



# CYBOT HUNTER

Data Sheet

## DASHBOARD



✓ 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

<input type="checkbox"/>	<a href="#">116-Compliance-NIST-Uncommon Software's Usage Summary</a>	This dashboard gives details of uncommon software's used by users
<input type="checkbox"/>	<a href="#">117-Compliance-NIST- Use of Non-Encrypted Protocols</a>	
<input type="checkbox"/>	<a href="#">118-Compliance- NIST- File Monitoring Event-File Changes</a>	File activities performed by selected user/host
<input type="checkbox"/>	<a href="#">120-Compliance- NIST- Windows Host Configuration Change Summary</a>	
<input type="checkbox"/>	<a href="#">122-Compliance- ISO-27001-Account Management Summary</a>	Package-Compliance-Account Management Summary
<input type="checkbox"/>	<a href="#">123-Compliance-ISO-27001-Access and Authentication Failure Summary</a>	This dashboard displays a summary of users with failed authentication.
<input type="checkbox"/>	<a href="#">126-Compliance-ISO-27001-Disabled &amp; Locked account summary</a>	A summary of Disabled & Locked accounts
<input type="checkbox"/>	<a href="#">127-Compliance- ISO 27001-Enabled &amp; Unlocked Account Summary</a>	A summary of enabled & unlocked account
<input type="checkbox"/>	<a href="#">129-Compliance-ISO 27001-Accounts Modification Summary</a>	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-SRH715D05HR\$  
Account Domain: TEST  
Logon ID: 0x3E7

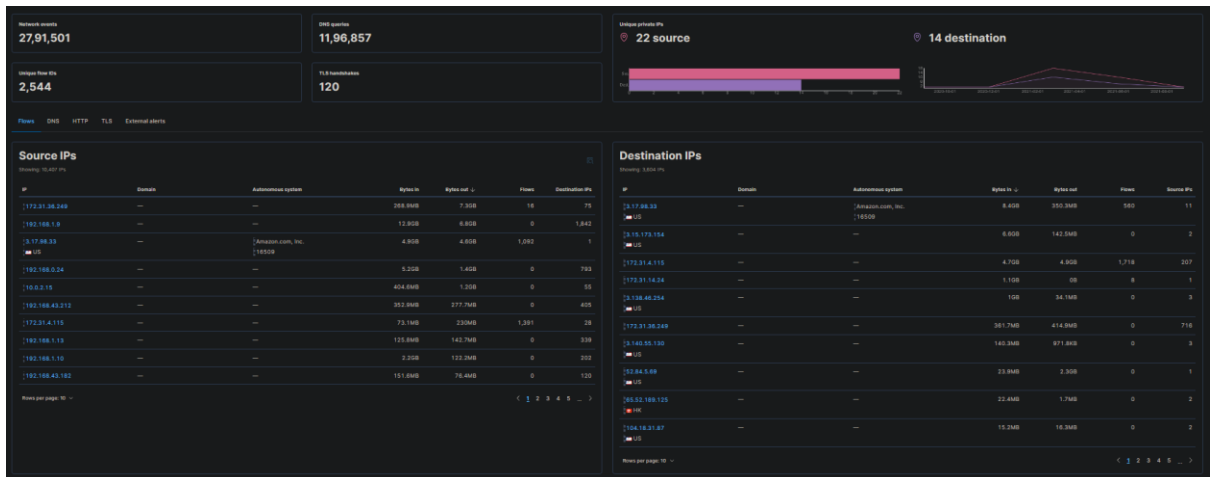
#### Target Account:

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

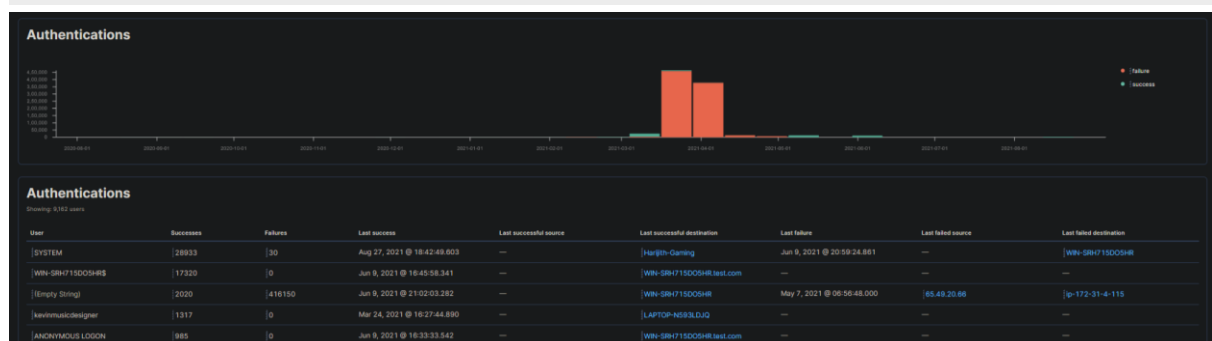
#### Changed Attributes:

