CYBOT HUNTER

Threat Hunting Platform

DATA SHEET

Dashboards

activebytes innovations

We've made hundreds of dashboard out of the box for both compliance and security analytics purposes on top of the data lake.

CONVENIENCE

- Capable of drilling down to granular level of events
- Faster understanding for analysts on huge volume of data – Look back to weeks, months or even years.
- **100+** Pre-built dashboards to review logs against compliance standards such as ISO27K, PCIDSS, NIST

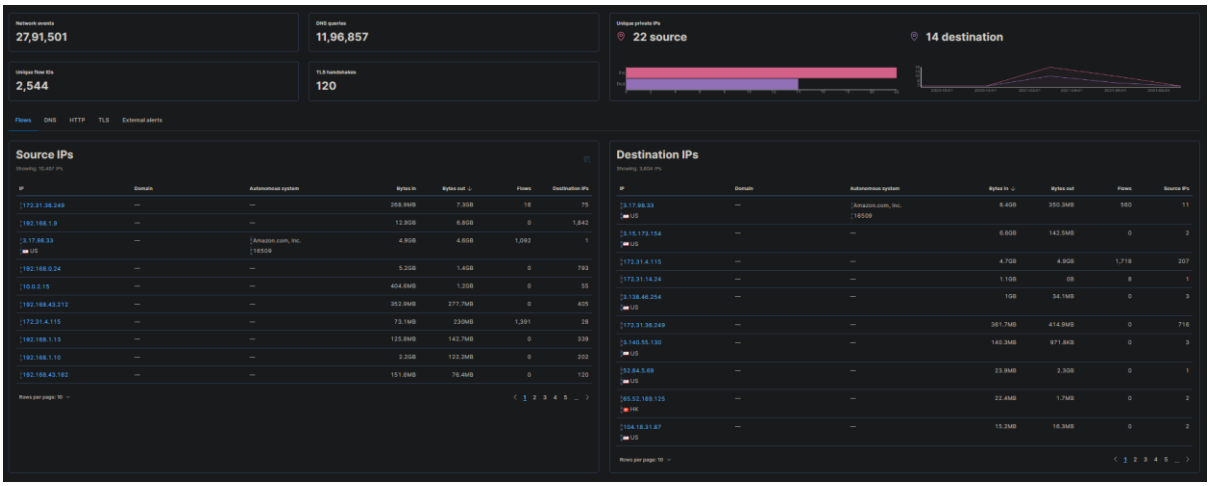
116-Compliance-NIST-Uncommon Software's Usage Summary	This dashboard gives details of uncommon software's used by users
117-Compliance-NIST- Use of Non-Encrypted Protocols	
118-Compliance- NIST- File Monitoring Event-File Changes	File activities performed by selected user/host
120-Compliance- NIST- Windows Host Configuration Change Summary	
122-Compliance- ISO-27001-Account Management Summary	Package-Compliance-Accountt Management Summary
123-Compliance-ISO-27001-Access and Authentication Failure Summary	This dashboard displays a summary of users with failed authentication.
126-Compliance-ISO-27001-Disabled & Locked account summary	A summary of Disabled & Locked accounts
127-Compliance- ISO 27001-Enabled & Unlocked Account Summary	A summary of enabled & unlocked account
129-Compliance-ISO 27001-Accounts Modification Summary	This dashboard displays a summary of account modification based on compliance.

- Access to the detailed and granular information for Threat Hunting team

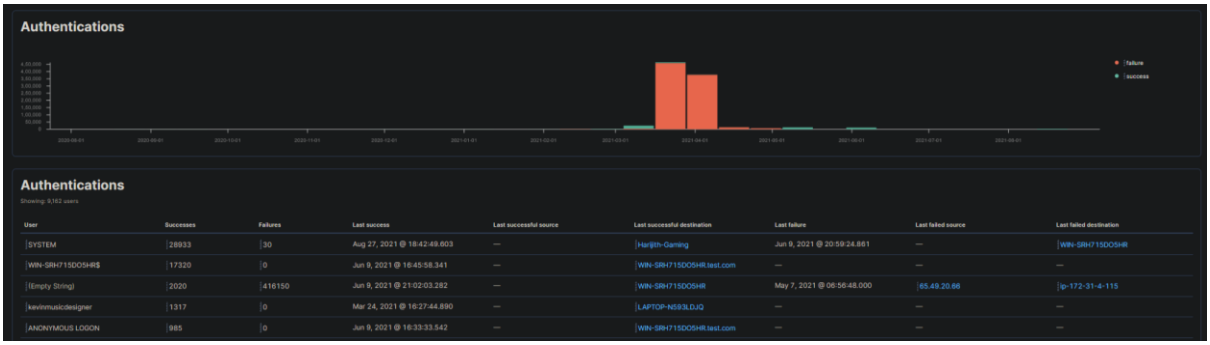
Recent Modification : Details of recent account modification events

```
A user account was changed.

Subject:
        Security ID:            S-1-5-18
        Account Name:           WIN-SRH715DO5HR$
        Account Domain:         TEST
        Logon ID:               0x3E7

Target Account:
        Security ID:            S-1-5-21-1176950347-982008390-404917063-1000
        Account Name:           Alice
        Account Domain:         TEST

Changed Attributes:
        SAM Account Name:       -
        Display Name:           -
        User Principal Name:    -
        Home Directory:         -
        Home Drive:             -
        Script Path:            -
        Profile Path:           -
        User Workstations:      -
        Password Last Set:      6/8/2021 4:01:42 PM
        Account Expires:                -
```

