Automating Incident Response With Splunk Phantom

by Mark Cooke, General Electric

September 2018 | Version 3.0

$WHOAMI

Mark Cooke

- Staff Incident Responder at GE
- Worked in IR for 4 years
- Python hacker
- Phantom playbook developer

General Electric

Imagination at work

+300K

+300K

1

24/7

50

3

Agenda

Highlights of today's discussion

Agenda

Overview

- Driving factors for automation
- Preparing for automation
- Implementing automation
- Demonstrating automation

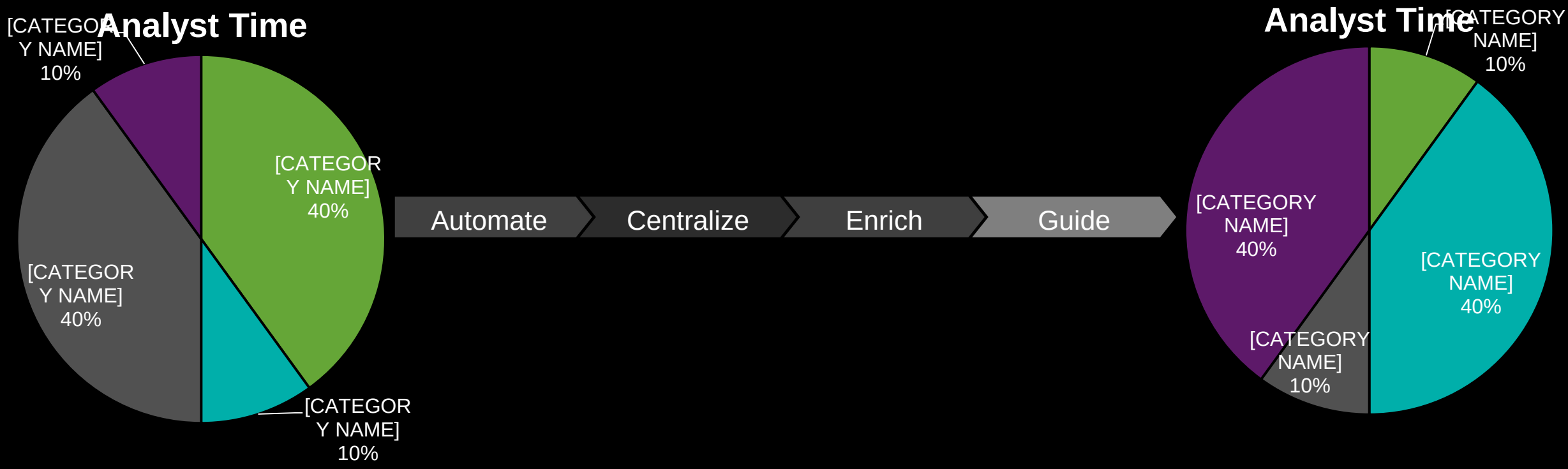
Driving Factors for Automation and Orch.

Goals for automating IR

splunk> .conf18

Driving Factors for Auto & Orch.

Analysts should primarily analyze data, NOT collect and move data around



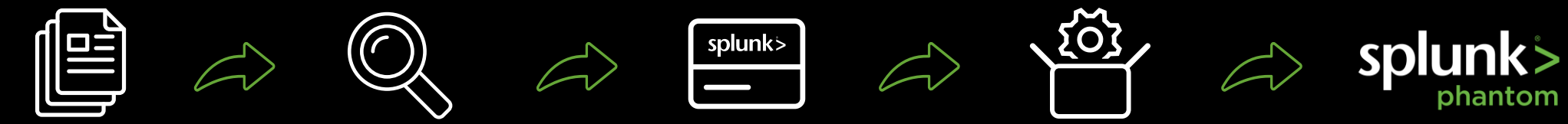
Preparing for Automation and Orch.

Designs and visions for automating IR

splunk> .conf18

Design and Vision

Gathering and moving data



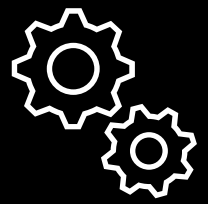
Required fields → Correlation search → Summary index → Phantom app → splunk> phantom

Design Logic:

- Consistent fields for automation
- Focused searches
- Manageable data set
- Fewer searches to move data

Design and Vision

Dividing and segmenting data flows



Automated

- Select scripts run automatically
- All decisions for triage, response and remediation are decided automatically

Semi-Automated

- Select playbooks and actions run automatically
- Analysts make triage, response and remediation decisions

Manual

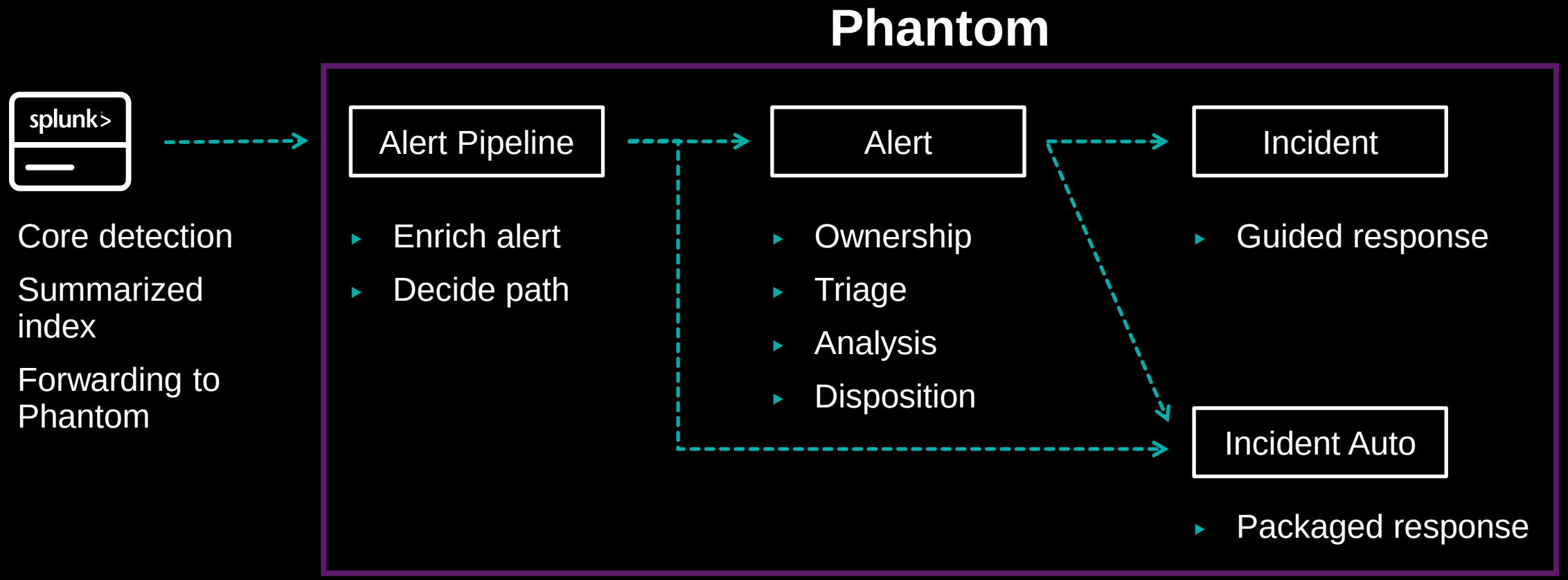
- Steps and scripts are all completed manually
- Analysts make triage, response and remediation decisions