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: -

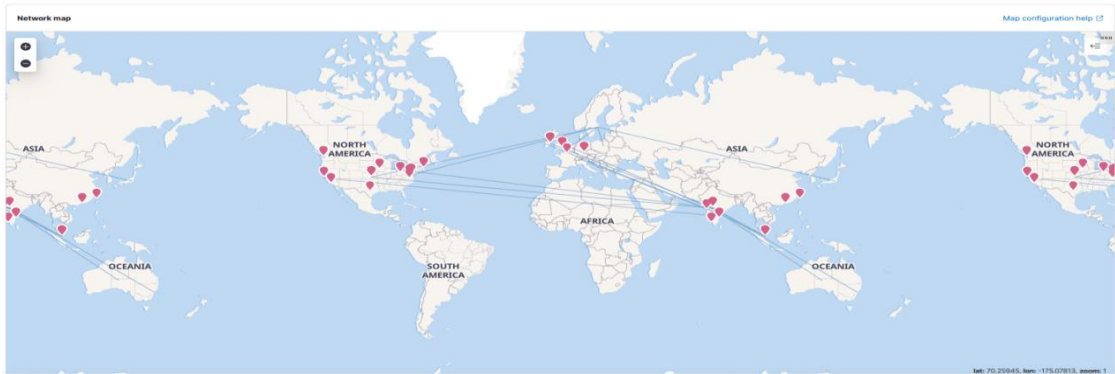
- ❑ Effective co-relation capabilities over detailed information provided by both network and host data extractors.
- ❑ Capability to investigate on user, host, network traffic and all activities around it with effective filtering and visualizations
- ❑ Faster reports and dashboard generation for longer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



- ✓ Visibility on all types of authentication failure and success activities, occurred in the infrastructure



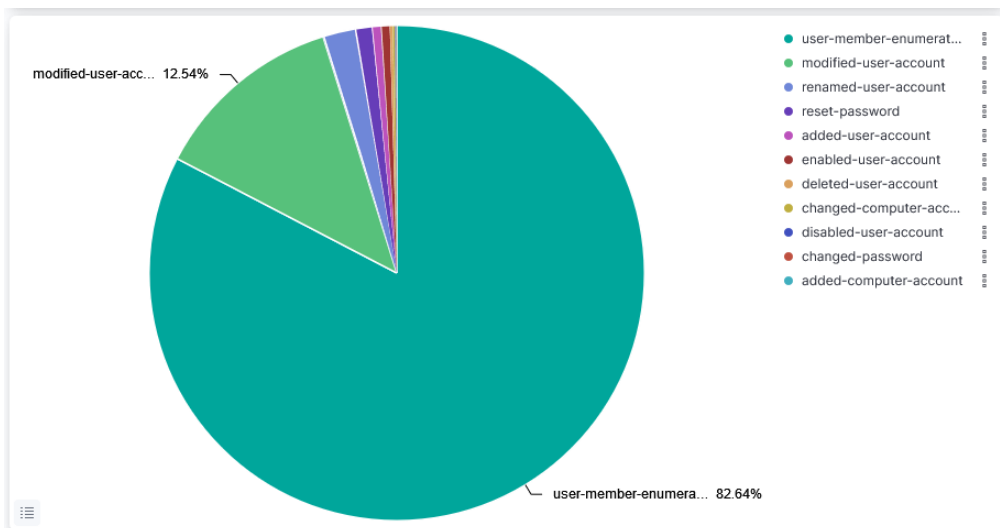
- ☐ In depth visibility on all file creation and modifications
- ☐ Visibility on web server activities on enterprise servers
- ☐ In depth view on operating system level executions and operations
- ☐ Enhanced visibility on network traffic



- ✓ 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

Description : An overview of accounts management activities performed across the organization.