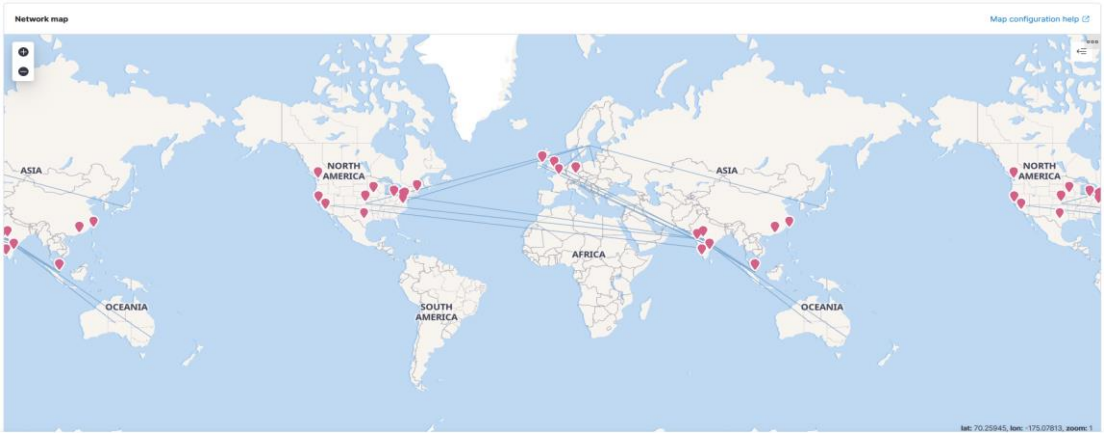
- Effective co-relation capabilities over detailed information provided by both network and host data extractors.
- Capability to investigate on user, host, network traffic and all activities around it with effective filtering and visualizations
- Faster reports and dashboard generation for longer historical data.
- Visualizes both host and network data



- visibility on all types of authentication failure and success activities occurred in the infrastructure

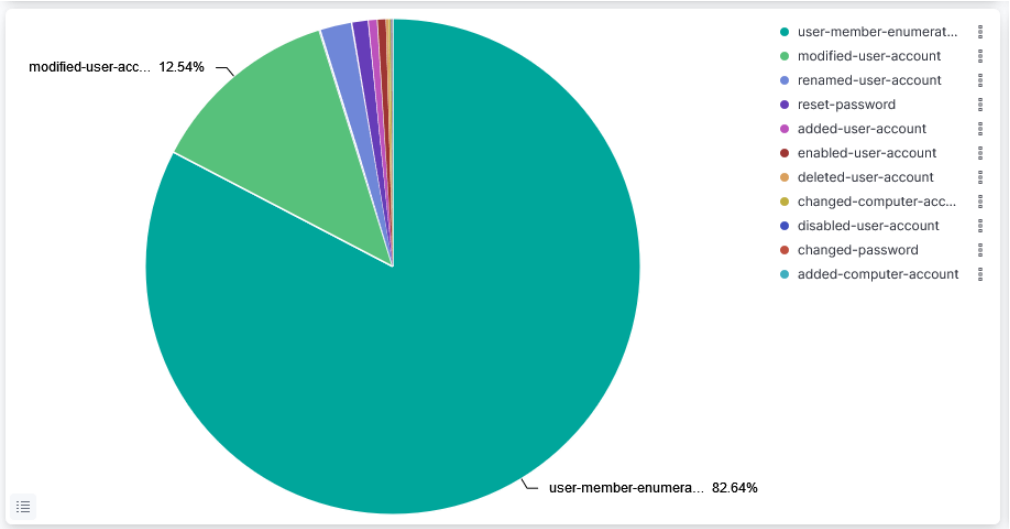


- In depth visibility on all file creation and modifications
- Visibility on web server activities on enterprise servers
- In depth view on operating system level executions and operations
- Enhanced visibility on network traffic



