

Workshop Walkthrough

Table Of Content

- Configurations
- Resource Configurations
- Attribute Configurations
- Pipeline mapping & Data Sources
- Ingestion
- Investigation
 - Risk score
 - Profile page (User and Entity)
 - Detection
 - Watch list
- Models
- Dashboards
- Reports
- Data exports
- Case management
 - Case actions
 - Alerts
- Playbook actions
- MITRE mapping

Configurations



GRA Dashboard Investigate Studio Respond Reports Pipelines Configure

Open Cases 50

Create and Manage

CREATE AND MANAGE USERS, RESOURCES, RESOURCE GROUPS, ACCOUNT AND ENTITLEMENT ATTRIBUTES. (MANAGE IS THE REPOSITORY TO STORE AND VIEW IDENTITY INFORMATION OF USERS AND RESOURCES.)

Resources
Create new resources, view existing resource details and view existing resource group roles.

Attributes
Create new attributes specific to users, accounts, entities, entitlements, accounts, entitlements and roles.

Account Types
Map the account type to GRA account type.

Manage Entities
Create new Entities based on activity attributes.

User Groups
Define group/un-group, conditions to be applied for Groups used for analyzing user data with their peers.

Incident Configurations
Select users for anomaly engines and configure incident notifications and assignments.

Monitor

MONITOR THE LOGIN AND LOGOUT DETAILS OF THE USER, RECORD TRANSACTION EVENTS AND WEB SERVICE REQUEST LOGS.

GRA Audit
Display event logs of users along with audit timestamp.

Application Audit
Display Web Server Logs, App Server Logs, and Import Job Logs.

Email Template List
Display list of all available Email templates in GRA.

Mail Configuration
Configure mail server to send Email notifications or alerts from GRA.

GRA Properties
Configure definition values in existing GRA properties.

Certification Setting
Configure reminders to be sent for Certification process.

GRA Data Collectors
Configure data collector, download, analyze and view list of all configured data collector jobs.

Monitoring Counters
Configure monitoring counters in GRA.

Data

CREATE/CONFIGURE DATA SOURCES, LOG MANAGERS, DATA FORWARDERS ETC TO ENABLE IMPORT/EXPORT OF DATA.

Setup
Create/Configure Data Sources and Log Managers.

Jobs
GRA jobs that can be enabled and triggered.

Purge Data
Purge all data related to the run of an anomaly engine.

Manage
Purge all data related to the run of an anomaly engine.

Certification
Create certificates against users assigned at the time of configuring the job.

Security and Privacy

DELEGATE TASK AND HANDLE PRIVILEGES GIVEN TO USERS. ADD/DELETE USER, DEFINE USER ROLE AND DATA ACCESS, CONFIGURE ADDITIONAL ATTRIBUTES FOR DISPLAY OF USER DETAILS.

Users
Create/Edit user profile.

Roles
Create Roles to provide specific privileges or accessses in GRA.

SSO
Configure Single Sign-On using SAML/LDAP authentication.

License
Upload new License.

Login Banner
Upload new Login Banner.

Web Service Management
Generate API keys for web service clients.

Data Masking and Unmasking
Mask data for selected attributes. Unmask data for selected User attributes.

Upload
Upload files to GRA.

Resource Configuration Screen



GR Dashboard Investigate Studio Respond Reports Pipelines Configure ...

Open Cases 50

CREATE AND MANAGE

RESOURCES RESOURCE GROUP

Resources

ENABLED 461 DISABLED 0

Search

Resource Groups

179 DEFAULT

- 52 Firewall
- 33 Cloud Applications
- 14 Anti Spam
- 14 Threat Intelligence
- 14 DLP
- 12 Identity and Access Management
- 11 Email Gateway
- 10 VPN
- 10 Network Monitoring
- 9 Operating Systems
- 8 Database server
- 8 Proxy
- 7 Document Monitoring
- 7 SIEM
- 6 Financial Applications
- 6 EDR
- 6 IDS

Resource	Description
1Password	
3Com	
ABMDEV	
ABMPROD	
ABMUAT	
Abnormal Security	Abnormal
Abuse.ch	
Account Payable	
Active Directory	
Active Directory Federate...	
AD Audit Plus	
ADFS Auditing	
GURUCUL	
airwatch by vmware	
AIX	
AT&T Business	

Attributes Configurations



CREATE AND MANAGE

USERS ACCOUNTS ENTITIES ENTITLEMENTS ACCOUNT ENTITLEMENTS ROLES

User Attributes

CANCEL ADD

Organization Name

Attribute Name	Tenant Name	Display Name	Attribute Type	Added Date	Added By	Modified Date	Modified By	Action
accountenabled	Organization Name	accountEnabled	Text	11/04/2022 22:37:52	graadmin			<button>Edit</button> <button>Delete</button>
activatedokta	Organization Name	Activated Okta	Text	07/21/2024 13:13:12	graadmin			<button>Edit</button> <button>Delete</button>
ad_accountExpirationDate	Organization Name	ad_accountExpirationDate	Text	03/11/2022 00:16:20	graadmin			<button>Edit</button> <button>Delete</button>
ad_accountExpires	Organization Name	ad_accountExpires	Text	03/11/2022 00:16:20	graadmin			<button>Edit</button> <button>Delete</button>
ad_c	Organization Name	ad_c	Text	03/11/2022 00:16:20	graadmin			<button>Edit</button> <button>Delete</button>
ad_cn	Organization Name	ad_cn	Text	03/11/2022 00:16:20	graadmin			<button>Edit</button> <button>Delete</button>
ad_co	Organization Name	ad_co	Text	03/11/2022 00:16:20	graadmin			<button>Edit</button> <button>Delete</button>
ad_company	Organization Name	ad_company	Text	03/11/2022 00:16:20	graadmin			<button>Edit</button> <button>Delete</button>
ad_countryCode	Organization Name	ad_countryCode	Text	03/11/2022 00:16:20	graadmin			<button>Edit</button> <button>Delete</button>
ad_department	Organization Name	ad_department	Text	03/11/2022 00:16:20	graadmin			<button>Edit</button> <button>Delete</button>
ad_description	Organization Name	AD Description	Text	09/13/2023 03:04:18	graadmin			<button>Edit</button> <button>Delete</button>

Pipelines Creation for respective data sources



Dashboard Investigate Studio Respond Reports **Pipelines** Configure ...

Open Cases 50

Ingestion Add Pipeline >

Organiz... | Ingestion | Add Pipeline > | Load >

ACCOUNT ENTITLEMENTS	ACCOUNTS	ACTIVITY	ENTITIES	ENTITLEMENTS	FEEDS	GRA USER	POLICIES	RESOURCE ATTRIBUTES	RESOURCES	ROLE ENTITLEMENTS	ROLES	Showing 28 of 28	Data	...	
USERS															
Name	Tenant Name	Data Source	↑	Resource	Status	History	Action								
Okta_Base_Line_Data_Ingestion	Organization Name	DefaultFileSystem		Okta	Enabled										
PaloAltoGlobalProtectData	Organization Name	DefaultFileSystem		Palo Alto Global Protect	Enabled										
Phase1-PhishingDataSimulator	Organization Name	DefaultFileSystem		Email	Enabled										
Printer_Data_Ingestion_CSV	Organization Name	DefaultFileSystem		Print	Enabled										
SharePoint_Metadata	Organization Name	DefaultFileSystem		Office 365 Sharepoint	Disabled										
SharepointDLPDemoData	Organization Name	DefaultFileSystem		Office 365 Sharepoint	Enabled										
SIEM_Vulnerability_Data_CSV_V3	Organization Name	DefaultFileSystem		tenable	Enabled										
Threat_Intelligence_Data	Organization Name	DefaultFileSystem		Threat Intelligence	Enabled										
Custom_Alert_Data_Source	Organization Name	DefaultSyslog		Suricata Alert	Enabled										
GRA Data Analytics - Consolidated Dashboard	Organization Name	DefaultSyslog		Gurucul DLP Analytics	Enabled										
GRA Syslog Threat_Intelligence_Data_ThreatFox	Organization Name	DefaultSyslog		Threat Intelligence	Disabled										
Gurucul DLP Analytics Data Ingestion - CSV Data	Organization Name	DefaultSyslog		Gurucul DLP Analytics	Enabled										

October 30th 2024 7:48:07 AM (UTC) 6

Data Ingestion Status for each pipeline



Dashboard Investigate Studio Respond Reports **Pipelines** Configure ...