Filter : To filter by username

ΔUser\_Name  
Select...  
Apply changes Cancel changes Clear form

Events Count : Total count of events

Event Count  
5,832

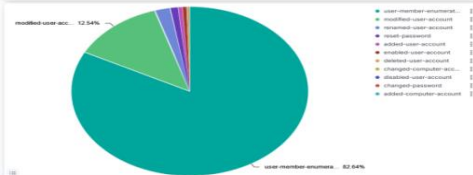
User Events : Count of events performed by the user

User Events  
5,334

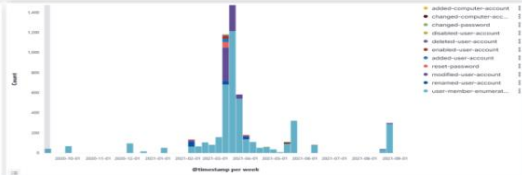
Group Events : Count of events performed by the groups

Group Events  
498

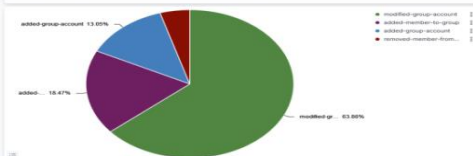
User Actions : Distribution of the most accurate user management actions



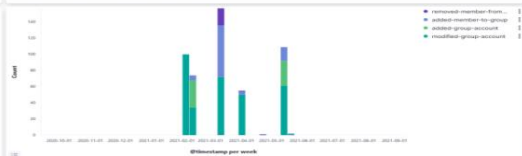
User Actions In Time : User management actions distributed over time



Group Actions : Distribution of the most accurate group management actions



Group Action In Time : Group management actions distributed over time



Created Accounts : Details of the Created Accounts

Created User	Performed By	Login ID	Count
Employee	91920	0-97755	4
OverWatch	91920	0-97755	4
defaultUser0	WIN-NE3L3L48JE...	0-3a7	3
test1	testa	0-3bda8	3
test2	testa	0-3bda8	3
test3	testa	0-3bda8	3

Modified Accounts : Details of the Modified accounts

User Name	Host Name	Event Action	Count
91920	LAPTOP-K03SL...	modified-user-acc...	439
testa	DESKTOP-H710...	modified-user-acc...	67
Administrator	EC2AMAZ-8OLF...	modified-user-acc...	10
Administrator	DESKTOP-H710...	modified-user-acc...	9
Administrator	WIN-SRH715D0S...	modified-user-acc...	7
anonymous	1.8BTHL-K03SL...	modified-user-acc...	16

Deleted Accounts : Details of the Deleted accounts

Deleted User	Performed By	Performed Login ID	Count
OverWatch	91920	0-97755	4
defaultUser0	testa	0-153b8d	3
defaultUser100000	DESKTOP-H710D0G...	0-3a7	1
defaultUser100001	DESKTOP-H710D0G...	0-3a7	1
testa_3fvgk7	testa	0-51024	1

User Management Summary : Details of frequently performed management events on the selected user

Event Action	Target User	User Domain	User Name	Login ID	Related User	Count
user-member-enumerated	Administrators	WORKGROUP	Administrators	0-3a7	LAPTOP-N593LDJ58	1,540
user-member-enumerated	Administrators	WORKGROUP	Administrators	0-3a7	LAPTOP-JADRAUVIS	496
user-member-enumerated	Administrators	WORKGROUP	Administrators	0-3a7	WIN-SRH715D0S4R8	299
user-member-enumerated	Administrators	WORKGROUP	Administrators	0-3a7	DESKTOP-V2N5ASV5	182
user-member-enumerated	Administrators	WORKGROUP	Administrators	0-3a7	HARLUTH-GAMINGS	161
user-member-enumerated	Administrators	WORKGROUP	Administrators	0-3a7	DESKTOP-H710D0G...	130
user-member-enumerated	Administrators	WORKGROUP	Administrators	0-3a7	WIN-NE3L3L48JE15	57
user-member-enumerated	Administrators	WORKGROUP	Administrators	0-3a7	EC2AMAZ-8OLFNFUS	38

Recent User Management events : Details of the recently performed user management events on the selected user