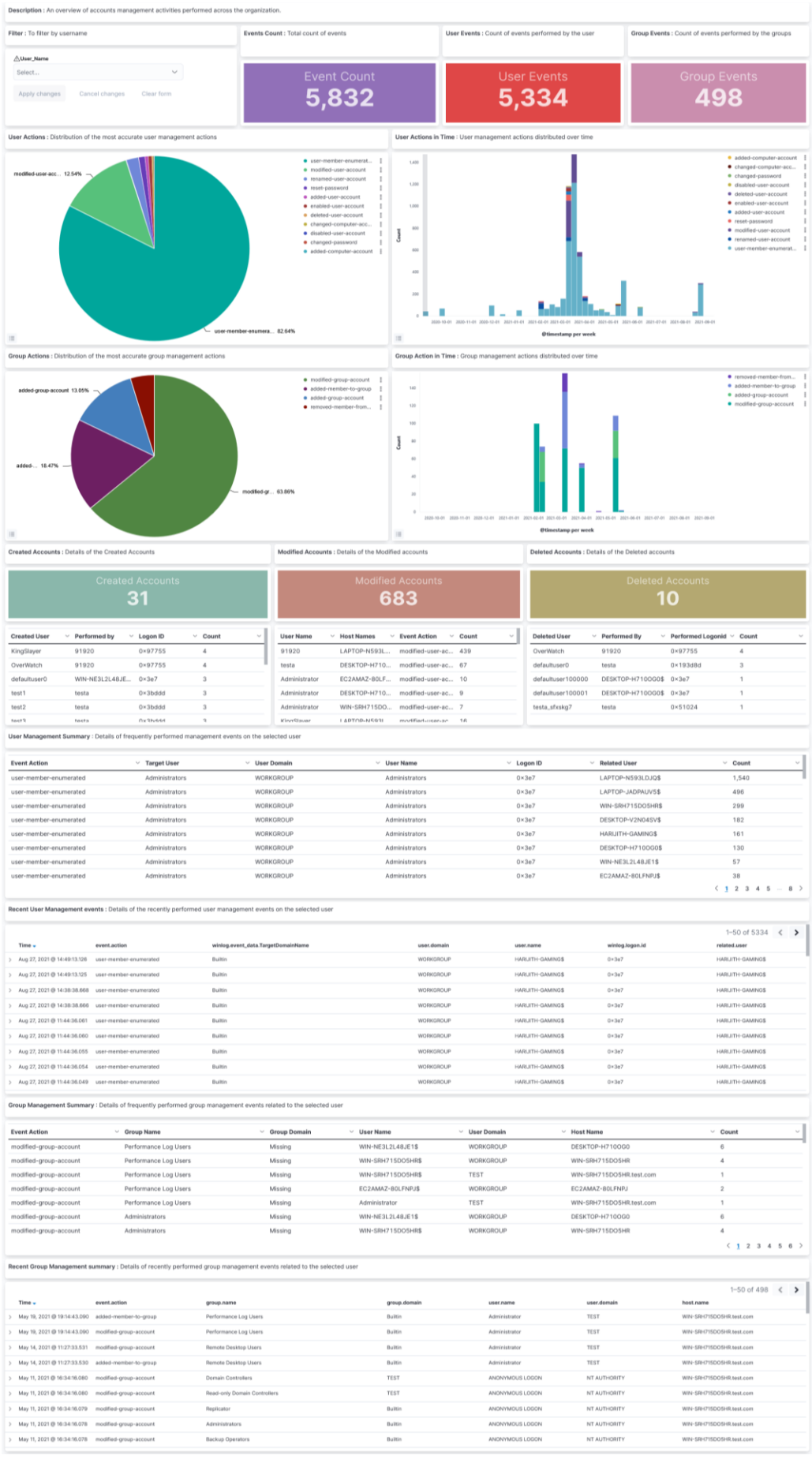
- Visibility on Microsoft network protocols activities occurred between active directory and end users
- Visibility on domain name lookups

- provide visibility on user management activities across the infrastructure on both Directory level and host level
- provide easy understanding on group management activities and enumerations.