Open Cases 50

Ingestion **GRA Syslog Azu...** Add Pipeline

Data Notifications

Ingestion Details From Date 10/24/2024 To Date 10/30/2024 **SHOW** Show Chart

Source DEFAULTSYSLOG **Resource** AZURE AD SIG... **Parser** **Mapping**

Source	Description	Start Time	End Time	Total Output Reco...	Total Skipped Rec...	Total Updated Rec...	Total Failed Records	Status
GRA Syslog	GRA Syslog Azure AD Sign-In	10/30/2024 04:00:09	10/30/2024 00:00:00	13	0	0	0	STREAMED
GRA Syslog	GRA Syslog Azure AD Sign-In	10/29/2024 04:00:10	10/30/2024 00:00:00	33	0	0	0	STREAMED
GRA Syslog	GRA Syslog Azure AD Sign-In	10/28/2024 04:00:09	10/29/2024 00:00:00	25	0	0	0	STREAMED
GRA Syslog	GRA Syslog Azure AD Sign-In	10/27/2024 04:00:09	10/28/2024 00:00:00	38	0	0	0	STREAMED
GRA Syslog	GRA Syslog Azure AD Sign-In	10/26/2024 04:00:03	10/27/2024 00:00:00	25	0	0	0	STREAMED
GRA Syslog	GRA Syslog Azure AD Sign-In	10/25/2024 12:16:34	10/26/2024 00:00:00	0	0	0	0	STREAMED

October 30th 2024 9:01:40 AM (UTC)

Investigate 01



New Search query

Write Custom Queries to find results for the default and custom time range

TODAY YESTERDAY LAST 24 HOURS LAST 7 DAYS LAST 30 DAYS PREVIOUS WEEK PREVIOUS MONTH PREVIOUS 3 MONTHS PREVIOUS 6 MONTHS PREVIOUS 12 MONTHS

Real Time Custom Date

Activities Anomalies Users Accounts Entities Roles Entitlements Account Entitlements Resources Peer Groups Watchlists Assets

Users can view specific Data required to initiate Investigation e.g. Activity Data, Anomalies, Users, Entities, Watchlist

How to Search

The feature enables a user to submit a specific search query and filter the data based on the query. The tabs Activities, Anomalies, Users, Accounts display the distinct values of their attributes based on the search query.

[Explore Investigate Search](#)

[Saved Queries](#)

Investigate 02 (Activities)



Here Today's data is being viewed for all the activities

Today **Activities 95.5K** **ANOMALIES** **USERS** **ACCOUNTS** **ENTITIES** **ROLES** **ENTITLEMENTS** **ACCOUNT ENTITLEMENTS** **RESOURCES** **PEER GROUPS** **WATCHLISTS** **ASSETS**

Attributes

- 200 Employee ID
- 0 hostname
- 25 Resource Name
- 200 Account Name
- 0 alerttype
- 2 application
- 200 autonomicoussystemnumber
- 200 autonomicoussystemnumber
- 0 categorycount
- 0 confidencelevel
- 0 confidencelevelint
- 116 country
- 0 Endpoint Type
- 0 eventcategory
- 200 Event
- 1 eventid
- 16 Event Type
- 0 group
- 200 hostname
- 0 iocdescription
- 0 ioctype
- 0 link2bref

Time Event

08:20:01 10/30/2024 Employee ID = nilesh@aftomathis.com Tenant Name = Organization Name Resource Name = Google Workspace License Event = Event Type = IP Address = Audit Date = 10/30/2024 08:20:04 Event Day = 10/30/2024 Machine ID = selflink = https://licensing.googleapis.com/apps/licensing/v1/product/Google-Apps/sku/1010020026/user/nilesh@aftomathis.com productid = Google-Apps kind = licensing#licenseAssignment productname = Google Workspace etags = "0g5M-vtRp0hNFOBYoqeulV4B7TqNx80pTjewPH8Y/CP4BINW60QA8igZ3bjqyBMg6Q-k" skuid = 1010020026 skuname = Google Workspace Enterprise Standard Raw Message

rawmessages = "skuName":"Google Workspace Enterprise Standard","productId":"Google-Apps","kind":"licensing#licenseAssignment","etags":"0g5M-vtRp0hNFOBYoqeulV4B7TqNx80pTjewPH8Y/CP4BINW60QA8igZ3bjqyBMg6Q-k","userId": "nilesh@aftomathis.com","skuid": "1010020026","productName": "Google Workspace",selfLink: "https://licensing.googleapis.com/apps/licensing/v1/product/Google-Apps/sku/1010020026/user/nilesh@aftomathis.com"}

08:20:01 10/30/2024 Employee ID = jh12961@aftomathis.com Tenant Name = Organization Name Resource Name = Google Workspace License Event = Event Type = IP Address = Audit Date = 10/30/2024 08:20:04 Event Day = 10/30/2024 Machine ID =

08:20:01 10/30/2024 Employee ID = apintegrationuser@aftomathis.com Tenant Name = Organization Name Resource Name = Google Work Event = Event Type = IP Address = Audit Date = 10/30/2024 08:20:04 Event Day = 10/30/2024 Machine ID =

08:20:00 10/30/2024 Employee ID = Tenant Name = Organization Name Resource Name = Fortinet Event = Event Type = signature Audit Date = 10/30/2024 08:20:01 Event Day = 10/30/2024

08:20:00 10/30/2024 Employee ID = Tenant Name = Organization Name Resource Name = Fortinet Event = Event Type = signature Audit Date = 10/30/2024 08:20:01 Event Day = 10/30/2024

08:20:00 10/30/2024 Employee ID = Tenant Name = Organization Name Resource Name = Fortinet Event = Event Type = signature Audit Date = 10/30/2024 08:20:01 Event Day = 10/30/2024

08:20:00 10/30/2024 Employee ID = Tenant Name = Organization Name Resource Name = Fortinet Event = Event Type = signature Audit Date = 10/30/2024 08:20:01 Event Day = 10/30/2024

Users can refer enriched logs along with the raw log

October 30th 2024 8:20:31 AM (UTC) 3.5K

Investigate 03 (Users)



Dashboard Investigate **Investigate** Studio Respond Reports Pipelines Configure ...