Time	event action	writing event_data.TargetDomainName	User domain	User name	writing login id	Related user
Aug 27, 2021 @ 16:49:13.028	user-member-enumerated	Butin	WORKGROUP	HARLUTH-GAMINGS	0-3a7	HARLUTH-GAMINGS
Aug 27, 2021 @ 16:49:13.025	user-member-enumerated	Butin	WORKGROUP	HARLUTH-GAMINGS	0-3a7	HARLUTH-GAMINGS
Aug 27, 2021 @ 16:38:38.886	user-member-enumerated	Butin	WORKGROUP	HARLUTH-GAMINGS	0-3a7	HARLUTH-GAMINGS
Aug 27, 2021 @ 16:38:38.886	user-member-enumerated	Butin	WORKGROUP	HARLUTH-GAMINGS	0-3a7	HARLUTH-GAMINGS
Aug 27, 2021 @ 11:44:38.081	user-member-enumerated	Butin	WORKGROUP	HARLUTH-GAMINGS	0-3a7	HARLUTH-GAMINGS
Aug 27, 2021 @ 11:44:38.080	user-member-enumerated	Butin	WORKGROUP	HARLUTH-GAMINGS	0-3a7	HARLUTH-GAMINGS
Aug 27, 2021 @ 11:44:38.050	user-member-enumerated	Butin	WORKGROUP	HARLUTH-GAMINGS	0-3a7	HARLUTH-GAMINGS
Aug 27, 2021 @ 11:44:38.054	user-member-enumerated	Butin	WORKGROUP	HARLUTH-GAMINGS	0-3a7	HARLUTH-GAMINGS
Aug 27, 2021 @ 11:44:38.048	user-member-enumerated	Butin	WORKGROUP	HARLUTH-GAMINGS	0-3a7	HARLUTH-GAMINGS

Group Management Summary : Details of frequently performed group management events related to the selected user

Event Action	Group Name	Group Domain	User Name	User Domain	Host Name	Count
modified-group-account	Performance Log Users	Missing	WIN-NE3L3L48JE15	WORKGROUP	DESKTOP-H710D0G...	6
modified-group-account	Performance Log Users	Missing	WIN-SRH715D0S4R8	WORKGROUP	WIN-SRH715D0S4R8	4
modified-group-account	Performance Log Users	Missing	WIN-SRH715D0S4R8	TEST	WIN-SRH715D0S4R8	1
modified-group-account	Performance Log Users	Missing	EC2AMAZ-8OLFNFUS	WORKGROUP	EC2AMAZ-8OLFNFUS	2
modified-group-account	Performance Log Users	Missing	Administrator	TEST	WIN-SRH715D0S4R8	1
modified-group-account	Administrators	Missing	WIN-NE3L3L48JE15	WORKGROUP	DESKTOP-H710D0G...	6
modified-group-account	Administrators	Missing	WIN-SRH715D0S4R8	WORKGROUP	WIN-SRH715D0S4R8	4

Recent Group Management summary : Details of recently performed group management events related to the selected user

Time	event action	group name	group domain	user name	user domain	host name
May 16, 2021 @ 16:14:45.090	added-member-to-group	Performance Log Users	Butin	Administrator	TEST	WIN-SRH715D0S4R8
May 16, 2021 @ 16:14:45.090	modified-group-account	Performance Log Users	Butin	Administrator	TEST	WIN-SRH715D0S4R8
May 14, 2021 @ 11:27:33.551	modified-group-account	Remote Desktop Users	Butin	Administrator	TEST	WIN-SRH715D0S4R8
May 14, 2021 @ 11:27:33.550	added-member-to-group	Remote Desktop Users	Butin	Administrator	TEST	WIN-SRH715D0S4R8
May 11, 2021 @ 16:34:16.080	modified-group-account	Domain Controllers	TEST	ANONYMOUS LOGON	NT AUTHORITY	WIN-SRH715D0S4R8
May 11, 2021 @ 16:34:16.080	modified-group-account	Read-only Domain Controllers	TEST	ANONYMOUS LOGON	NT AUTHORITY	WIN-SRH715D0S4R8
May 11, 2021 @ 16:34:16.079	modified-group-account	Replicator	Butin	ANONYMOUS LOGON	NT AUTHORITY	WIN-SRH715D0S4R8
May 11, 2021 @ 16:34:16.078	modified-group-account	Administrators	Butin	ANONYMOUS LOGON	NT AUTHORITY	WIN-SRH715D0S4R8
May 11, 2021 @ 16:34:16.076	modified-group-account	Backup Operators	Butin	ANONYMOUS LOGON	NT AUTHORITY	WIN-SRH715D0S4R8