Response Guidance

- Guide analysts through triage, response and remediation decisions
- Builds baseline for required actions
- Records incident data and actions

Design and Vision

Putting it all together



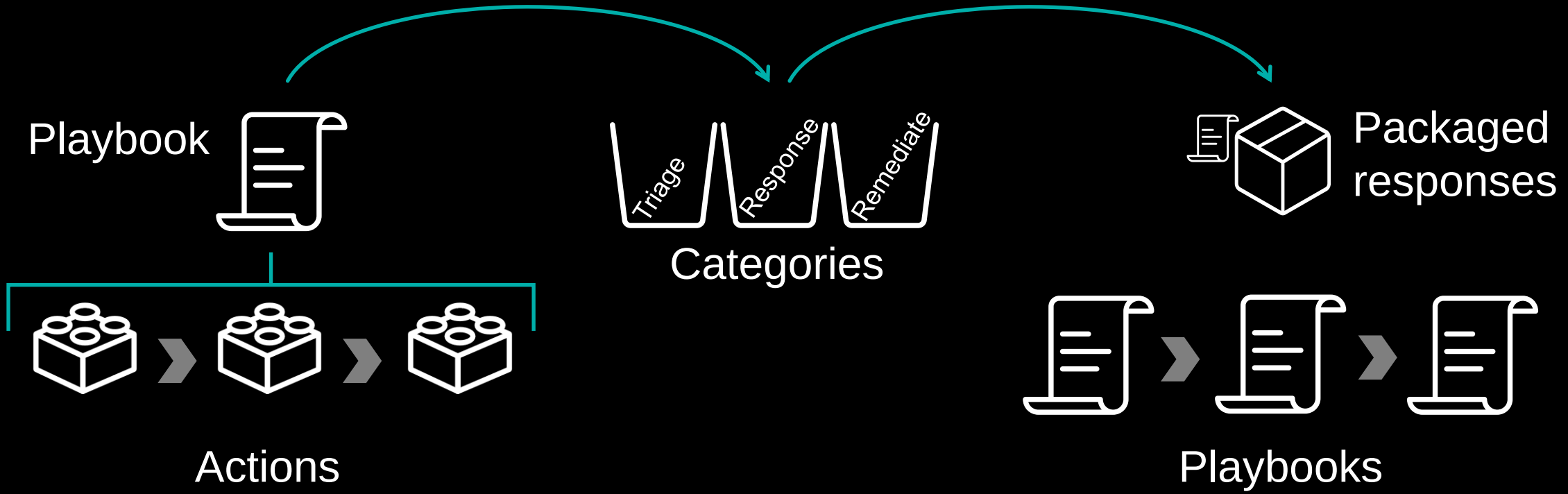
Implementing Automation and Orch.