New Search query

Total Users

Save Load Report History Add Filter Go

ACTIVITIES ANOMALIES **USERS 60.3K** ACCOUNTS ENTITIES ROLES ENTITLEMENTS ACCOUNT ENTITLEMENTS RESOURCES PEER GROUPS WATCHLISTS ASSETS

Attributes Hide 56 Department

Name & Employee ID	Tenant Name	Department & Title	Manager	Risk Identified Date	Risky Since (In Days)	User Risk
 Ken Winston kw22083	 Organization Name	Sales and Trading Senior Trust Consultant	yb36657	09/12/2024	48	HIGH 95
 Elisha Penman ep15379	 Organization Name	Equity Research Investment Management...	cv52121	09/13/2024	47	HIGH 94
 Henry Jacob hj72393	 Organization Name	Back Office Operations Desktop Support Engineer	ac23116	09/12/2024	48	HIGH 92
 James Carter jc24065	 Organization Name	IT Infrastructure Cloud Architect	bf61093	09/13/2024	47	HIGH 91
 Claire Coughlan U562427	 Organization Name	Liquidity Management Personal Banker	506898	09/12/2024	48	HIGH 87
 Anya Chappelle ac25761	 Organization Name	Consumer Lending Personal Banker	av23071	09/19/2024	41	HIGH 87
 Bo Stoneman bs41990	 Organization Name	Private Banking Anti-Money Laundering ...	mc48143	09/19/2024	41	HIGH 87
 Dylan Gauhart dg12345	 Organization Name	Fraud Prevention & ...				HIGH 87

Brief User Information along with the Risk Score

All Users 60.3K Watchlist Users 3.5K Terminated Users 73 High Risk Users 14 Departing Users 0 New Hires 0

October 30th 2024 8:25:39 AM (UTC) 10

User Profile 01



GRA Dashboard Investigate Studio Respond Reports Pipelines Configure ...

Open Cases 50

Ken Winston

ACTIVE

kw22083

Expand for more

TITLE
Senior Trust Cons...

MANAGER
yb36657

START DATE
05/19/2011

END DATE
09/01/2023

Watch list/Risk/Anomalies/Cases

WATCHLISTS 3 **RISK** 95 **ANOMALIES** 16 **CASES** 2

< Sep 08 - Sep 15 >

RISK
34% increase in risk score for time period

ANOMALIES
10 of 11 Anomalies are new for time period

ACTIVITIES

DEVICES & PLACES

09/08 09/09 09/10 09/11 09/12 09/13 09/14 09/15 09/16

MONTHLY WEEKLY DAILY From 09/08/2024 to 09/15/2024

User Profile Overview

User Profile 02



90 RISK
8:00:59 AM
09/10/2024

&

7 Anomalies detected with 392 anomalous transactions across 4 resources in a duration of 15 hrs, 52 mins, 11 secs

ACTIVITIES	ANOMALIES	CLASSIFIERS	START TIME	END TIME	DURATION
10 Ironport	TA0010: Exfiltration: Exfiltration Over Alternative Protocol - Self Email to Personal Domains	departing user gurucul MITRE -> Exfiltration -> Exfiltration O... Compliance -> CISA Insider Threat -> Data Exfiltration SEDEMO	11:07:10 PM	11:53:10 PM	46 mins

Date Specific Anomalies Detection

27	Financial Record...	TA0009: Collection: Sensitive Customer Information Exploration - Sudden Increase In Accessing Customer Portfolio Holdings	Resources -> Financial Records Applicat... MITRE -> Collection -> Data from Inform... SEDEMO Categories -> Outlier Analysis	03:02:14 PM	05:55:29 PM	2 hrs, 53 mins, 15 secs
92	Financial Record...	TA0009: Collection: Spike In Accessing Customer Contact List	Resources -> Financial Records Applicat... MITRE -> Collection -> Data from Inform... SEDEMO Categories -> Outlier Analysis	09:22:02 AM	05:59:53 PM	8 hrs, 37 mins, 51 secs
38	Financial Record...	TA0009: Collection: Sensitive Information Exploration - Spike In Accessing Customer Portfolio Details	Resources -> Financial Records Applicat... MITRE -> Collection -> Data from Inform... SEDEMO Categories -> Outlier Analysis	09:11:40 AM	06:00:52 PM	8 hrs, 49 mins, 12 secs
112	Cisco Proxy	Predictive Flight Risk - Excessive Activity on Job Sites	MITRE -> Exfiltration Categories -> Frequency Analysis Resources -> Cisco Proxy SEDEMO	08:00:59 AM	06:23:41 PM	10 hrs, 22 mins, 42 secs

112	Cisco Proxy	Career Switch Exploration Behavior - User Accessing Job Recruiting Web Sites	MITRE -> Exfiltration Categories -> Frequency Analysis Resources -> Cisco Proxy SEDEMO	08:00:59 AM	06:23:41 PM	10 hrs, 22 mins, 42 secs

CASE ID

STATUS

ACTION

143

Open

Investigate Respond

Brief information

about Anomalies

Investigate 04 (Entities)



Dashboard Investigate **Investigate** Studio Respond Reports Pipelines Configure ...

New Search query

Total Entities

Save Load Report History Go

ACTIVITIES ANOMALIES USERS ACCOUNTS **ENTITIES 31.1K** ROLES ENTITLEMENTS ACCOUNT ENTITLEMENTS RESOURCES PEER GROUPS WATCHLISTS ASSETS

Risk Score Descending Showing 30 of 31.1K

Entity Value	Tenant Name	Entity Name	First Seen & Last Seen	Risk Identified Date	Risky Since (In Days)	Risk Score
DESKTOP-WIN-198	Organization Name	hostname	hostname 06/28/2023 23:45:52 10/15/2024 19:44:28	09/12/2024	48	HIGH 95
192.168.7.40	Organization Name	Source IP Address	Source IP Address 10/04/2024 06:52:19 10/04/2024 06:52:19	10/04/2024	26	HIGH 90
192.168.7.41	Organization Name	Source IP Address	Source IP Address 09/20/2024 11:52:47 09/20/2024 11:52:47	09/18/2024	42	HIGH 89
192.168.7.47	Organization Name	Source IP Address	Source IP Address 09/20/2024 11:52:47 09/20/2024 11:52:47	09/18/2024	42	HIGH 89
192.168.7.46	Organization Name	Source IP Address	Source IP Address 09/20/2024 11:52:47 09/20/2024 11:52:47	09/19/2024	41	HIGH 89
C8033	Organization Name	Client ID	Client ID 10/11/2024 05:35:15 10/11/2024 05:35:15	10/10/2024	20	HIGH 89

Brief Entity Information along with the Risk Score
High Risk entities would be displayed at the Top

October 30th 2024
8:30:14 AM (UTC)

3.5K

Entity Profile 01



GRA Dashboard Investigate Studio Respond Reports Pipelines Configure ...

Open Cases 50

Watch list/Risk/Anomalies/Cases

WATCHLISTS	RISK	ANOMALIES	CASES
0	95	3	1

hostname DESKTOP-WIN-198

FIRST SEEN LAST SCAN DATE OPERATING SYSTEM OWNER

06/28/2023 23:45... 2024-01-16T13:19... Windows 10 U562427

LAST SEEN TYPE

10/15/2024 19:44... workstation

< Sep 08 - Sep 15 >

09/08 09/09 09/10 09/11 09/12 09/13 09/14 09/15 09/16

MONTHLY WEEKLY DAILY From 09/08/2024 to 09/15/2024

RISK
95% increase in risk score for time period

ANOMALIES
3 of 3 Anomalies are new for time period

ACTIVITIES

DEVICES & PLACES

Entity Profile Overview

Entity Profile 02



Timeline

95 RISK
9:11:21 AM
09/12/2024
&

Date Specific Anomalies Detection

3 Anomalies detected with 5 anomalous transactions across 2 resources in a duration of 3 mins, 57 secs

ACTIVITIES	ANOMALIES	CLASSIFIERS	START TIME	END TIME	DURATION
2 Carbon Black	Carbon Black - Medium Severity Known Malware Detected	Categories > Host Compromise Resources > Carbon Black MITRE > Command and Control	09:15:18 AM	09:15:18 AM	
2 Carbon Black	Threat Chain: Malicious File Download Followed by EDR Known Malware Alert	Resources > Carbon Black Categories > Suspicious or Malicious B... MITRE > Command and Control Categories > Command and Control	09:11:21 AM	09:15:18 AM	3 mins, 57 secs
1 Zscaler Proxy	Zscaler Proxy - Suspicious Payload Download	Categories > Host Compromise Categories > Suspicious or Malicious B... Resources > Zscaler Proxy MITRE > Execution	09:11:21 AM	09:11:21 AM	

Brief information about Anomalies

CASE ID	STATUS	ACTION
155	Open	Investigate Respond

8:48:31 AM (UTC)



15

Investigate 05 (Resources)



Dashboard Investigate **Investigate** Studio Respond Reports Pipelines Configure ...