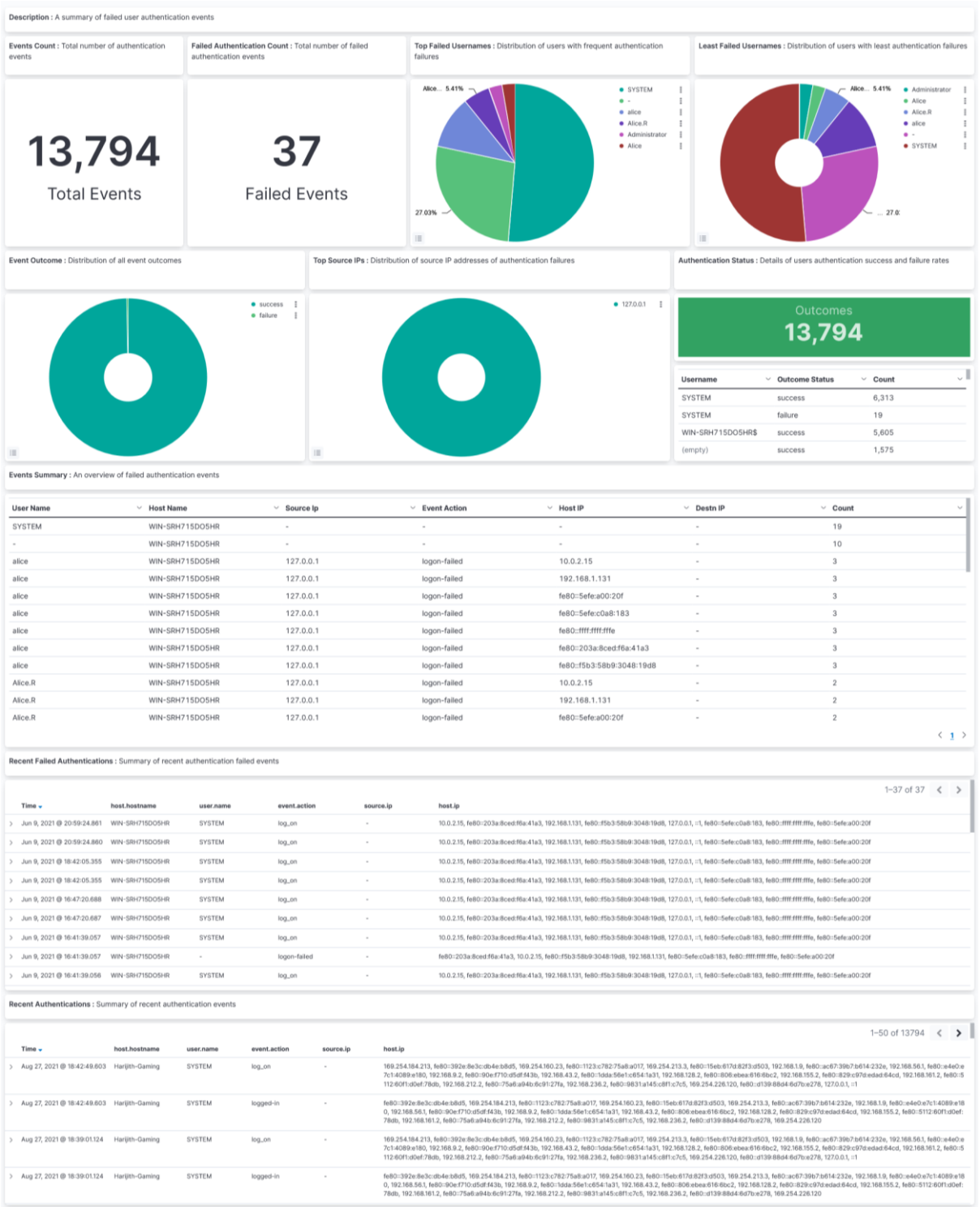


SAMPLE DASHBOARDS

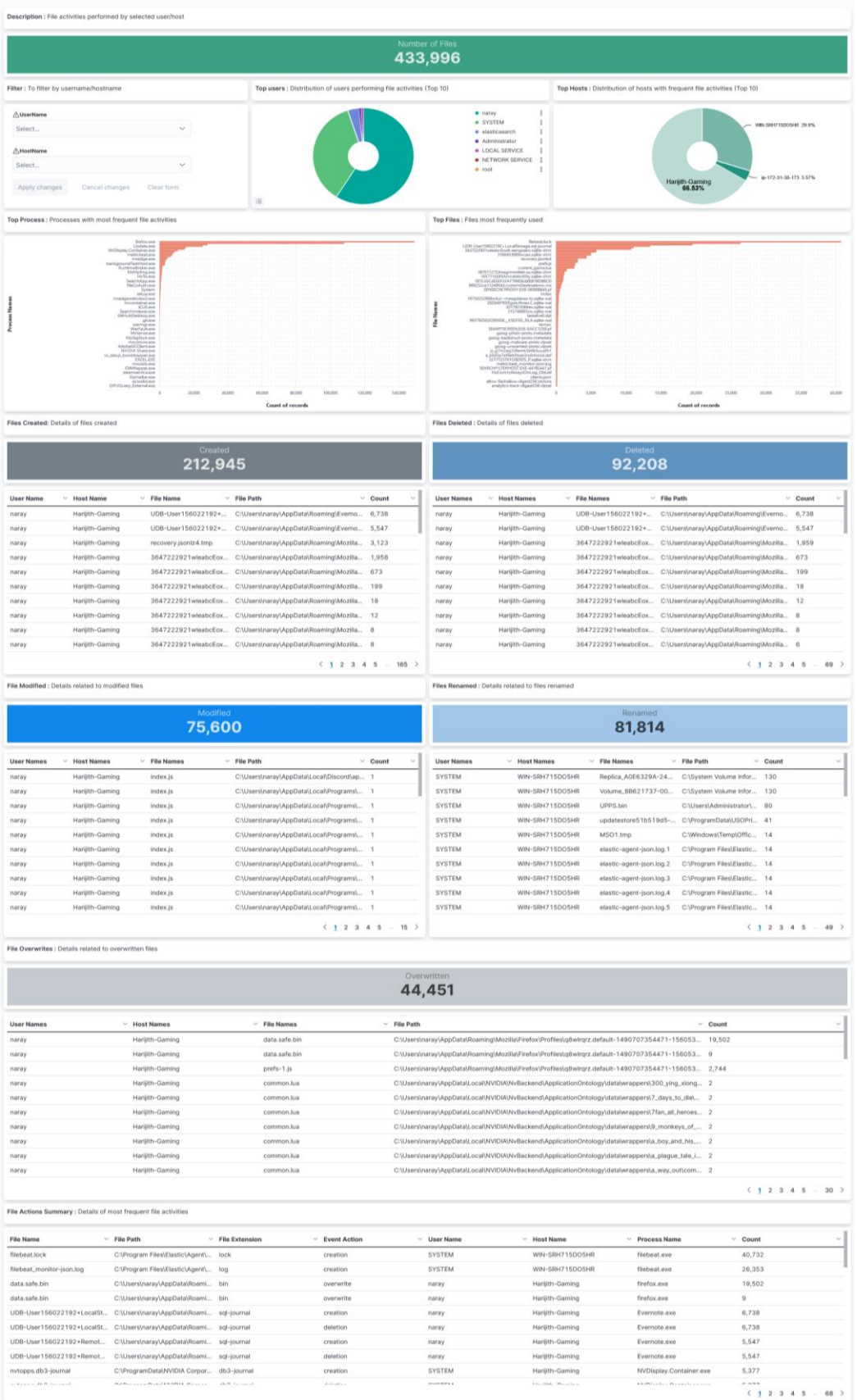
- Account management Summary



- Dashboard of Authentication Failures



- Dashboard of File Operations



FULL LIST OF DASHBOARDS

#	Name	Description
1	Security Analytics - Endpoint - User Overview	This dashboard is for displaying the overview of events which is performed by the user.
2	Security Analytics - Endpoint - Host Overview	This dashboard is for displaying the overview of events which is performed by the host.
3	Security Analytics - Endpoint - User Management Events	Information on user management events taking place on each endpoint
4	Security Analytics - Endpoint - Group Management Events	Group management activity.
5	Security Analytics - Endpoint - Network Overview	Details about network activities of selected user/host
6	Security Analytics- Endpoint- File Overview	File activities performed by selected user/host
7	Security Analytics- Endpoint- DNS Overview	Detailed DNS overview
8	Security Analytics- Endpoint- Registry Overview	This visualization is for displaying the overview of registry which is performed by the user/host.
9	Security Analytics- Endpoint- Process Overview	Details of processes under selected user/host
10	Security Analytics- Endpoint- User logins Overview	This dashboard is for displaying the overview of user login in an organization.
11	Security Analytics- Endpoint- SSH logins Overview	This dashboard is for displaying the overview of SSH login which is performed by the user.
12	Security Analytics- Network Sensor- Overview	Overview of all events captured by network sensor
13	Security Analytics- Network Sensor- HTTP Overview	Dashboard shows the http overview which is based on network sensor
14	Security Analytics- Network Sensor- SMB Overview	This dashboard shows an overview of SMB events that obtained from the network sensor
15	Security Analytics- Network Sensor- DNS Overview	This dashboard shows an overview of DNS events that obtained from the network sensor.
16	Security Analytics- Network Sensor- DHCP Overview	This dashboard shows an overview of DHCP events that obtained from the network sensor.
17	Security Analytics- Network Sensor- Files Overview	This dashboard shows an overview of File events that obtained from the network sensor.
18	Security Analytics- Network Sensor- FTP Overview	This dashboard shows an overview of FTP events that obtained from the network sensor.
19	Security Analytics- Network Sensor- IRC Overview	This dashboard shows an overview of IRC events that obtained from the network sensor.