Components for making this work

splunk> .conf18

Playbook Development

Developing playbooks



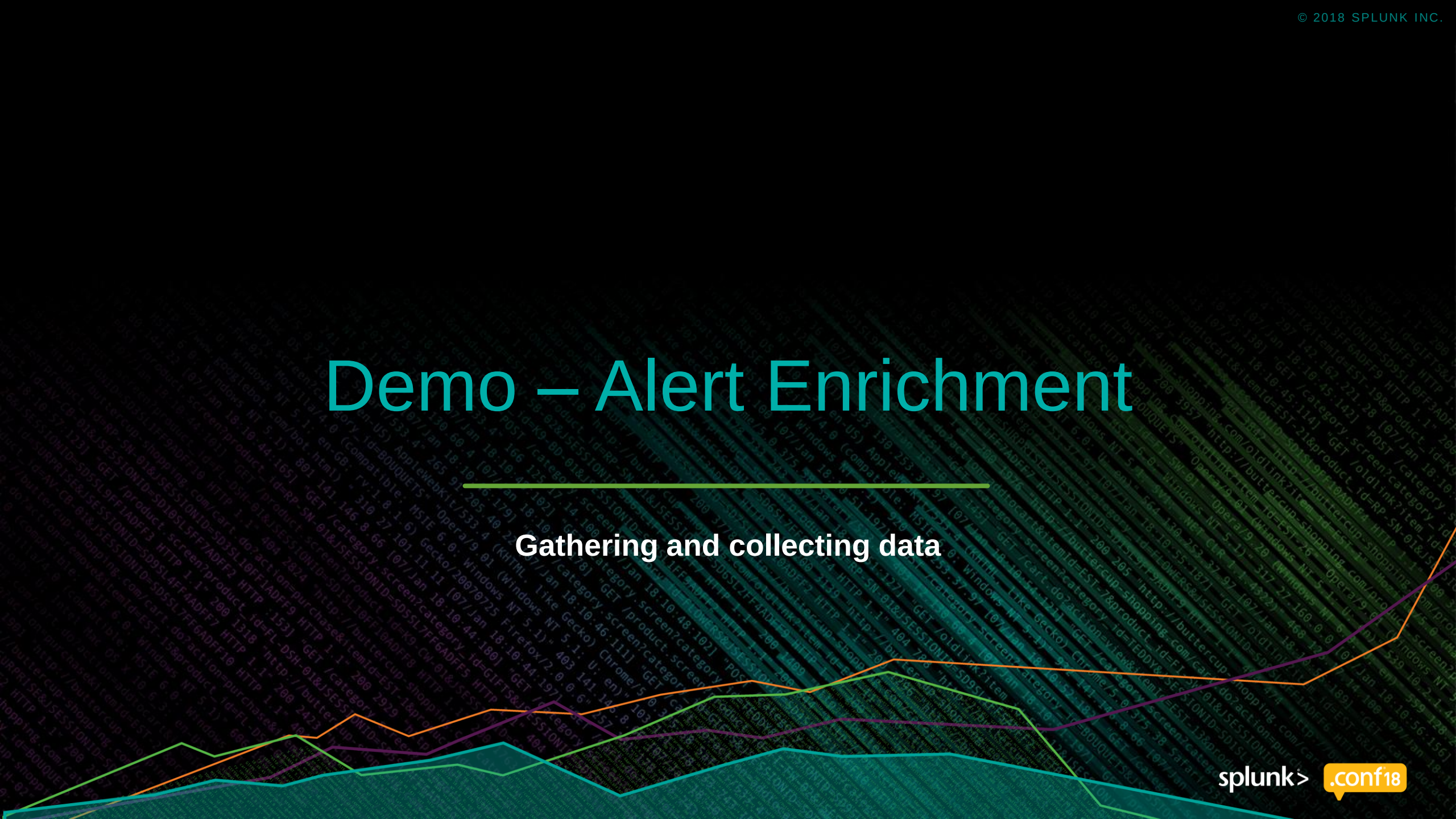
Playbook Highlights

Demo

Automation and orchestration in action

Demo – Alert Enrichment

Gathering and collecting data



Phantom | Analyst Queue

Phantom

version 3.5.210

Mark Cooke

Sources

Show Select a filter

EVENT IMPORT

Top Events

No Events

Severity

0 Low | 0 Medium | 0 High

Status

0 New | 0 Open | 0 Resolved

Top Owners

No Owners

Label: alert_pipeline CLEAR SAVE

Dynamic Updates Show Stats

ID STATUS NAME ARTIFACTS CREATED TAGS

No matching events

Phantom | Analyst Queue

Phantom

version 3.5.210

Mark Cooke

Sources

Show Select a filter

+ EVENT

IMPORT

Top Events	Severity			Status			Top Owners
1	0	1	0	1	0	0	
alert_pipeline	Low	Medium	High	New	Open	Resolved	

Label: alert_pipeline CLEAR SAVE

Dynamic Updates Show Stats

ID	STATUS	NAME	ARTIFACTS	CREATED	TAGS
132952	New	GE CIRT Malicious Behaviour Detected	1	0 minutes ago	

1

Show 50

Label: alert_pipeline CLEAR SAVE

ID	STATUS	NAME
132952	New	GE CIRT Malicious Behaviour Detected

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

alert_pipeline ID: 132952

GE CIRT Malicious Behaviour Detected

MEDIUM | TLP:RED | SLA: a day remaining | More

Owner Select... | Set Status New

Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports

▶ ACTION | ▶ PLAYBOOK | ✚ ARTIFACT

Recent Activity All

ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY	TAGS
1967811	event		0 minutes ago	0 minutes ago	MEDIUM	Mark Cooke	

Show 50 | COLLAPSE

Widgets | Notes | MANAGE WIDGETS

automation a few seconds ago

gecirt_utility_alert_pipeline

gecirt_triage_ticket_history

list tickets

1 action failed for app Request Tracker (GE)[65]