# Dashboard of Authentication Failures

Description : A summary of failed user authentication events

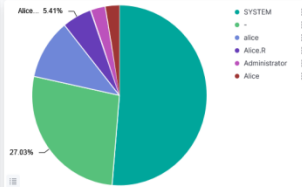
Events Count : Total number of authentication events

13,794  
Total Events

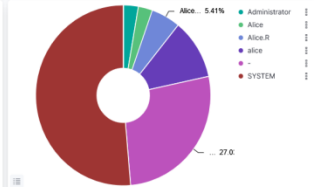
Failed Authentication Count : Total number of failed authentication events

37  
Failed Events

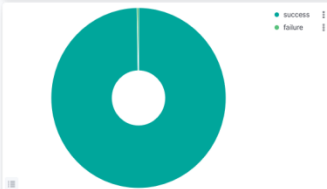
Top Failed Usernames : Distribution of users with frequent authentication failures



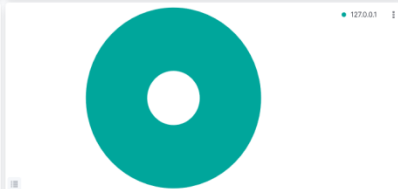
Least Failed Usernames : Distribution of users with least authentication failures



Event Outcome : Distribution of all event outcomes



Top Source IPs : Distribution of source IP addresses of authentication failures



Authentication Status : Details of users authentication success and failure rates

Outcomes		
13,794		
Username	Outcome Status	Count
SYSTEM	success	6,313
SYSTEM	failure	19
WIN-SRH71SDOSHRS	success	5,605
(empty)	success	1,575

Events Summary : An overview of failed authentication events

User Name	Host Name	Source Ip	Event Action	Host IP	Destn IP	Count
SYSTEM	WIN-SRH71SDOSHRS	-	-	-	-	19
-	WIN-SRH71SDOSHRS	-	-	-	-	10
alice	WIN-SRH71SDOSHRS	127.0.0.1	login-failed	10.0.2.15	-	3
alice	WIN-SRH71SDOSHRS	127.0.0.1	login-failed	192.168.1.131	-	3
alice	WIN-SRH71SDOSHRS	127.0.0.1	login-failed	fe80::5efea000:20f	-	3
alice	WIN-SRH71SDOSHRS	127.0.0.1	login-failed	fe80::5efec0a8:183	-	3
alice	WIN-SRH71SDOSHRS	127.0.0.1	login-failed	fe80::ffff:ffff	-	3
alice	WIN-SRH71SDOSHRS	127.0.0.1	login-failed	fe80::203a:8ced:f6a:41a3	-	3
alice	WIN-SRH71SDOSHRS	127.0.0.1	login-failed	fe80::f5b3:58b9:3048:19a8	-	3
Alice.R	WIN-SRH71SDOSHRS	127.0.0.1	login-failed	10.0.2.15	-	2
Alice.R	WIN-SRH71SDOSHRS	127.0.0.1	login-failed	192.168.1.131	-	2
Alice.R	WIN-SRH71SDOSHRS	127.0.0.1	login-failed	fe80::5efea000:20f	-	2