Open Cases 50 Save Load History Go

Total Resources

New Search query

ACTIVITIES ANOMALIES USERS ACCOUNTS ENTITIES ROLES ENTITLEMENTS ACCOUNT ENTITLEMENTS **RESOURCES 3.2K** PEER GROUPS WATCHLISTS ASSETS

Attributes Hide

12 Owner
7 Resource Class
2 Asset Value

Name & Resource Group	Tenant Name	Resource Class & Resource Type	Owner	Risk Identified Date	Risky Since (In Days)	Risk Score
Windows Security Operating Systems	Organization Name	PROD Application	graadmin	09/11/2024	49	HIGH 95
Microsoft 365 E5	Organization Name	PROD Application	graadmin	03/01/2024	243	HIGH 88
Google Workspace Cloud Applications	Organization Name	PROD Application	graadmin	10/08/2024	22	HIGH 87
Azure AD Sign-In Cloud Applications	Organization Name	PROD Application	graadmin	09/19/2024	41	HIGH 87
Digital Guardian DLP	Organization Name	PROD Application	graadmin	06/19/2024	133	HIGH 87
Zscaler Proxy Proxy	Organization Name	PROD Application	graadmin	09/18/2024	42	HIGH 87
Okta DEFAULT	Organization Name	PROD Application	graadmin	05/29/2024	154	HIGH 87
Financial Records		PROD	graadmin			

Firewall 664 **Cloud Application** 453 **DEFAULT** 191 **DLP** 170 **Threat Intelligence** 122 **Operating System** 117

Brief Resource Information along with the Risk Score High Risk Resources would be displayed at the Top

October 30th, 2024 8:33:01 AM (UTC) 3.5K 16

Investigate 06 (Watchlist)



Dashboard Investigate Studio Respond Reports Pipelines Configure History

New Search query Admins/Analyst can have their customized watch list to track the high risk/potentially high risks users/entities

ACTIVITIES ANOMALIES USERS ACCOUNTS ENTITIES ROLES ENTITLEMENTS ACCOUNT ENTITLEMENTS RESOURCES PEER GROUPS WATCHLISTS 3.5K ASSETS

User Risk Descending Showing 30 of 3.5K

Name & Employee ID	Tenant Name	Department & Title	Manager	Risk Identified Date	Risky Since (In Days)	User Risk	User Risk
Ken Winston kw22083	Organization Name	Sales and Trading Senior Trust Consultant	yb36657	09/12/2024	48	HIGH	95
Elisha Penman ep15379	Organization Name	Equity Research Investment Management Ope...	cv52121	09/13/2024	47	HIGH	94
Henry Jacob hj72393	Organization Name	Back Office Operations Desktop Support Engineer	ac23116	09/12/2024	48	HIGH	92
James Carter jc24065	Organization Name	IT Infrastructure Cloud Architect	bf61093	09/13/2024	47	HIGH	91
Claire Coughlan U562427	Organization Name	Liquidity Management Personal Banker	506898	09/12/2024	48	HIGH	87
Jack Hicks jh12961	Organization Name	Back Office Operations Custody Investment Specialist	ad33001	10/08/2024	22	HIGH	85
Markus Jones mj36141	Organization Name	Sales and Trading Custody Investment Specialist	tg26926	09/11/2024	49	HIGH	84
Janet Filson jf12345	Organization Name	Business Banking					

October 30th 2024 8:54:22 AM (UTC) 3.5K



GRA Dashboard Investigate **Studio** Respond Reports Pipelines Configure ...

Open Cases 50

Organizati... Add Canvas **Studio** ENABLE ALL ON Load

Models

Showing 30 of 176

Model Name	Tenant Name	Added Date	Added By	Modified Date	Modified By	History	Action
Zscaler Proxy - Suspicious Payload Download	Organization Name	08/24/2023 20:09:24	graadmin	10/15/2024 16:30:30	amol.bhagwat	Audit History	
Zscaler Proxy - Payload Delivery - Rare Website Access followed by Document Download	Organization Name	07/26/2023 00:59:30	graadmin	09/14/2024 05:37:50	graadmin	Audit History	
Windows Security - User Added and Removed from Security Group in Short Time Span	Organization Name	10/15/2024 19:58:12	mikel.s	10/15/2024 19:59:10	mikel.s	Audit History	
Windows Security - Kerberoasting Attack	Organization Name	10/15/2024 19:09:07	mikel.s	10/15/2024 19:35:46	mikel.s	Audit History	
Windows Security - Excessive Kerberos Tickets Requested in Short Period of Time	Organization Name	10/15/2024 19:54:17	mikel.s			Audit History	
Windows Host - Pass	Organization Name	09/19/2024 19:30:32	graadmin	09/19/2024 21:24:26	graadmin	Audit History	

Models 02



Dashboard Investigate **Studio** Respond Reports Pipelines Configure Open Cases 50 Profile Logout G

Studio Windows Secu... Add Canvas ENABLE ON CLONE PREVIEW EXECUTE MODEL Findings Load

Data Models Risk Aggregation Visualize Actions Configuration

Entity HOSTNAME Resource WINDOWS SECU... Model WINDOWS SECU... Filter 5 MINUTES Resource WINDOWS SECU...
Model WINDOWS SECU... Filter 120 MINUTES Resource WINDOWS SECU... Model WINDOWS SECU...

Edit Behavior Model

TEMPLATE NAME: Pattern Recognition on Feature

NEW MODEL NAME: * Windows Security - Kerberos

MODEL DESCRIPTION: This template is used to detect threats based on the known single or multi-feature data

TARGET ATTRIBUTE: hostname

FEATURE ATTRIBUTES: eventtype

FEATURE DATA: 4732

FEATURE CRITERIA

Update

October 30th 2024 9:08:10 AM (UTC) 3.5K

Custom Dashboards 01 (Admin)



GRF Dashboard Investigate Studio Respond Reports Pipelines Configure ...

Open Cases 50

MI - Admin Dashboard

Activity Trend

Top Resource Activity Trend

Resource	Activity Count
DHCP	15.7K
Ironport	14.8K
Proxy	14.8K
Fortinet	12K
Juniper OS	11K

Risky Resources Count: 7

Active Agents Count: 0

Inactive Agents Count: 22

Open Alerts Count: 2K

Incident Alerts Count: 0

Alerts

Ingested Activities - Real time

Resources Trend

Open Cases

Active Running Jobs

Job Name	Status
reportJobName	0%
Okta_Real_Time_Logs_Se	100%

SEE ALL >

Ingested Activities Overview

Cases

Case ID	Owner	Status
WIN-57KCGQ6C9US	GRADMIN	OPEN
ec29027	GRADMIN	OPEN
f117857	GRADMIN	OPEN
C8033	GRADMIN	OPEN
C8009	GRADMIN	OPEN