list tickets

Comment

automation a few seconds ago

gecirt_utility_alert_pipeline

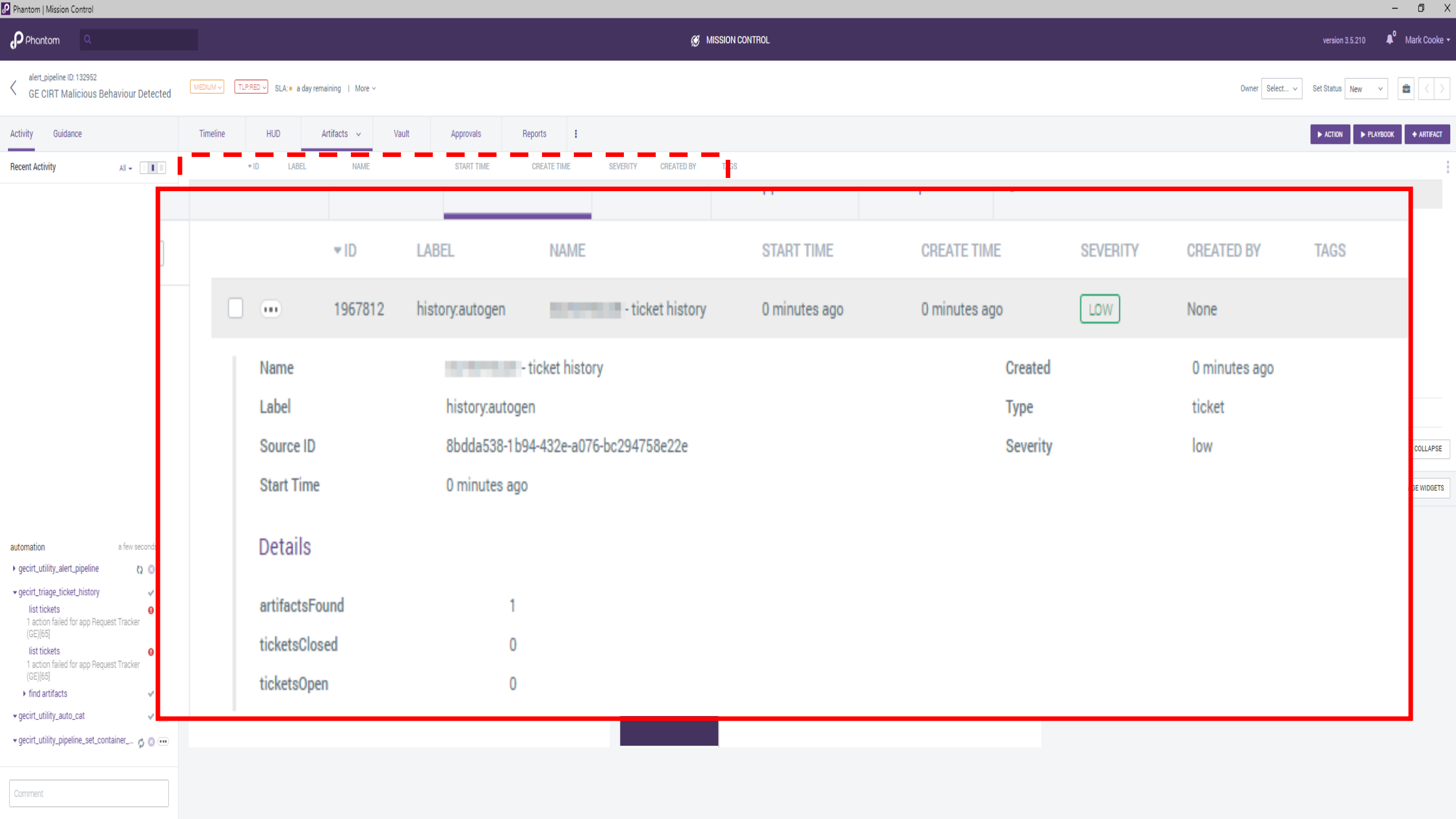
gecirt_triage_ticket_history

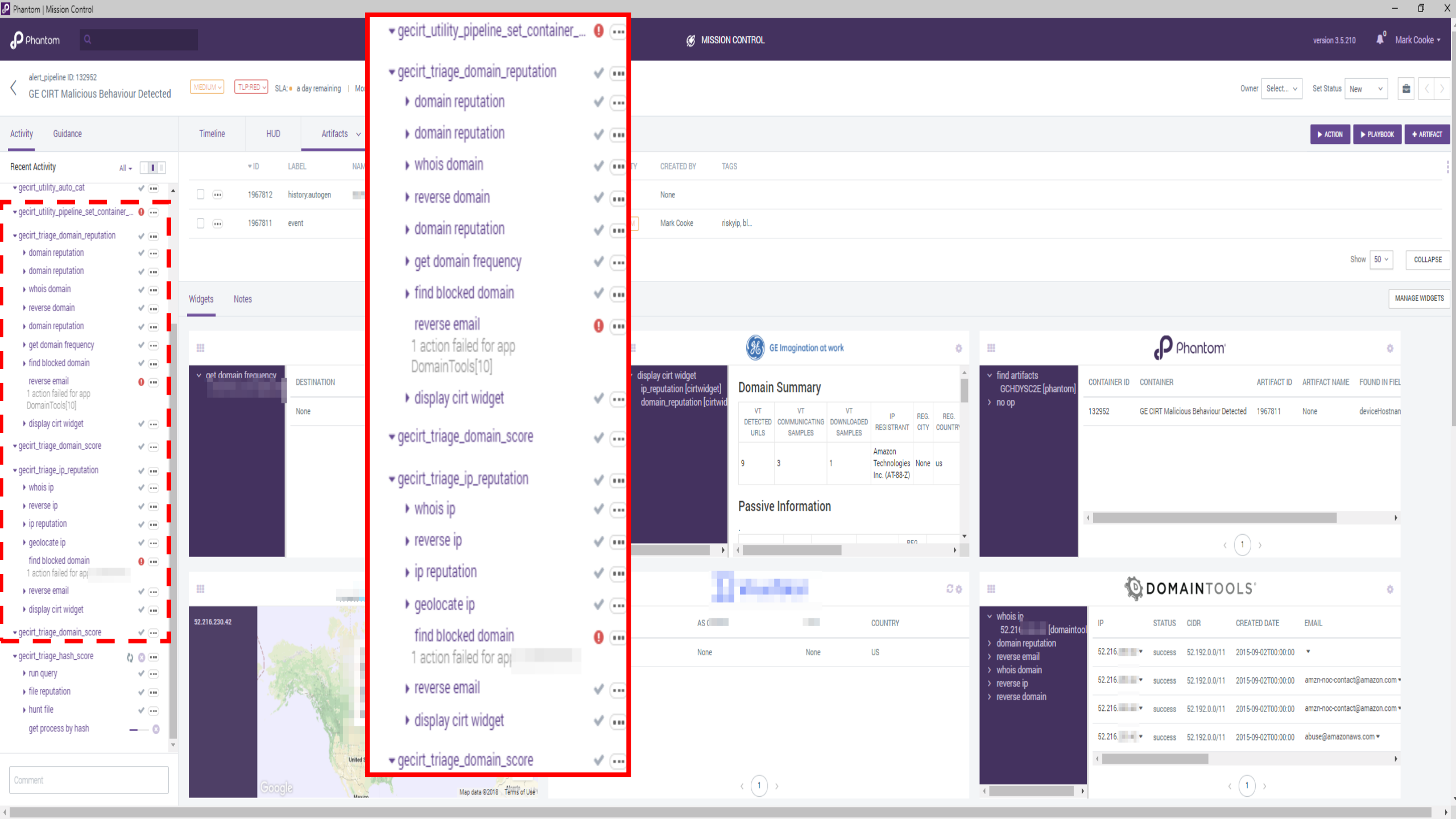
list tickets

1 action failed for app Request Tracker (GE)[65]

list tickets

Comment


Phantom | Mission Control
Phantom
MISSION CONTROL
version 3.5.210
Mark Cooke
alert_pipeline ID: 132952
GE CIRT Malicious Behaviour Detected
MEDIUM
TLP:RED
SLA: a day remaining | More
Owner Select...
Set Status New
Activity
Guidance
Timeline
HUD
Artifacts
Vault
Approvals
Reports
ACTION
PLAYBOOK
ARTIFACT
Recent Activity
All
ID
LABEL
NAME
START TIME
CREATE TIME
SEVERITY
CREATED BY
TAGS
1967812
history:autogen
- ticket history
0 minutes ago
0 minutes ago
LOW
None
Name
- ticket history
Label
history:autogen
Source ID
8bdda538-1b94-432e-a076-bc294758e22e
Start Time
0 minutes ago
Created
0 minutes ago
Type
ticket
Severity
low
Details
artifactsFound
1
ticketsClosed
0
ticketsOpen
0
COLLAPSE
automation
a few seconds
gecirt_utility_alert_pipeline
gecirt_triage_ticket_history
list tickets
1 action failed for app Request Tracker (GE)(65)
list tickets
1 action failed for app Request Tracker (GE)(65)
find artifacts
gecirt_utility_auto_cat
gecirt_utility_pipeline_set_container_...
Comment