Recent Failed Authentications : Summary of recent authentication failed events

Time	host.hostname	user.name	event.action	source.ip	host.ip
Jun 9, 2021 @ 20:59:24.861	WIN-SRH71SDOSHRS	SYSTEM	log_on	-	10.0.2.15, fe80::203a:8ced:f6a:41a3, 192.168.1.131, fe80::f5b3:58b9:3048:19a8, 127.0.0.1, fe80::5efec0a8:183, fe80::ffff:ffff, fe80::5efea000:20f
Jun 9, 2021 @ 20:59:24.860	WIN-SRH71SDOSHRS	SYSTEM	log_on	-	10.0.2.15, fe80::203a:8ced:f6a:41a3, 192.168.1.131, fe80::f5b3:58b9:3048:19a8, 127.0.0.1, fe80::5efec0a8:183, fe80::ffff:ffff, fe80::5efea000:20f
Jun 9, 2021 @ 18:42:05.355	WIN-SRH71SDOSHRS	SYSTEM	log_on	-	10.0.2.15, fe80::203a:8ced:f6a:41a3, 192.168.1.131, fe80::f5b3:58b9:3048:19a8, 127.0.0.1, fe80::5efec0a8:183, fe80::ffff:ffff, fe80::5efea000:20f
Jun 9, 2021 @ 18:42:05.355	WIN-SRH71SDOSHRS	SYSTEM	log_on	-	10.0.2.15, fe80::203a:8ced:f6a:41a3, 192.168.1.131, fe80::f5b3:58b9:3048:19a8, 127.0.0.1, fe80::5efec0a8:183, fe80::ffff:ffff, fe80::5efea000:20f
Jun 9, 2021 @ 16:47:20.688	WIN-SRH71SDOSHRS	SYSTEM	log_on	-	10.0.2.15, fe80::203a:8ced:f6a:41a3, 192.168.1.131, fe80::f5b3:58b9:3048:19a8, 127.0.0.1, fe80::5efec0a8:183, fe80::ffff:ffff, fe80::5efea000:20f
Jun 9, 2021 @ 16:47:20.687	WIN-SRH71SDOSHRS	SYSTEM	log_on	-	10.0.2.15, fe80::203a:8ced:f6a:41a3, 192.168.1.131, fe80::f5b3:58b9:3048:19a8, 127.0.0.1, fe80::5efec0a8:183, fe80::ffff:ffff, fe80::5efea000:20f
Jun 9, 2021 @ 16:41:39.057	WIN-SRH71SDOSHRS	SYSTEM	log_on	-	10.0.2.15, fe80::203a:8ced:f6a:41a3, 192.168.1.131, fe80::f5b3:58b9:3048:19a8, 127.0.0.1, fe80::5efec0a8:183, fe80::ffff:ffff, fe80::5efea000:20f
Jun 9, 2021 @ 16:41:39.057	WIN-SRH71SDOSHRS	-	login-failed	-	fe80::203a:8ced:f6a:41a3, 10.0.2.15, fe80::f5b3:58b9:3048:19a8, 192.168.1.131, fe80::5efec0a8:183, fe80::ffff:ffff, fe80::5efea000:20f
Jun 9, 2021 @ 16:41:39.056	WIN-SRH71SDOSHRS	SYSTEM	log_on	-	10.0.2.15, fe80::203a:8ced:f6a:41a3, 192.168.1.131, fe80::f5b3:58b9:3048:19a8, 127.0.0.1, fe80::5efec0a8:183, fe80::ffff:ffff, fe80::5efea000:20f