SEE ALL >

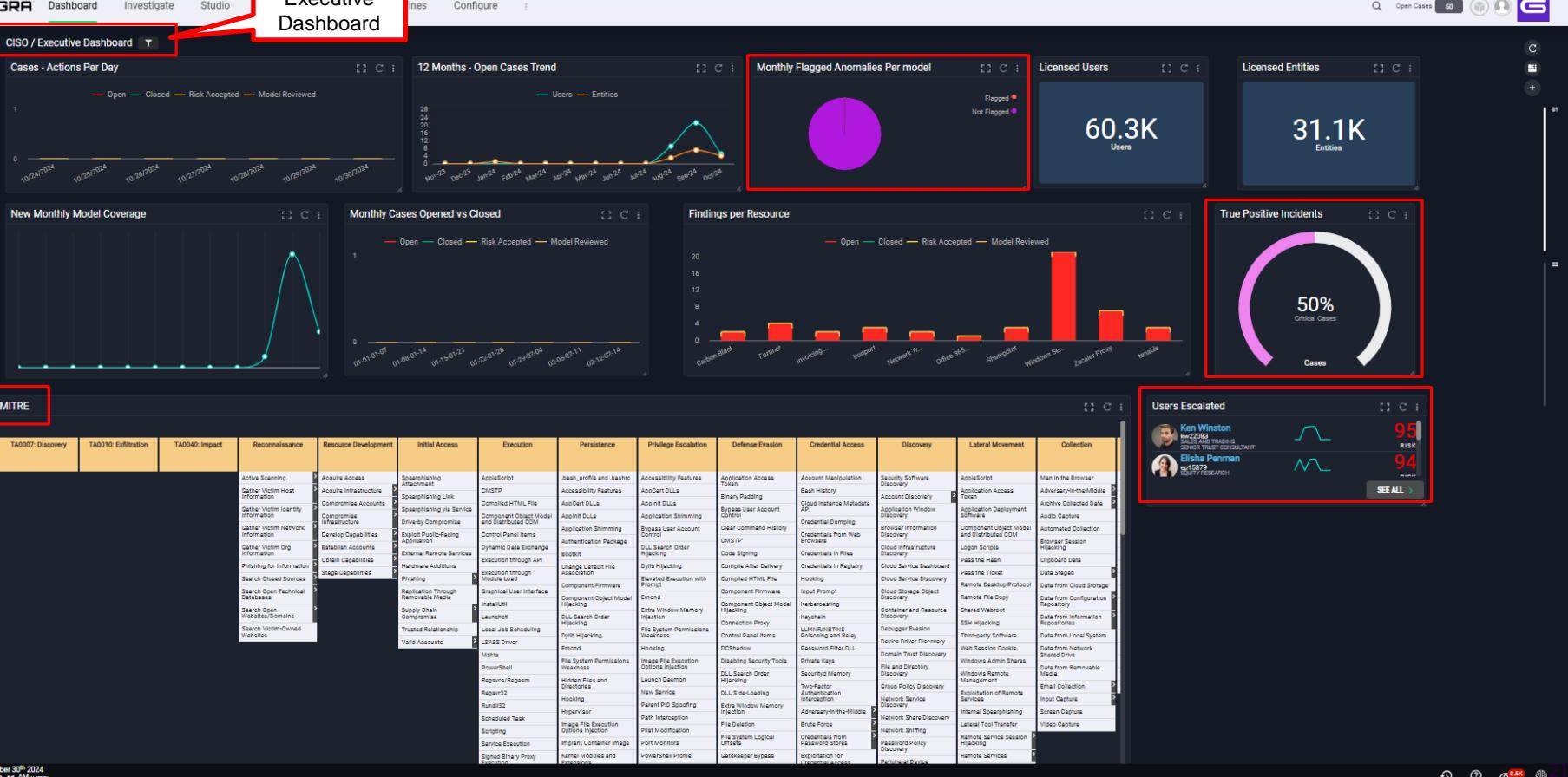
October 30th 2024
9:16:57 AM (UTC)

20

Custom Dashboards 02 (Executive)



Executive Dashboard



Custom Dashboards 03 (Compliance)



Dashboard Investigate Studio Respond Reports Pipelines Configure Open Cases 50 User G

ITDR Insights Dashboard

Monitored Users: 60.3K Accounts: 75.9K Service Accounts: 134 Identity Sources: 17.3K ITDR Alerts: 0 ITDR Cases: 1 Entitlements: 27.5K

Top ITDR Alerts

ITDR Risky Users

ITDR Risky Privileged Users

ITDR Risky Service Accounts

Initial Access / Phishing

Session Hijacking

Account Compromise

DC Attacks

Rare / Risky Geo location

Authentication Failed - Last 24 Hrs

Accounts Locked Out - Last 24 Hrs

Policy Configuration Changes

My Dashboards

Compliance

Monitoring

Compliance - FISMA

Compliance - GDPR

Compliance - GLBA

Compliance - GPG 13

Compliance - HIPAA

Compliance - ISLP

Compliance - ISO

Compliance - NERC CIP

Compliance - NESA UAE

Compliance - Network Firewall Monitoring

Compliance - Network Traffic Monitoring

Compliance - NIST

Compliance - PCI DSS

Compliance - PDPA

Add new Widget

Compliance Dashboards

Add new Dashboard

October 30th 2024
9:11:09 AM (UTC)

22

Custom Dashboards 04 (MITRE)



GR4 Dashboard Investigate Studio Respond Reports Pipelines Configure : Open Cases 50 Profile Logout Help

1-MITRE Dashboard ▼

MITRE Incidents by Data Source

Recent True Positive TTPs

MITRE

TA0007: Discovery	TA0010: Exfiltration	TA0040: Impact	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Active Scanning			Acquire Access	Spearphishing Attachment	AppleScript	bash_profile and bashrc	Accessibility Features	Application Access Token	Account Manipulation	Security Software Discovery	AppleScript	Man in the Browser	
Gather Victim Host Information			Acquire Infrastructure	Spearphishing Link	CMSTP	Accessibility Features	AppCert DLLs	Binary Padding	Bash History	Account Discovery	Application Access Token	Adversary-in-the-Middle	
Gather Victim Identity Information			Compromise Accounts	Spearphishing via Service	Compiled HTML File	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Cloud Instance Metadata API	Application Window Discovery	Application Deployment Software	Archive Collected Data	
Gather Victim Network Information	4	1	Compromise Infrastructure	Drive-by Compromise	Component Object Model and Distributed COM	Application Shimming	Application Shimming	Clear Command History	Credential Dumping	Browser Information Discovery	Component Object Model and Distributed COM	Audio Capture	
Gather Victim Org Information			Develop Capabilities	Exploit Public-Facing Application	Control Panel Items	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Cloud Infrastructure Discovery	Component Object Model and Distributed COM	Automated Collection	
Phishing for Information			Establish Accounts	External Remote Services	Execution through API	Bootkit	DLL Hijacking	Compiled HTML File	Credentials in Files	Credentials from Web Browsers	Logon Scripts	Browser Session Hijacking	
Search Closed Sources			Obtain Capabilities	Hardware Additions	Execution through Module Load	Change Default File Association	Elevated Execution with Prompt	Component Firmware	Cloud Service Dashboard	Cloud Infrastructure Discovery	Pass the Hash	Clipboard Data	
Search Open Technical Databases			Stage Capabilities	Replication Through Removable Media	Graphical User Interface	Component Object Model Hijacking	Emond	Component Firmware	Cloud Service Discovery	Cloud Storage Object Discovery	Pass the Ticket	Data Staged	
Search Open Websites/Domains			Supply Chain Compromise	InstallUtil	DLL Search Order Hijacking	Extra Window Memory Injection	Extra Window Memory Injection	Kerberoasting	Container and Resource Discovery	Cloud Storage Object Discovery	Remote Desktop Protocol	Data from Cloud Storage	
Search Victim-Owned Websites			Trusted Relationship	LaunchUtil	File System Permissions Weakness	File System Permissions Weakness	File System Permissions Weakness	Keychain	Debugger Evasion	Container and Resource Discovery	Shared Webroot	Data from Configuration Repository	
			Valid Accounts	Local Job Scheduling	Dylib Hijacking	Hooking	Hooking	LLMNR/NBT-NS Poisoning and Relay	Device Driver Discovery	Cloud Storage Object Discovery	SSH Hijacking	Data from Information Repositories	
				LSASS Driver	LSASS Driver	DCShadow	Image File Execution Options Injection	Disabling Security Tools	Domain Trust Discovery	Domain Trust Discovery	Third-party Software	Data from Local System	
				Mehra	Emond	File System	File System	Private Keys	Windows Admin Shares	Windows Admin Shares	Web Session Cookie		