Phantom | Mission Control
Phantom
MISSION CONTROL
version 3.5.210
Mark Cooke
alert_pipeline ID: 132952
GE CIRT Malicious Behaviour Detected
MEDIUM
TLP:RED
SLA: a day remaining
Owner
Select...
Set Status
New
Activity
Guidance
Timeline
HUD
Artifacts
ACTION
PLAYBOOK
ARTIFACT
Recent Activity
All
ID
LABEL
CREATED BY
TAGS
1967812
history:autogen
None
1967811
event
Mark Cooke
riskyip, bl...
Show
50
COLLAPSE
Widgets
Notes
MANAGE WIDGETS
gecirt_utility_auto_cat
gecirt_utility_pipeline_set_container_...
gecirt_triage_domain_reputation
domain reputation
domain reputation
whois domain
reverse domain
domain reputation
get domain frequency
find blocked domain
reverse email
1 action failed for app DomainTools[10]
display cirt widget
gecirt_triage_domain_score
gecirt_triage_ip_reputation
whois ip
reverse ip
ip reputation
geolocate ip
find blocked domain
1 action failed for app
reverse email
display cirt widget
gecirt_triage_domain_score
gecirt_triage_hash_score
run query
file reputation
hunt file
get process by hash
Comment
get domain frequency
DESTINATION
None
display cirt widget
ip_reputation [cirtwidget]
domain_reputation [cirtwid
GE Imagination at work
Domain Summary
VT DETECTED URLS
VT COMMUNICATING SAMPLES
VT DOWNLOADED SAMPLES
IP REGISTRANT
REG. CITY
REG. COUNTRY
9
3
1
Amazon Technologies Inc. (AT-88-Z)
None
us
Passive Information
find artifacts
GCHDYSC2E [phantom]
no op
CONTAINER ID
CONTAINER
ARTIFACT ID
ARTIFACT NAME
FOUND IN FIEL
132952
GE CIRT Malicious Behaviour Detected
1967811
None
deviceHostnan
52.216.230.42
Google
Map data ©2018
Terms of Use
AS
COUNTRY
None
None
US
DOMAINTOOLS
whois ip
52.21 [domaintool
domain reputation
reverse email
whois domain
reverse ip
reverse domain
IP
STATUS
CIDR
CREATED DATE
EMAIL
52.216.
success
52.192.0.0/11
2015-09-02T00:00:00
amzn-noc-contact@amazon.com
abuse@amazonaws.com

alert_pipeline ID: 132952

GE CIRT Malicious Behaviour Detected

MEDIUM TLP:RED SLA: a day remaining | More

Owner Select... Set Status New

Activity Guidance

Recent Activity All

- gecirt_utility_auto_cat
- gecirt_utility_pipeline_set_container_...
- gecirt_triage_domain_reputation
  - domain reputation
  - domain reputation
  - whois domain
  - reverse domain
  - domain reputation
  - get domain frequency
  - find blocked domain
  - reverse email
  - display cirt widget
- gecirt_triage_domain_score
- gecirt_triage_ip_reputation
  - whois ip
  - reverse ip
  - ip reputation
  - geolocate ip
  - find blocked domain
    1 action failed for app
  - reverse email
  - display cirt widget
- gecirt_triage_domain_score
- gecirt_triage_hash_score
  - run query
  - file reputation
  - hunt file
  - get process by hash

Comment

display cirt widget
ip_reputation [cirtwidget]
domain_reputation [cirtwid

GE Imagination at work

Domain Summary

VT DETECTED URLS	VT COMMUNICATING SAMPLES	VT DOWNLOADED SAMPLES	IP REGISTRANT	REG. CITY	REG. COUNTRY	PHY. CITY	PHY. COUNTRY	CRITS IDENTIFIED		# NETWORK EVENTS
9	3	1	Amazon Technologies Inc. (AT-88-Z)	None	us	Ashburn	United States	False	False	0

Passive Information

IP ADDRESS	IP TO DOMAIN COUNT	IP TO DOMAIN NAMES	REG. WHOIS RECORDS	REG. EMAIL DOMAIN COUNT	REG. EMAIL DOMAIN NAMES
52.216.	21	52.216.	Amazon Technologies Inc. (AT-88-Z)	0	memberservices@domaintools.com

Associated Files

Communicating Samples

SCAN DATE	SHA256	DETECTION RATION
2018-06-20 13:03:15	be84152f172e125e95e9c98cc7fa8a8c03234c4e85f88519	14/68
2017-12-15 23:14:13	cc8b3df59197d87c8031357adbaa9dff201059e8879c814	10/67
2017-11-19 03:02:10	96f68f54e3a0f9a42dcafff231168e3f74530d70f0686605b	8/68

Refferred Samples

SCAN DATE	SHA256	DETECTION RATION

Downloaded Samples

SCAN DATE	SHA256	DETECTION RATION
2018-02-12 04:02:21	b71f469f83e172131270c181b243afe753c9b4e98f0efa8d	11/56

URLs & Network Traffic

Detected URLs

SCAN DATE	URL	DETECTION RATION
2018-07-14 15:30:24		1/67
2018-07-08 11:05:37		2/67
2018-06-10 07:50:07		1/67
2018-05-21 21:30:12		5/67
2018-04-22 19:46:44		8/67
2018-02-12 04:02:17		6/67
2018-01-17 12:08:54		1/66
2017-12-04 21:35:39		3/66