Recent Authentications : Summary of recent authentication events

Time	host.hostname	user.name	event.action	source.ip	host.ip
Aug 27, 2021 @ 18:42:49.603	Harjit-Gaming	SYSTEM	log_on	-	169.254.184.213, fe80::392e:8a3c:db4e:bd8f, 169.254.184.213, fe80::1123:c782:75ab:a077, 169.254.213.3, fe80::15eb:677a:8273:d503, 192.168.1.9, fe80::ac67:3967:b614:232e, 192.168.156.1, fe80::a4e0:e7c1:4089:e180, 192.168.9.2, fe80::90e:f770:cd5f:f43b, 192.168.43.2, fe80::1a5a:56e1:c854:1a31, 192.168.128.2, fe80::806:eb0e:a18:80c2, 192.168.155.2, fe80::829:c97e:edea:64cd, 192.168.161.2, fe80::512:60f1:dbef:78ab, 192.168.212.2, fe80::75ab:a94b:dc91:27fa, 192.168.236.2, fe80::9831:a145:c8f1:c7c5, 169.254.226.120, fe80::a139:6864:6c7b:e278, 127.0.0.1, 11
Aug 27, 2021 @ 18:42:49.603	Harjit-Gaming	SYSTEM	logged-in	-	fe80::392e:8a3c:db4e:bd8f, 169.254.184.213, fe80::1123:c782:75ab:a077, 169.254.184.213, fe80::15eb:677a:8273:d503, 169.254.213.3, fe80::ac67:3967:b614:232e, 192.168.1.9, fe80::a4e0:e7c1:4089:e180, 192.168.561, fe80::90e:f770:cd5f:f43b, 192.168.9.2, fe80::1a5a:56e1:c854:1a31, 192.168.43.2, fe80::806:eb0e:a18:80c2, 192.168.128.2, fe80::829:c97e:edea:64cd, 192.168.155.2, fe80::512:60f1:dbef:78ab, 192.168.161.2, fe80::75ab:a94b:dc91:27fa, 192.168.212.2, fe80::9831:a145:c8f1:c7c5, 169.254.226.120, fe80::a139:6864:6c7b:e278, 169.254.226.120
Aug 27, 2021 @ 18:39:01.124	Harjit-Gaming	SYSTEM	log_on	-	169.254.184.213, fe80::392e:8a3c:db4e:bd8f, 169.254.184.213, fe80::1123:c782:75ab:a077, 169.254.213.3, fe80::15eb:677a:8273:d503, 192.168.1.9, fe80::ac67:3967:b614:232e, 192.168.156.1, fe80::a4e0:e7c1:4089:e180, 192.168.9.2, fe80::90e:f770:cd5f:f43b, 192.168.43.2, fe80::1a5a:56e1:c854:1a31, 192.168.128.2, fe80::806:eb0e:a18:80c2, 192.168.155.2, fe80::829:c97e:edea:64cd, 192.168.161.2, fe80::512:60f1:dbef:78ab, 192.168.212.2, fe80::75ab:a94b:dc91:27fa, 192.168.236.2, fe80::9831:a145:c8f1:c7c5, 169.254.226.120, fe80::a139:6864:6c7b:e278, 127.0.0.1, 11
Aug 27, 2021 @ 18:39:01.124	Harjit-Gaming	SYSTEM	logged-in	-	fe80::392e:8a3c:db4e:bd8f, 169.254.184.213, fe80::1123:c782:75ab:a077, 169.254.184.213, fe80::15eb:677a:8273:d503, 169.254.213.3, fe80::ac67:3967:b614:232e, 192.168.1.9, fe80::a4e0:e7c1:4089:e180, 192.168.561, fe80::90e:f770:cd5f:f43b, 192.168.9.2, fe80::1a5a:56e1:c854:1a31, 192.168.43.2, fe80::806:eb0e:a18:80c2, 192.168.128.2, fe80::829:c97e:edea:64cd, 192.168.155.2, fe80::512:60f1:dbef:78ab, 192.168.161.2, fe80::75ab:a94b:dc91:27fa, 192.168.212.2, fe80::9831:a145:c8f1:c7c5, 169.254.226.120, fe80::a139:6864:6c7b:e278, 169.254.226.120

# Dashboard of File Operations

Description : File activities performed by selected user/host

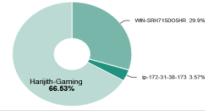
Number of Files  
433,996

Filter : To filter by username/hostname

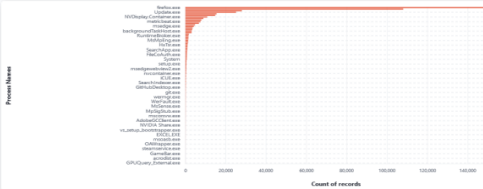
Top users : Distribution of users performing file activities (Top 10)



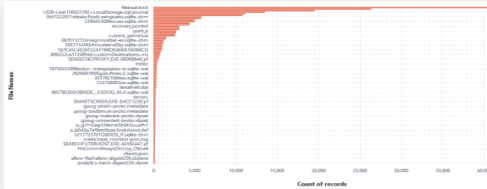
Top Hosts : Distribution of hosts with frequent file activities (Top 10)



Top Process : Processes with most frequent file activities



Top Files : Files most frequently used



Files Created : Details of files created

Created  
212,945

User Name	Host Name	File Name	File Path	Count
nary	Harjith-Gaming	UDB-User156022192+...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	6,738
nary	Harjith-Gaming	UDB-User156022192+...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	5,547
nary	Harjith-Gaming	recovery.joint4.tmp	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	3,123
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1,958
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	673
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	199
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	18
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	12
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	8
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	8

Files Deleted : Details of files deleted

Deleted  
92,208

User Names	Host Names	File Names	File Path	Count
nary	Harjith-Gaming	UDB-User156022192+...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	6,738
nary	Harjith-Gaming	UDB-User156022192+...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	5,547
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1,959
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	673
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	199
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	18
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	12
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	8
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	8
nary	Harjith-Gaming	3647222921.welabCEx...	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	6

Files Modified : Details related to modified files

Modified  
75,600

User Names	Host Names	File Names	File Path	Count
nary	Harjith-Gaming	index.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1
nary	Harjith-Gaming	index.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1
nary	Harjith-Gaming	index.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1
nary	Harjith-Gaming	index.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1
nary	Harjith-Gaming	index.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1
nary	Harjith-Gaming	index.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1
nary	Harjith-Gaming	index.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1
nary	Harjith-Gaming	index.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1
nary	Harjith-Gaming	index.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1
nary	Harjith-Gaming	index.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	1