20	Security Analytics- Network Sensor- Kerberos Overview	This dashboard shows an overview of Kerberos events captured by the network sensor.
21	Security Analytics- Network Sensor- MySQL Overview	This dashboard shows an overview of MySQL events that obtained from the network sensor.
22	Security Analytics- Network Sensor- NTLM Overview	This dashboard is for displaying the NTLM overview of events based on network sensor.
23	Security Analytics- Network Sensor- RADIUS Overview	This dashboard shows an overview of RADIUS events that obtained from the network sensor.
24	Security Analytics- Network Sensor- RDP Overview	This dashboard shows an overview of RDP events captured by network sensor.
25	Security Analytics- Network Sensor- SIP Overview	This dashboard is for displaying the overview of sip events in an organization.
26	Security Analytics- Network Sensor- SMTP Overview	This dashboard shows an overview of SMTP events that obtained from the network sensor.
27	Security Analytics- Network Sensor- SNMP Overview	This Dashboard displays the snmp datasets collects the Zeek snmp.log file, which contains SNMP messages.
28	Security Analytics- Network Sensor- SOCKS Overview	This dashboard shows an overview of the socks dataset collects the Zeek socks.log file, which contains SOCKS proxy requests.
29	Security Analytics- Network Sensor- SSH Overview	This dashboard shows the details of SSH events collected by network sensor
30	Security Analytics- Network Sensor- SSL Overview	This dashboard shows an overview of SSL events obtained from the network sensor.

31	Security Analytics- Network Sensor- X.509 Overview	This dashboard shows and overview of x509 events collected by network sensor
32	Compliance- Access and Authentication Failure Summary	This dashboard displays a summary of users with failed authentication.
33	Compliance- Accounts Modification Summary	This dashboard displays a summary of account modification based on compliance.
34	Compliance- Applications Accessed By User Summary	This dashboard displays a summary of application accessed by the user based on compliance.
35	Compliance- Privileged Account Management Activity Summary	This dashboard displays a summary of privileged account management activities by the user based on compliance.
36	Compliance- Privileged Authentication Activity Summary	This dashboard displays a summary of privileged authentication activities based on compliance.