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

alert_pipeline ID: 132952

GE CIRT Malicious Behaviour Detected

MEDIUM | TLP:RED | SLA: a day remaining | More

Owner: Select... | Set Status: New

Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK | ARTIFACT

Recent Activity: All

- gecirt_triage_domain_reputation
  - domain reputation
  - domain reputation
  - whois domain
  - reverse domain
  - domain reputation
  - get domain frequency
  - find blocked domain
  - reverse email
  - display cirt widget
- gecirt_triage_domain_score
- gecirt_triage_ip_reputation
  - whois ip
  - reverse ip
  - ip reputation
  - geolocate ip
  - find blocked domain (1 action failed for app 2)
  - reverse email
  - display cirt widget
- gecirt_triage_domain_score
- gecirt_triage_hash_score
  - run query
  - file reputation
  - hunt file
  - get process by hash
- gecirt_utility_merge_related_alerts
- gecirt_utility_extract_artifact_iocs

Comment

ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY	TAGS
1967812	history:autogen	- ticket history	1 minutes ago	1 minutes ago	LOW	None	
1967811	event		1 minutes ago	1 minutes ago	MEDIUM	Mark Cooke	riskyip, ha...

Label	event	Created	1 minutes ago
Created by	Mark Cooke	Type	
Source ID	555d76e9-d8c7-4fd8-94e8-ed0ce055d4a4	Severity	medium
Start Time	1 minutes ago	Tags	riskyip, hash-malicious, blocked domain, _protection-true, riskydomain

Details

command
destinationAddress
destinationDnsDomain
detectionIndicator
deviceHostname
fileHash
fileHashMd5
fileHashSha256
fileName
filePath
sourceAddress

1 minutes ago

medium

riskyip, hash-malicious, blocked domain, _protection-true, riskydomain

Show 50 | COLLAPSE

Widgets | Notes | MANAGE WIDGETS

GE Imagination at work

display cirt widget
ip_reputation [cirtwidget]
domain_reputation [cirtwid

Domain Summary

VT DETECTED URLS	VT COMMUNICATING SAMPLES	VT DOWNLOADED SAMPLES	IP REGISTRANT	REG. CITY	REG. COUNTRY	PHY. CITY	PHY. COUNTRY	CRITS IDENTIFIED	LOCKED	# NETWORK EVENTS
9	3	1	Amazon Technologies Inc. (AT-88-Z)	None	us	Ashburn	United States	False	False	0

Passive Information

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

alert_pipeline ID: 132952

GE CIRT Malicious Behaviour Detected

MEDIUM | TLP:RED | SLA: a day remaining | More

Owner: Select... | Set Status: New

Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK | ARTIFACT

Recent Activity: All

- find blocked domain
- reverse email
- display cirt widget
- gecirt_triage_domain_score
- gecirt_triage_ip_reputation
  - whois ip
  - reverse ip
  - ip reputation
  - geolocate ip
  - find blocked domain
    1 action failed for
  - reverse email
  - display cirt widget
- gecirt_triage_domain_score
- gecirt_triage_hash_score
  - run query
  - file reputation
  - hunt file
  - get process by hash
- gecirt_utility_merge_related_alerts
- gecirt_utility_extract_artifact_iocs
- gecirt_triage_asset_info
  - get lake client info
  - lookup employee by sso
  - check vip by sso
- gecirt_utility_template_picker

promoted to case "GE CIRT Malicious Behaviour Detected" (id: 132952)

Comment

	ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY
	1967814	user:autogen	[redacted] - User Info	0 minutes ago	0 minutes ago	LOW	None
	1967813	device:autogen	[redacted] - ...	0 minutes ago	0 minutes ago	LOW	None

Show 50 | COLLAPSE

Widgets | Notes | MANAGE WIDGETS

GE Imagination at work

NT	REG. CITY	REG. COUNTRY	PHY. CITY	PHY. COUNTRY	CRITS IDENTIFIED	[redacted]	# NETWORK EVENTS
nc. (AT-88-Z)	None	us	Ashburn	United States	False	False	0

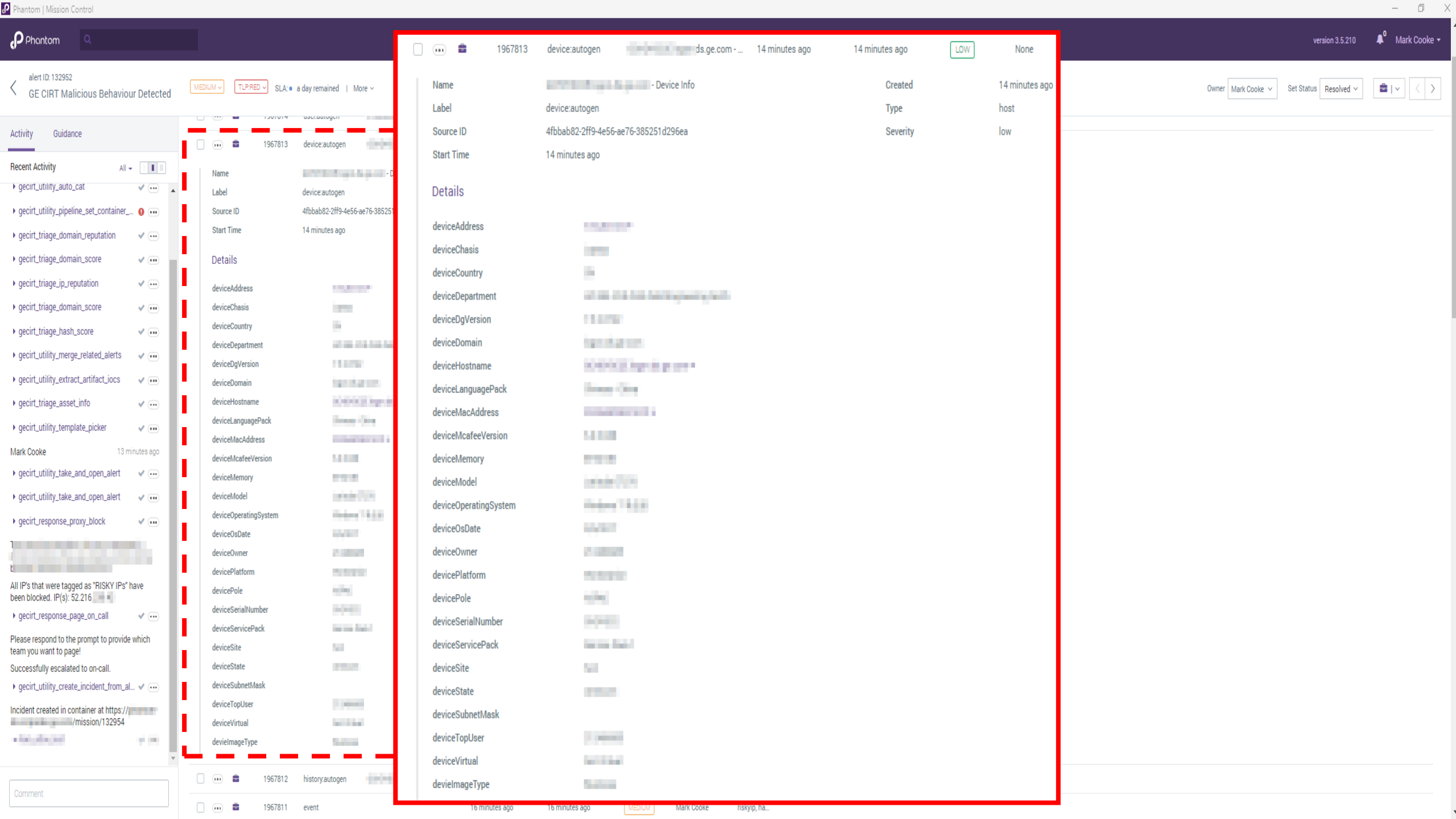
EMAIL DOMAIN COUNT	REG. EMAIL DOMAIN NAMES
	memberservices@domaintools.com