Files Renamed : Details related to files renamed

Renamed  
81,814

User Names	Host Names	File Names	File Path	Count
SYSTEM	WIN-SRH71SD0SHR	Replica_AGE632BA-24...	C:\System Volume Information\Replica_AGE632BA-24...	130
SYSTEM	WIN-SRH71SD0SHR	Volume_B8621737-00...	C:\System Volume Information\Volume_B8621737-00...	130
SYSTEM	WIN-SRH71SD0SHR	UPPS.bin	C:\Users\Administrator\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	80
SYSTEM	WIN-SRH71SD0SHR	updatestore51051845...	C:\Users\Administrator\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	41
SYSTEM	WIN-SRH71SD0SHR	MSO1.tmp	C:\Users\Administrator\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	14
SYSTEM	WIN-SRH71SD0SHR	elastic-agent-jon.log.1	C:\Program Files\Elastic\elastic-agent-jon.log.1	14
SYSTEM	WIN-SRH71SD0SHR	elastic-agent-jon.log.2	C:\Program Files\Elastic\elastic-agent-jon.log.2	14
SYSTEM	WIN-SRH71SD0SHR	elastic-agent-jon.log.3	C:\Program Files\Elastic\elastic-agent-jon.log.3	14
SYSTEM	WIN-SRH71SD0SHR	elastic-agent-jon.log.4	C:\Program Files\Elastic\elastic-agent-jon.log.4	14
SYSTEM	WIN-SRH71SD0SHR	elastic-agent-jon.log.5	C:\Program Files\Elastic\elastic-agent-jon.log.5	14

File Overwrites : Details related to overwritten files

Overwritten  
44,451

User Names	Host Names	File Names	File Path	Count
nary	Harjith-Gaming	data.safe.bin	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	19,502
nary	Harjith-Gaming	data.safe.bin	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	9
nary	Harjith-Gaming	prefe-1.js	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	2,744
nary	Harjith-Gaming	common.lua	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	2
nary	Harjith-Gaming	common.lua	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	2
nary	Harjith-Gaming	common.lua	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	2
nary	Harjith-Gaming	common.lua	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	2
nary	Harjith-Gaming	common.lua	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	2
nary	Harjith-Gaming	common.lua	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	2
nary	Harjith-Gaming	common.lua	C:\Users\nary\AppData\Local\Programs\Microsoft Windows\Windows Defender\Windows Defender Security Center\Windows Defender Security Center.exe	2

File Actions Summary : Details of most frequent file activities

File Name	File Path	File Extension	Event Action	User Name	Host Name	Process Name	Count
filebeat.lock	C:\Program Files\Elastic\Agent\...	lock	creation	SYSTEM	WIN-SRH71SD0SHR	filebeat.exe	40,732
filebeat_monitor-jon.log	C:\Program Files\Elastic\Agent\...	log	creation	SYSTEM	WIN-SRH71SD0SHR	filebeat.exe	26,353
data.safe.bin	C:\Users\nary\AppData\Local\Roam...	bin	overwrite	nary	Harjith-Gaming	firefox.exe	19,502
data.safe.bin	C:\Users\nary\AppData\Local\Roam...	bin	overwrite	nary	Harjith-Gaming	firefox.exe	9
UDB-User156022192+LocalS...	C:\Users\nary\AppData\Local\Roam...	sqf-journal	creation	nary	Harjith-Gaming	Evernote.exe	6,738
UDB-User156022192+LocalS...	C:\Users\nary\AppData\Local\Roam...	sqf-journal	deletion	nary	Harjith-Gaming	Evernote.exe	6,738
UDB-User156022192+Remot...	C:\Users\nary\AppData\Local\Roam...	sqf-journal	creation	nary	Harjith-Gaming	Evernote.exe	5,547
UDB-User156022192+Remot...	C:\Users\nary\AppData\Local\Roam...	sqf-journal	deletion	nary	Harjith-Gaming	Evernote.exe	5,547
nvtopps.dtb-journal	C:\ProgramData\NVIDIA Corpor...	db3-journal	creation	SYSTEM	Harjith-Gaming	NVDisplay.Container.exe	5,377

## 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

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 occurring 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

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

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