37	Compliance-Applications Accessed By Privileged User Summary	This Dashboard is based on activities of privileged users
38	Compliance- Temporary Account Management Activity Summary	This dashboard is for displaying the account management activities related to temporary accounts
39	Compliance- Temporary Authentication Activity Summary	This dashboard displays a summary of temporary authentication activities based on compliance.
40	Compliance- Use Of Non-Encrypted Protocols Summary	This dashboard shows the usage of non encrypted protocols in the organization
41	Compliance-Uncommon Software's Usage Summary	This dashboard gives details of uncommon software's used by users
42	Compliance-Traffic to Internet Summary	A summary of internet traffic activities performed
43	Compliance-Traffic to Uncommon Ports Summary	A summary of network events to uncommon destination ports
44	Dashboard-Account Management Summary	Summarizing account management activities in the organization
45	Dashboard-Default Act Auth/Accs Failure Summary	Authentication and access failures related to default accounts
46	Dashboard-Default Act Auth/Accs Success Summary	Displaying details related to Succesful Authentication and access related to default accounts
47	Dashboard-Default Act Management Summary	Summarizing account management activities in the organization related to default accounts
48	Dashboard-Disabled & Locked Account Summary	Displaying details related to disabled and locked accounts
49	Dashboard-Enabled & Unlocked Account Summary	Displaying details related to enabled and unlocked accounts
50	Compliance- PCI DSS - Applications Accessed By User Summary	This dashboard displays a summary of application accessed by the user based on compliance. For PCI DSS Compliance
51	Compliance- PCI DSS - Authentication Failure Summary	This dashboard displays a summary of users with failed authentication. For PCI DSS Compliance
52	Compliance- PCI DSS - Configuration or Policy Change Summary	This dashboard displays details related to configuration and policy changes in hosts across the organization for PCI DSS compliance
53	Compliance- PCI DSS - Data Transfer Summary	This dashboard displays details related to data being transferred out of endpoints across the organization for PCI DSS compliance
54	Compliance- PCI DSS - Disabled & Locked Account Summary	Displaying details related to disabled and locked accounts for PCI DSS Compliance
55	Compliance- PCI DSS - Enabled & Unlocked Account Summary	Displaying details related to enabled and unlocked accounts for PCI DSS Compliance