October 30th 2024 9:28:55 AM (UTC) 3.5K 23

Reports 01



Dashboard Investigate Studio Respond **Reports** Pipelines Configure :

Open Cases 50

REPORT **MANAGE**

Reports

10
8
6
4
2
0 October 01 Today

CLASSIFIERS

Report Name	Description	Type	Administrator	Created Date	History	Action
13 Clear History Summary Report	SOX Compliance Report	Custom Reports	graadmin	10/11/2023 05:49:46	View History	Run Now
7 Weekly Network DOS Summary Report	NESA Compliance Report	Custom Reports	graadmin	10/11/2023 07:03:44	View History	Run Now
AAAzureAD_Login	reportDesc_1696443918157	Investigate Queries	graadmin	07/06/2023 11:21:26	View History	Edit Run Now Delete
Access Collector Report	Listing of users and associated accounts that have not been used for a period of time	User Reports	graadmin	03/11/2022 00:16:15	View History	Run Now
Activity by Country	reportDesc_1725032165621	Investigate Queries	fernando.arias@gurucul.com	08/30/2024 15:36:56	View History	Edit Run Now Delete
Activity Details By Department Report	List of Activities Grouped by Department	Custom Reports	grauser	03/11/2022 00:16:15	View History	Edit Run Now

October 30th 2024
9:31:54 AM (UTC) 3.5K 24

Reports 02



Report Name ↑	Description	Type	Administrator	Created Date	History	Action
AAAzureAD_Login	reportDesc_1696443918157	Investigate Queries	 graadmin	07/06/2023 11:21:26	View History	Edit Run Now Delete
<div style="display: flex; justify-content: flex-end; align-items: center;">Execution Date Descending Showing 3 of 3 Search ⚙</div>						
Report Id	Report Name	Description	Report Category	Format	Execution Date ↓	Action
1696443938868	AAAzureAD_Login	reportDesc_1696443918157	Investigate Queries	PDF	10/04/2023	Download Delete
1696443854347	AAAzureAD_Login	reportDesc_1696443836226	Investigate Queries	PDF	10/04/2023	Download Delete
1688642486566	AAAzureAD_Login	reportDesc_1688642410827	Investigate Queries	PDF	07/06/2023	Download Delete



UPLOAD REPORTS

Reports

Choose file to upload to GRA, you can either browse for it on your computer or simply drag and drop into a box outlined below.

[BROWSE](#)

Reports 04



Dashboard Investigate **Reports** Pipelines Configure ...

New Search query

TODAY YESTERDAY LAST 24 HOURS LAST 7 DAYS LAST 30 DAYS PREVIOUS WEEK PREVIOUS MONTH PREVIOUS 3 MONTHS PREVIOUS 6 MONTHS PREVIOUS 12 MONTHS

Real Time Custom Date

ACTIVITIES ANOMALIES USERS ACCOUNTS ENTITIES ROLES ENTITLEMENTS ACCOUNT ENTITLEMENTS RESOURCES PEER GROUPS WATCHLISTS ASSETS

Add Alert Save Load **Report** History

Add Filter Go

Execute Report For Query

SAVED QUERIES NEW SEARCH QUERY

SAVED SEARCH QUERIES Select... Select Saved Search from drop-down

REPORT NAME Enter Report Name

REPORT DESCRIPTION reportDesc_1730281188520

JOB NAME reportJobName_1730281188520

CLASSIFIER NAME Investigate Queries

TENANTS Select Tenants

SELECT ALL

EXPORT FIELDS

START

How to Search

The feature enables a user to submit a specific search query and filter the data based on the query. The tabs Activities, Users, Accounts display the distinct values of their attributes based on the search query.

[Explore Investigate Search](#)

[Saved Queries](#)

Query based custom reports can be run as per business need

October 30th 2024
9:40:00 AM (UTC)

Open Cases 50

3.5K

7

Data Export 01 (Investigate)



GRA Dashboard **Investigate** Studio Respond Reports Pipelines Configure ...

New Search query

Open Cases 50

Add Alert Save Load Report History

Real Time Custom Date

Add Filter Go

TODAY YESTERDAY LAST 24 HOURS LAST 7 DAYS LAST 30 DAYS PREVIOUS WEEK PREVIOUS MONTH PREVIOUS 3 MONTHS PREVIOUS 6 MONTHS PREVIOUS 12 MONTHS

ACTIVITIES 109.6K ANOMALIES USERS ACCOUNTS ENTITIES ROLES ENTITLEMENTS ACCOUNT ENTITLEMENTS RESOURCES PEER GROUPS WATCHLISTS ASSETS

Attributes Hide

Time Event

Time	Event	Resource Name	Tenant Name	Event	Event Type	IP Address	Audit Date	Event Day
09:43:00 10/30/2024	Resource Name = GRA Agent	Tenant Name = Organization Name	Event = 2024-10-30 09:43:00 INFO scheduled execution at 2024-10-30 09:43:00	Event Type = heartbeat	IP Address = 192.168.6.22	Audit Date = 10/30/2024 09:43:03	Event Day = 10/30/2024	
09:43:00 10/30/2024	Resource Name = GRA Agent	Tenant Name = Organization Name	Event = 2024-10-30 09:43:00 INFO scheduled execution at 2024-10-30 09:43:00	Event Type = heartbeat	IP Address = 192.168.6.28	Audit Date = 10/30/2024 09:43:03	Event Day = 10/30/2024	
09:43:00 10/30/2024	Resource Name = GRA Agent	Tenant Name = Organization Name	Event = 2024-10-30 09:43:00 INFO scheduled execution at 2024-10-30 09:43:00	Event Type = heartbeat	IP Address = 192.168.6.30	Audit Date = 10/30/2024 09:43:03	Event Day = 10/30/2024	
09:43:00 10/30/2024	Resource Name = GRA Agent	Tenant Name = Organization Name	Event = 2024-10-30 09:43:00 INFO scheduled execution at 2024-10-30 09:43:00	Event Type = heartbeat	IP Address = 192.168.6.161	Audit Date = 10/30/2024 09:43:03	Event Day = 10/30/2024	
09:43:00 10/30/2024	Resource Name = GRA Agent	Tenant Name = Organization Name	Event = 2024-10-30 09:43:00 INFO scheduled execution at 2024-10-30 09:43:00	Event Type = heartbeat	IP Address = 192.168.6.74	Audit Date = 10/30/2024 09:43:03	Event Day = 10/30/2024	
09:43:00 10/30/2024	Resource Name = GRA Agent	Tenant Name = Organization Name	Event = 2024-10-30 09:43:00 INFO scheduled execution at 2024-10-30 09:43:00	Event Type = heartbeat	IP Address = 192.168.6.62	Audit Date = 10/30/2024 09:43:03	Event Day = 10/30/2024	
09:43:00 10/30/2024	Resource Name = GRA Agent	Tenant Name = Organization Name	Event = 2024-10-30 09:43:00 INFO scheduled execution at 2024-10-30 09:43:00	Event Type = heartbeat	IP Address = 192.168.6.20	Audit Date = 10/30/2024 09:43:03	Event Day = 10/30/2024	
09:43:00 10/30/2024	Resource Name = GRA Agent	Tenant Name = Organization Name	Event = 2024-10-30 09:43:00 INFO scheduled execution at 2024-10-30 09:43:00	Event Type = heartbeat	IP Address = 192.168.6.18	Audit Date = 10/30/2024 09:43:03	Event Day = 10/30/2024	
09:43:00 10/30/2024	Resource Name = GRA Agent	Tenant Name = Organization Name	Event = 2024-10-30 09:43:00 INFO scheduled execution at 2024-10-30 09:43:00	Event Type = heartbeat	IP Address = 192.168.6.88	Audit Date = 10/30/2024 09:43:03	Event Day = 10/30/2024	
09:43:00 10/30/2024	Resource Name = GRA Agent	Tenant Name = Organization Name	Event = 2024-10-30 09:43:00 INFO scheduled execution at 2024-10-30 09:43:00	Event Type = heartbeat	IP Address = 192.168.6.31	Audit Date = 10/30/2024 09:43:03	Event Day = 10/30/2024	

