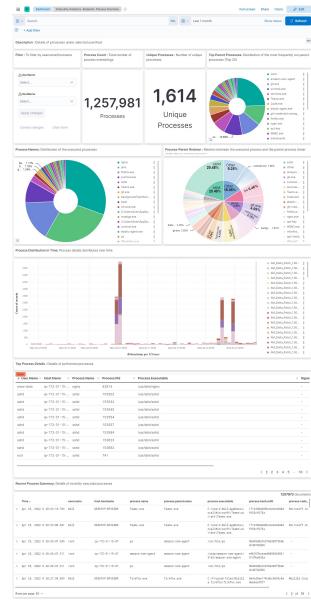
**This security analytics dashboard displays information related to events SSH login events performed by users/hosts in the organization.**



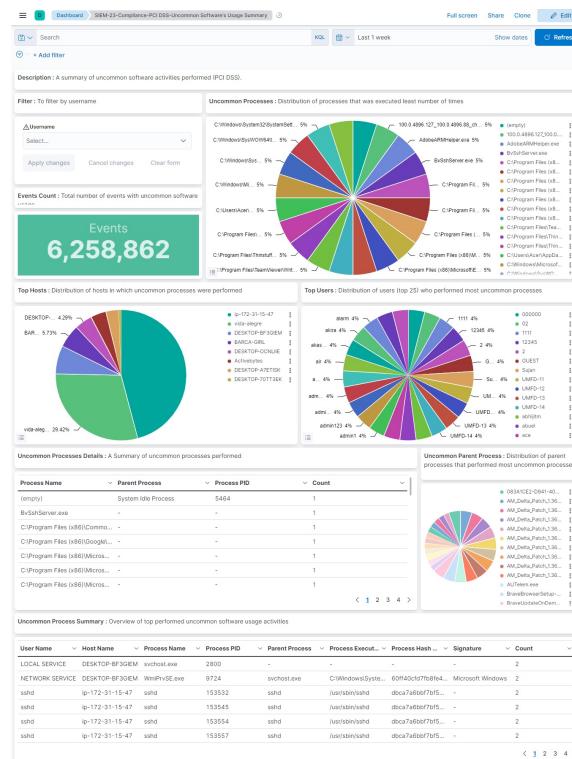
This security analytics dashboard shows the DNS (Domain Name System) activities performed by the selected user/host.



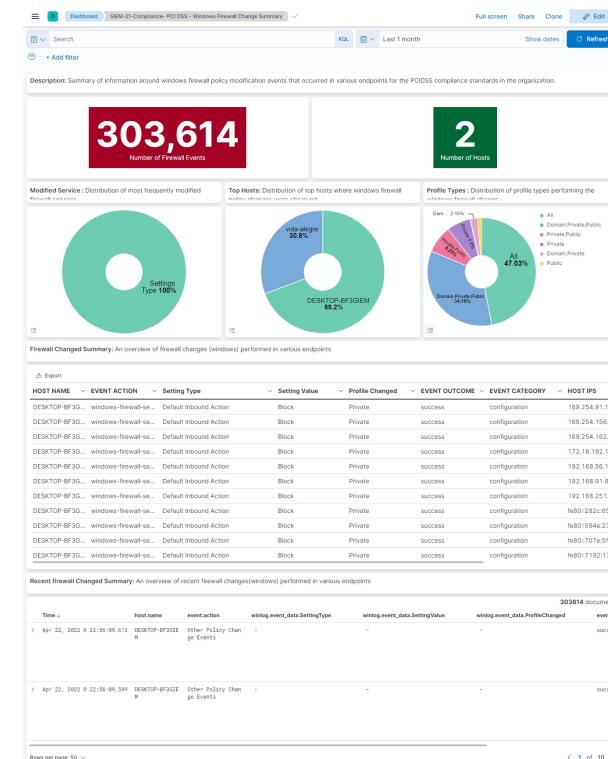
### *Summary of applications accessed by the selected users for PCI-DSS compliance.*