FULL LIST OF DASHBOARDS

56	Compliance- PCI DSS - File Integrity Monitor Log Summary	Summarizes the events relating to integrity changes occurring on a particular file for PCI DSS Compliance
57	Compliance- PCI DSS - Accounts Modification Summary	This dashboard displays a summary of account modification for PCI DSS compliance.
58	Compliance- PCI DSS - Traffic to internet Summary	A summary of internet traffic activities performed across the organization for PCI DSS Compliance
59	Compliance- PCI DSS - Traffic to uncommon ports Summary	A summary of network events to uncommon destination ports for PCI DSS Compliance
60	Compliance- PCI DSS - Windows Firewall ChangeSummary	A summary of windows firewall changes that occurred in the organization for PCI DSS Compliance
61	Compliance- PCI DSS - User Priv Escalation (SU & SUDO)	A summary of user privilege escalation events on linux machines for PCI DSS Compliance
62	Compliance- PCI DSS - Rejected Connection to Network	A summary of rejected connections to network from endpoints for PCI DSS compliance
63	Compliance- PCI DSS - Uncommon softwares usage summary	This dashboard gives details of uncommon software's used by users for PCI DSS Compliance
64	Compliance- PCI DSS - Use of Non-Encrypted Protocols	This dashboard shows the usage of non encrypted protocols in the organization for PCI DSS Compliance
65	Compliance- PCI DSS - File Monitoring Event-File Changes	This dashboard shows file events particular to file changes performed across the organization for PCI DSS Compliance
66	Compliance- PCI DSS - Software Installed Summary	This dashboard shows summary of recent software installations across the organization for PCI DSS Compliance
67	Compliance- PCI DSS - Windows Host Configuration Change Summary	This dashboard shows the summary of recent windows hosts' configuration changes across the organization for PCI DSS Compliance
68	Compliance- PCI DSS - User Priv Escalation (Windows) Summary	This dashboard shows summary of privilege escalation events taking place on windows hosts across the organization for PCI DSS Compliance
69	Compliance- PCI DSS - Account Management Summary	Summarizing account management activities in the organization for PCI DSS Compliance
70	Compliance- NIST *NIX Host Configuration Change Summary	This dashboard summarizes configuration changes occuring in linux based hosts across the organization for NIST Compliance
71	Compliance- NIST - User Priv Escalation (SU & SUDO)	A summary of user privilege escalation events on linux machines for NIST Compliance
72	Compliance- NIST - Applications Accessed By User Summary	This dashboard displays a summary of application accessed by the user based on compliance. For NIST Compliance
73	Compliance- NIST - Account Management Summary	Summarizing account management activities in the organization for NIST Compliance
74	Compliance- NIST - Authentication Failure Summary	This dashboard displays a summary of users with failed authentication. For NIST Compliance
75	Compliance- NIST - Configuration or Policy Change Summary	This dashboard displays details related to configuration and policy changes in hosts across the organization for NIST compliance
76	Compliance- NIST - Data Transfer Summary	This dashboard displays details related to data being transferred out of endpoints across the organization for NIST compliance
77	Compliance- NIST - Disabled & Locked Account Summary	Displaying details related to disabled and locked accounts for NIST Compliance
78	Compliance- NIST - Enabled & Unlocked Account Summary	Displaying details related to enabled and unlocked accounts for NIST Compliance
79	Compliance- NIST - File Integrity Monitor Log Summary	Sumarrizes the events relating to integrity changes occurring on a particular file for NIST Compliance