100% Options Show Chart

Excel CSV Tabular Layout Visualize Modes

109.6K

Data Export 02 (Dashboard)



Dashboard Investigate Studio Respond Reports Pipelines Configure ...

Open Cases 50

Dashboard Options
Owner: graham.read

Auto Arrange
 Rename
 Share
 Duplicate
 Export (highlighted with a red box)
 Set As Default
 Refresh
 Change Owner
 Download
 Email
Delete Dashboard

Source (Bar Chart): Open (red), Closed (green), Risk Accepted (yellow), Model Reviewed (orange). Legend: Open (red), Closed (green), Risk Accepted (yellow), Model Reviewed (orange). Data: Carbon Black, Fortinet, Ivanti, Iport, Network Tr..., Office 365, Sharepoint, Windows Se..., Zscaler Proxy, tenable.

Recent True Positive TTPs (Donut Chart): Brute Force Authentication Attempts - Failed Logon (orange), Successful login attempt after continuous failed logons (yellow), Privilege Escalation - Spike in Member Removal (blue), User Added to Local Admin Group - Update (yellow), Exploitation for Privilege Escalation - Self Privileged User (purple), Golden Ticket Attack Detection - Windows Security (green), Logon Scripts: Lateral Movement Persistence: (orange).

Entire Dashboard data can be exported in PDF format

Data Export 03 (Reports)



Dashboard Investigate Studio Respond **Reports** Pipelines Configure :

Open Cases 50

Run Now

JOB NAME * reportJobName_173028187179:
JOB DESCRIPTION * reportJobDesc_1730281871795

REPORT NAME * reportDisplayName_173028187179:

TENANTS Select Tenants

EXPORT FORMAT * PDF CSV **PDF** TXT

RUN NOW SET SCHEDULE

Reports Can be Downloaded in CSV, PDF and TXT format

Report Name Description Type Administrator Created Date History Action

Report Name	Description	Type	Administrator	Created Date	History	Action
User Access - Windows - Report	Secure Configuration, Investigate Queries	Administrator	09/20/2024 09:07:57	View History		
Compliance - Cyber Essentials - User Account Changes - Windows - Report	Cyber Essentials Requirement D.2 Secure Configuration	Investigate Queries	arti.kane@gurucul.com	09/25/2024 08:58:49	View History	
Compliance - Cyber Essentials - User Account Validation - Report	Cyber Essentials Requirement D.2 Secure Configuration,	Investigate Queries	arti.kane@gurucul.com	09/25/2024 08:38:47	View History	
Compliance - Cyber Essentials - User Group Changes - Windows - Report	Cyber Essentials Requirement D.2 Secure Configuration	Investigate Queries	arti.kane@gurucul.com	09/25/2024 08:55:13	View History	
Compliance - ECC - Account Group Changes - Report	Cybersecurity event logs and monitoring management	Investigate Queries	graadmin	08/29/2024 12:47:28	View History	

Report Id Report Name Description Report Category Format Execution Date Action

Report Id	Report Name	Description	Report Category	Format	Execution Date	Action
1724935649053	Compliance - ECC - Account Group Changes - Report	Cybersecurity event logs and monitoring management	Investigate Queries	PDF	08/29/2024	

October 30th 2024 9:51:23 AM (UTC) 3.5K

Export 04 (User/Entity Profile)



Profile Option

- [Export](#) (highlighted with a red box)
- [Unmask Attributes](#)

Johnston

TITLE Senior Trust Cons...	MANAGER yb36657	START DATE 05/19/2011	END DATE 09/01/2023
DEPARTMENT Sales and Trading			

< Sep 08 - Sep 12 >

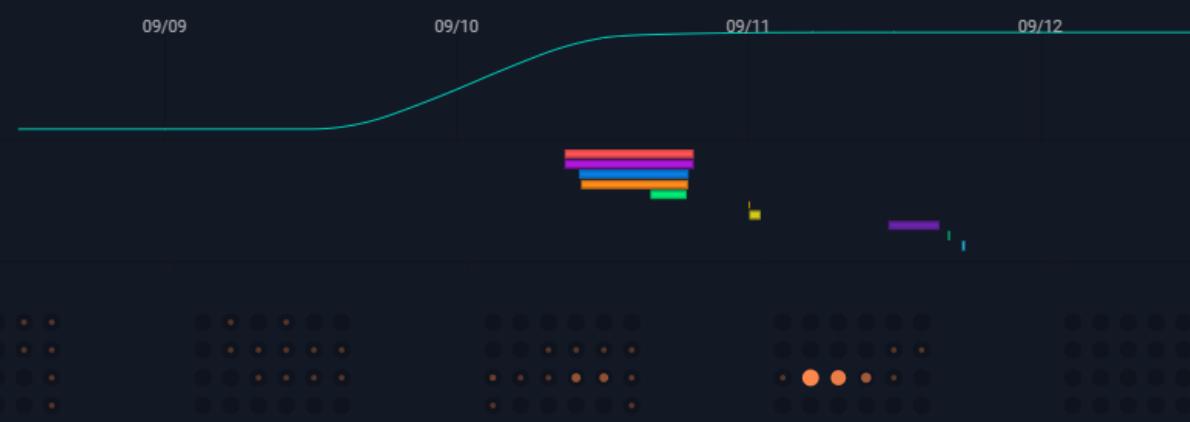
RISK
34% increase in risk score for time period

ANOMALIES
10 of 11 Anomalies are new for time period

ACTIVITIES >

DEVICES & PLACES >

User/Entity Profile can be downloaded in PDF format



Case Management 01 (Case)



GRA Dashboard Investigate Studio **Respond** Reports Pipelines Configure ...