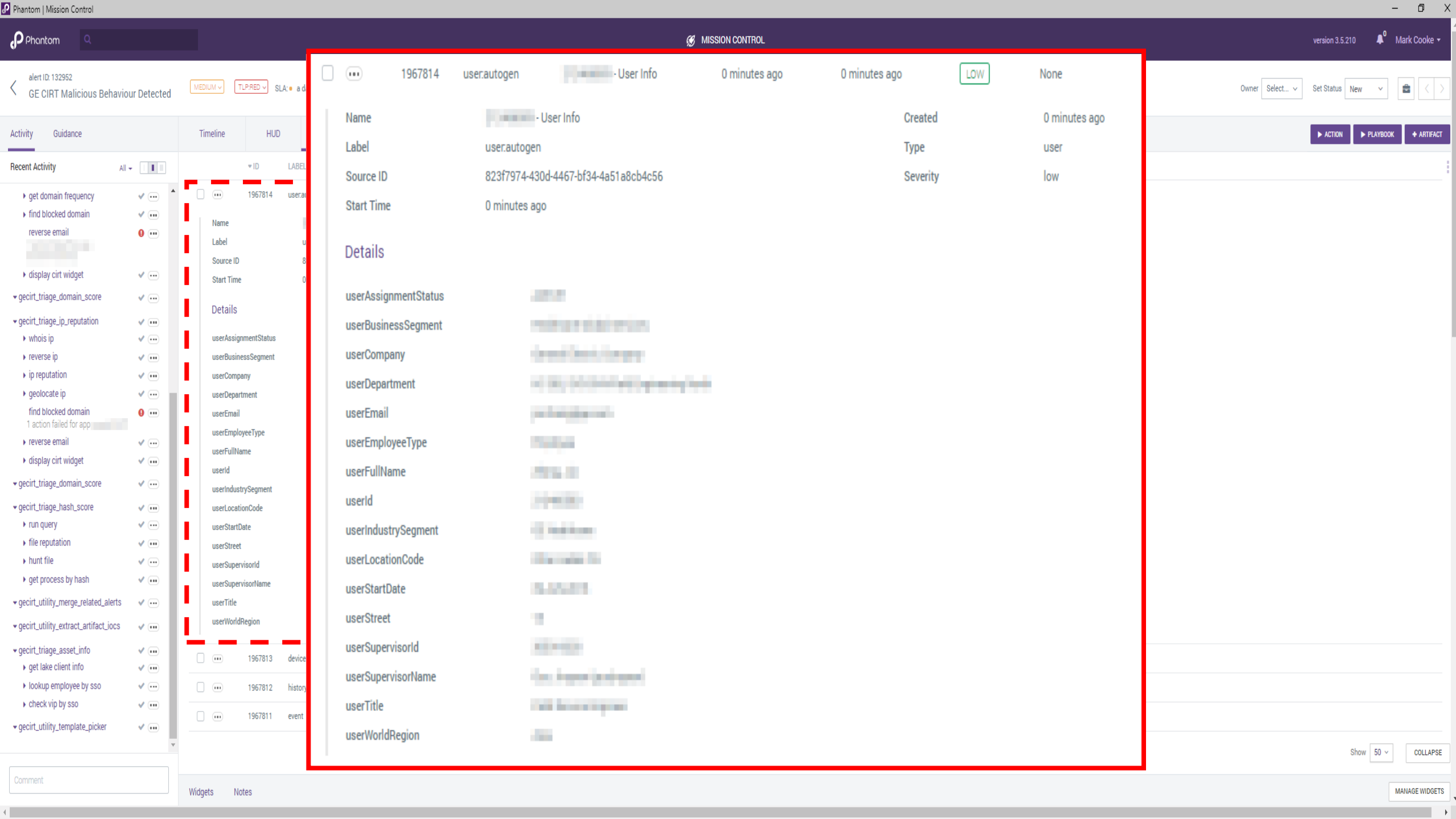
ECTION RATION
68
67
8

ECTION RATION

- gecirt_utility_merge_related_alerts
- gecirt_utility_extract_artifact_iocs
- gecirt_triage_asset_info
  - get lake client info
  - lookup employee by sso
  - check vip by sso
- gecirt_utility_template_picker