FULL LIST OF DASHBOARDS

80	Compliance- NIST - Accounts Modification Summary	This dashboard displays a summary of account modification for NIST compliance.
81	Compliance- NIST - Traffic to internet Summary	A summary of internet traffic activities performed across the organization for NIST Compliance
82	Compliance- NIST - Traffic to uncommon ports Summary	A summary of network events to uncommon destination ports for NIST Compliance
83	Compliance- NIST - Windows Firewall ChangeSummary	A summary of windows firewall changes that occurred in the organization for NIST Compliance
84	Compliance- NIST - User Priv Escalation (Windows) Summary	This dashboard shows summary of privilege escalation events taking place on windows hosts across the organization for NIST Compliance
85	Compliance- NIST - Rejected Connection to Network	A summary of rejected connections to network from endpoints for NIST compliance
86	Compliance- NIST - Uncommon softwares usage summary	This dashboard gives details of uncommon software's used by users for NIST Compliance
87	Compliance- NIST - Use of Non-Encrypted Protocols	This dashboard shows the usage of non encrypted protocols in the organization for NIST Compliance
88	Compliance- NIST - File Monitoring Event-File Changes	This dashboard shows file events particular to file changes performed across the organization for NIST Compliance
89	Compliance- NIST - Software Installed Summary	This dashboard shows summary of recent software installations across the organization for NIST Compliance
90	Compliance- NIST - Windows Host Configuration Change Summary	This dashboard shows the summary of recent windows hosts' configuration changes across the organization for NIST Compliance
91	Compliance- ISO 27001- *NIX Host Configuration Change Summary	This dashboard summarizes configuration changes occurring in linux based hosts across the organization for ISO 27001 Compliance
92	Compliance- ISO 27001- Account Management Summary	Summarizing account management activities in the organization for ISO 27001 Compliance
93	Compliance- ISO 27001- Authentication Failure Summary	This dashboard displays a summary of users with failed authentication. For ISO 27001 Compliance
94	Compliance- ISO 27001- Configuration or Policy Change Summary	This dashboard displays details related to configuration and policy changes in hosts across the organization for ISO 27001 compliance
95	Compliance- ISO 27001- Data Transfer Summary	This dashboard displays details related to data being transferred out of endpoints across the organization for ISO 27001 compliance
96	Compliance- ISO 27001- Disabled & Locked Account Summary	Displaying details related to disabled and locked accounts for ISO 27001 Compliance
97	Compliance- ISO 27001- Enabled & Unlocked Account Summary	Displaying details related to enabled and unlocked accounts for ISO 27001 Compliance
98	Compliance- ISO 27001- File Integrity Monitor Log Summary	Summarizes the events relating to integrity changes occurring on a particular file for ISO 27001 Compliance
99	Compliance- ISO 27001- Accounts Modification Summary	This dashboard displays a summary of account modification for ISO 27001 compliance.
100	Compliance- ISO 27001- Traffic to internet Summary	A summary of internet traffic activities performed across the organization for ISO 27001 Compliance

FULL LIST OF DASHBOARDS

101	Compliance- ISO 27001- Traffic to uncommon ports Summary	A summary of network events to uncommon destination ports for ISO 27001 Compliance
102	Compliance- ISO 27001- Windows Firewall Change Summary	A summary of windows firewall changes that occurred in the organization for ISO 27001 Compliance
103	Compliance- ISO 27001- Applications Accessed By User Summary	This dashboard displays a summary of application accessed by the user based on compliance. For ISO 27001 Compliance
104	Compliance- ISO 27001- Rejected Connection to Network	A summary of rejected connections to network from endpoints for ISO 27001 compliance
105	Compliance- ISO 27001- Uncommon softwares usage summary	This dashboard gives details of uncommon software's used by users for ISO 27001 Compliance
106	Compliance- ISO 27001- File Monitoring Event-File Changes	This dashboard shows file events particular to file changes performed across the organization for ISO 27001 Compliance
107	Compliance- ISO 27001- Use of Non-Encrypted Protocols	This dashboard shows the usage of non encrypted protocols in the organization for ISO 27001 Compliance
108	Compliance- ISO 27001- Software Installed Summary	This dashboard shows summary of recent software installations across the organization for ISO 27001 Compliance
109	Compliance- ISO 27001- Windows Host Configuration Change Summary	This dashboard shows the summary of recent windows hosts' configuration changes across the organization for ISO 27001 Compliance
110	Compliance- ISO 27001- User Priv Escalation (Windows) Summary	This dashboard shows summary of privilege escalation events taking place on windows hosts across the organization for ISO 27001 Compliance
111	Compliance- ISO 27001- User Priv Escalation (SU & SUDO)	A summary of user privilege escalation events on linux machines for ISO 27001 Compliance
112	Threat Intelligence- Overview	This dashboard shows summary of overall threat intelligence information and acts as a home page for the threat intelligence section
113	Threat Intelligence- Management Summary	This dashboard acts as a summary for management level users for threat intelligence information
114	Threat Intelligence- Event Details	This dashboard gives granular event level details for a particular event from the community feeds
115	Threat Intelligence- News Summary	This dashboard gives Threat Intelligence News summary for management level users regarding recent events
116	Threat Intelligence- Vulnerabilities Summary	This dashboard gives latest vulnerabilities and exploit information to users
117	Threat Intelligence- Community Feeds overview	This dashboard provides an overview of all community sources of events
118	Threat Intelligence- Activbytes Threat Feed Summary	This dashboard provides an overview of Activebytes threat feeds