Open Cases 50

Organizational Structure | Cases Alerts Playbook Certifications

From 09/15/2024 to 10/14/2024

PREVIOUS WEEK PREVIOUS MONTH

Cases

16 OPEN 0 CLOSED 0 RISK ACCEPTED 0 MODEL REVIEWED

Threat Distribution

CLASSIFIERS

Threat Intelligence Resources: MITRE: ITDR: Fraud: Categories:

September 15 to October 14

High (Yellow) Critical (Red)

Anomaly Count Ascending Showing 16 of 16 Search

Case Id	Tenant Name	Anomaly Count	Name & Employee ID	Entity	Status	Open Date	Risk Date	Owner Name	Risk Score	History	Action
CS-158	Organization Name	1	Dylon Gayhart dg37177	dg37177	Open	09/20/2024	09/18/2024	graadmin	High 87		
CS-159	Organization Name	1	Bo Stone... bs41990	bs41990	Open	09/20/2024	09/19/2024	graadmin	High 87		
CS-160	Organization Name	1	Anya Chapp... ac25761	ac25761	Open	09/20/2024	09/19/2024	graadmin	High 87		
CS-161	Organization Name	1		192.168.7.47	Open	09/20/2024	09/18/2024	graadmin	High 89		
CS-162	Organization Name	1		192.168.7.41	Open	09/20/2024	09/18/2024	graadmin	High 89		

October 30th 2024 10:06:19 AM (UTC) 32

Case Management 02 (Case)



Case Id	Tenant Name	Anomaly Count ↑	& Employee ID	Entity	Status	Open Date	Risk Date	Owner Name	Risk Score	History	Action
CS-158	Organization Name	1	Dylon Gayhart dg37177	 dg37177	Open	09/20/2024	09/18/2024	 graadmin	HIGH 87	 View History	 Investigate  Respond
Date  Descending  Search  											
Anomaly Name	Resource Name	Event Desc	Event By	Event By Type	Assignee	Assignee Type	Date ↓	Comment		Action	
User Accessing Phishing URL Detected by TI - Zscaler Proxy	Zscaler Proxy	Opened	graadmin	User	Platform ReadOnly	Role	09/20/2024 12:27:29				
User Accessing Phishing URL Detected by TI - Zscaler Proxy	Zscaler Proxy	Opened	graadmin	User	graadmin	Role	09/20/2024 12:27:29				

Case Management 03 (Actions)



Case Id	Tenant Name	Anomaly Count ↑	Name & Employee ID	Entity	Status	Open Date	Risk Date	Owner Name	Risk Score	History	Action
CS-158	Organization Name	1	Dylon Gayhart dg37177	(B) dg37177	Open	09/20/2024	09/18/2024	gradmin	HIGH 87	ⓘ View History	Q Investigate ↗ Respond
CS-159	Organization Name	1	Bo Stone... bs41990	(B) bs41990	Open	09/20/2024	09/19/2024	gradmin	HIGH 87	ⓘ View History	Q Investigate
CS-160	Organization Name	1	Anya Chapp... ac25761	(B) ac25761	Open	09/20/2024	09/19/2024	gradmin	HIGH 87	ⓘ View History	Q Investigate
CS-161	Organization Name	1		192.168.7.47	Open	09/20/2024	09/18/2024	gradmin	HIGH 89	ⓘ View History	Q Investigate
CS-162	Organization Name	1		192.168.7.41	Open	09/20/2024	09/18/2024	gradmin	HIGH 89	ⓘ View History	Q Investigate ↗ Respond

- ⓘ Add Comments
- ⓘ Assign
- ⓘ Change Owner
- ⓘ Close
- ⓘ Close As Risk Managed
- ⓘ In Progress
- ⓘ Model Review
- ⓘ On Hold

Alerts



GRADashboard Investigate Studio **Respond** Reports Pipelines Configure ...

Open Cases 50

ALERTS CASES PLAYBOOK CERTIFICATIONS

1 MIN 5 MIN 1 HOUR 24 HOURS

Alerts

266 0 OPEN 0 IN PROGRESS 0 CLOSED 0 INCIDENT 0 NOT AN INCIDENT

Alert Id	Tenant Name	Anomaly Name	Name & Employee ID	Entity	Status	Incident Type	Classifiers	Resource Name	Detection Timestamp	Assignee	Assignee Type	Severity	Risk Score	History	Action
AL-186329	Organization Name	UserAgent - SCAN - Suspicious User-Agent Detected (friendly-scanner)	Gurucul_India...	Open			Categories > Pattern Analysis, SEDEMO, Kill Chain > Weaponization, Resources > Suricata Alert	Suricata Alert	10/29/2024 11:25:32	graadmin,Platform ReadOnly	ROLE	MEDIUM	7		
AL-186579	Organization Name	MSSQL Port Scan / Attack - Suspicious inbound to mySQL port 3306	Gurucul_AP...	Open			Categories > Pattern Analysis, SEDEMO, Resources > Suricata Alert, Kill Chain > Delivery	Suricata Alert	10/30/2024 10:05:32	graadmin,Platform ReadOnly	ROLE	MEDIUM	9		

Playbook Action



Dashboard Investigate Studio **Respond** Reports Pipelines Configure ...

Open Cases 50

Organization... CASES ALERTS **PLAYBOOK** CERTIFICATIONS ADD

Playbook Name Tenant Name Description Added Date Added By Modified By Modified Date History Action

#Block Email and Disable User Account Organization Name #Block Email and Disable User Account 09/14/2023 22:40:50 habeeb.ali@gurucul.com

Start Date Descending Showing 30 of 101 Search

Executed By	Start Date	End Date	Execution Status	Error Message	Screen Type	Execution Stage Details
paul.john@gurucul.com	10/28/2024 08:20:40	10/28/2024 08:20:40	Success		Investigate Users	
david.croteau	03/04/2024 18:33:29	03/04/2024 18:33:29	Success		Investigate Activities	
graadmin	01/12/2024 20:50:21	01/12/2024 20:50:21	Success		Investigate Activities	
graadmin	12/12/2023 16:23:52	12/12/2023 16:23:52	Success		Investigate Activities	
david.croteau	11/07/2023 17:16:17	11/07/2023 17:16:17	Success		Investigate Activities	
david.croteau	11/07/2023 15:58:52	11/07/2023 15:58:52	Success		Investigate Activities	
david.croteau	11/06/2023 14:22:12	11/06/2023 14:22:12	Success		Investigate Activities	
david.croteau	11/06/2023 14:20:59	11/06/2023 14:21:00	Success		Investigate Activities	
graadmin	09/26/2023 13:48:40	09/26/2023 13:48:40	Success		Investigate Activities	

Start Date Descending Showing 9 of 9 Search

#This playbook blocks IP #This playbook blocks IP

MITRE Mapping with Models



Dashboard Investigate Studio **Respond** Reports Pipelines Configure ...

Open Cases 50

ENABLE ALL Load

Organizational Studio Add Canvas

Models

ENABLED 105		DISABLED 2344		Showing 30 of 105 Search						
Model Name	Organization Name	Tenant Name	Classifiers	Added Date	Added By	Modified Date	Modified By	History	Action	
Zscaler Proxy - Suspicious Payload Download	Zscaler	Resources -> Zscaler Proxy, MITRE -> Execution, Categories -> Host Compromise, Categories -> Suspicious or Malicious Behavior	2023-08-24 09:24	graadmin	2024-10-15 16:30:30	amol.bhagwat		Audit History		
Windows Host - Pass The Hash Pattern	Zscaler	Organization Name	Categories -> Default, Resources -> Windows Security, MITRE -> Lateral Movement, MITRE -> Credential Access, Threat Intelligence, ITDR	2024-09-19 19:30:32	graadmin	2024-09-19 21:24:26	graadmin		Audit History	
Vulnerable Host Exploitation - ROMCOM Remote Trojan	Zscaler	Organization Name	Resources -> Carbon Black, MITRE -> Privilege Escalation, Compliance -> NIST, SEDEMO	2023-06-29 01:41:02	graadmin	2024-09-14 05:37:50	graadmin		Audit History	
User Sharing Document To External Users - Collaboration Tools - TA0010:Exfiltration	Zscaler	Organization Name	Technology Group -> Collaboration Tools, Categories -> Insider Threat - Espionage / Snooping / Hoarding, MITRE -> Exfiltration, MITRE -> Exfiltration -> Exfiltration Over	2024-10-07 19:01:25	habeeb.ali@gurucul.com	2024-10-08 06:27:40	graadmin		Audit History	

October 30th 2024
10:21:33 AM (UTC)

3.5K

Thank you