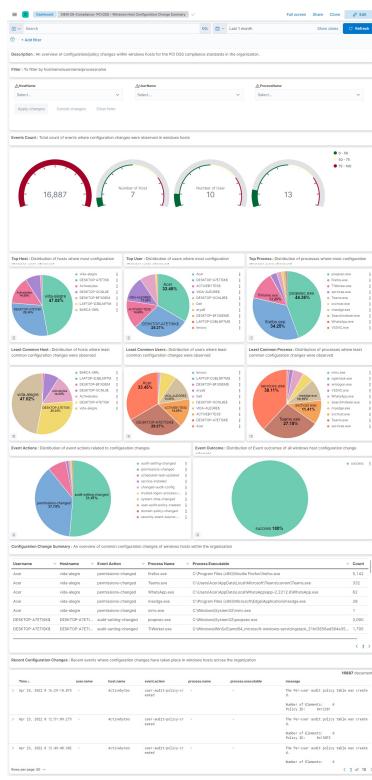
*This security analytics dashboard gives details of processes under selected user/host.*



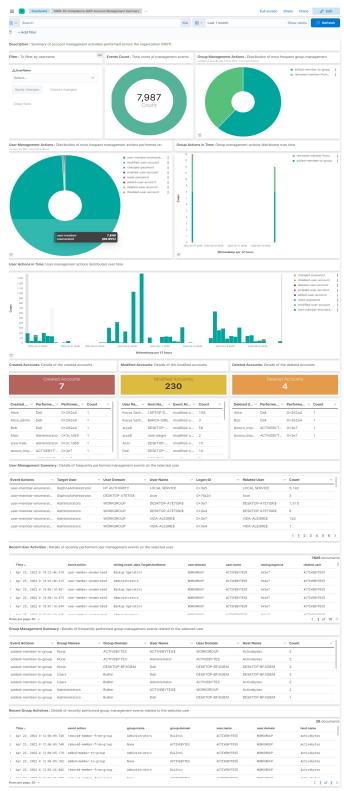
*Summary of uncommon software activities performed for PCI-DSS compliance.*



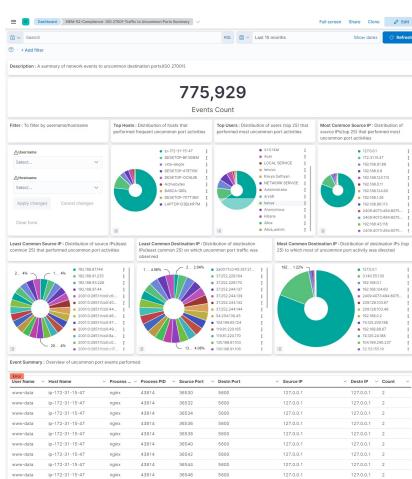
*An overview of windows firewall policy modification events for the PCI DSS compliance standards in the organization.*



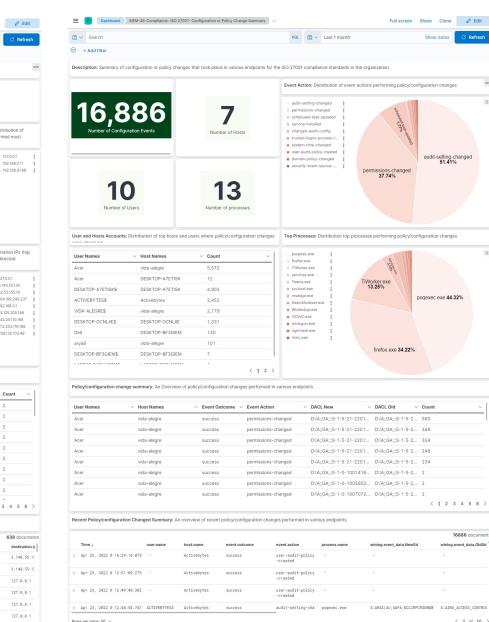
An overview of configuration/policy changes in windows hosts for the PCI DSS compliance standards in the organization.



**Summary of 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



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                 |
| <b>PCI DSS Compliance</b>                                                   |
| 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 Alerts 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](http://www.active-bytes.com) / [contact@active-bytes.com](mailto:contact@active-bytes.com)  
+971 50 513 3973

---