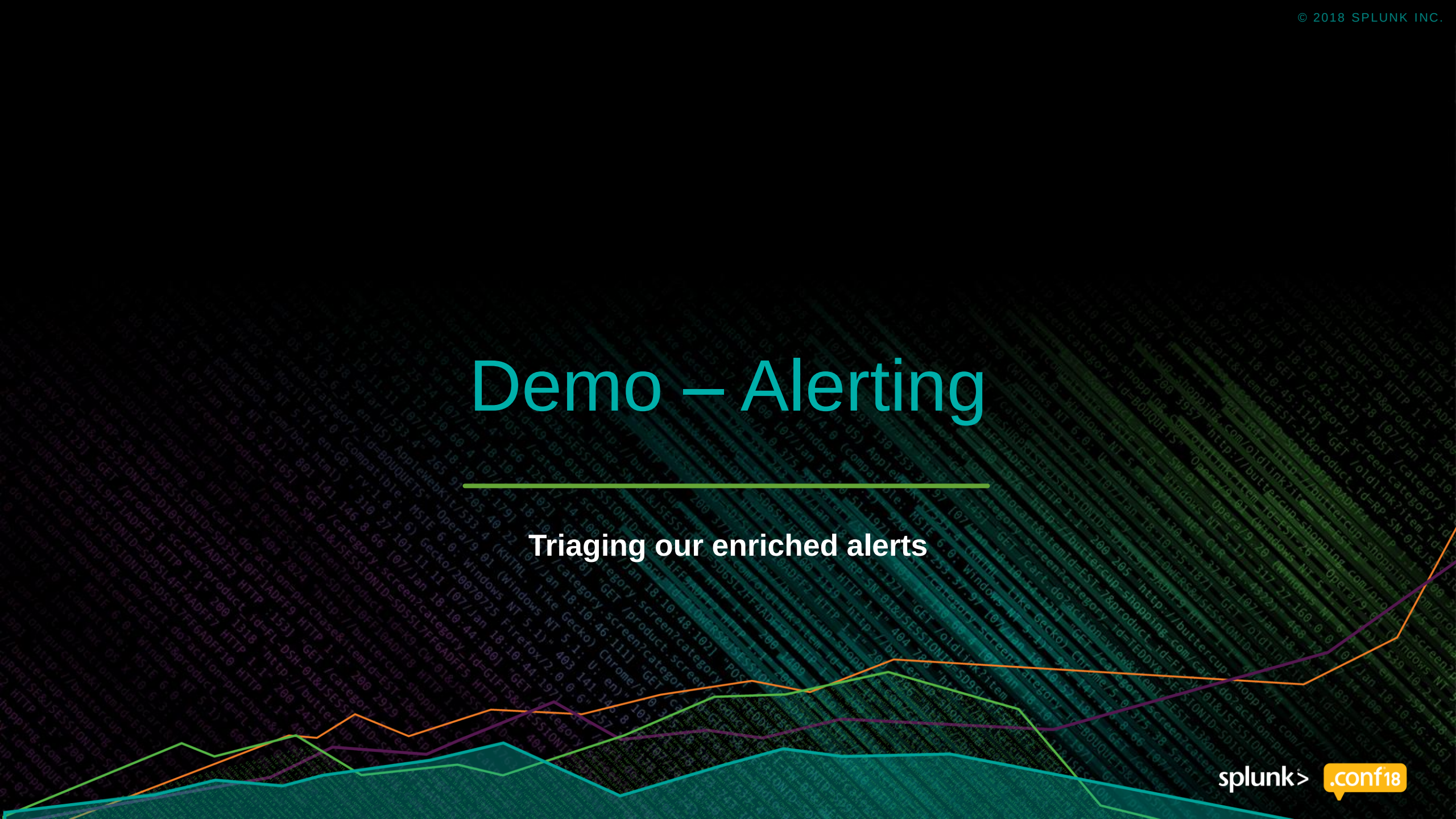
promoted to case "GE CIRT Malicious Behaviour


Phantom | Mission Control
Phantom
version 3.5.210
Mark Cooke
alert ID: 132952
GE CIRT Malicious Behaviour Detected
MEDIUM
TLP:RED
SLA: a day remained
More
Owner
Mark Cooke
Set Status
Resolved
Activity
Guidance
Recent Activity
All
gecirt_utility_auto_cat
gecirt_utility_pipeline_set_container_...
gecirt_triage_domain_reputation
gecirt_triage_domain_score
gecirt_triage_ip_reputation
gecirt_triage_domain_score
gecirt_triage_hash_score
gecirt_utility_merge_related_alerts
gecirt_utility_extract_artifact_iocs
gecirt_triage_asset_info
gecirt_utility_template_picker
Mark Cooke
13 minutes ago
gecirt_utility_take_and_open_alert
gecirt_utility_take_and_open_alert
gecirt_response_proxy_block
All IP's that were tagged as "RISKY IPs" have been blocked. IP(s): 52.216
gecirt_response_page_on_call
Please respond to the prompt to provide which team you want to page!
Successfully escalated to on-call.
gecirt_utility_create_incident_from_al...
Incident created in container at https://
/mission/132954
Comment
1967813
device:autogen
14 minutes ago
14 minutes ago
LOW
None
Name
- Device Info
Label
device:autogen
Source ID
4fbbab82-2ff9-4e56-ae76-385251d296ea
Start Time
14 minutes ago
Created
14 minutes ago
Type
host
Severity
low
Details
deviceAddress
deviceChasis
deviceCountry
deviceDepartment
deviceDgVersion
deviceDomain
deviceHostname
deviceLanguagePack
deviceMacAddress
deviceMcafeeVersion
deviceMemory
deviceModel
deviceOperatingSystem
deviceOsDate
deviceOwner
devicePlatform
devicePole
deviceSerialNumber
deviceServicePack
deviceSite
deviceState
deviceSubnetMask
deviceTopUser
deviceVirtual
devieImageType
1967812
history:autogen
1967811
event
16 minutes ago
16 minutes ago
MEDIUM
Mark Cooke


Phantom | Mission Control
Phantom
MISSION CONTROL
version 3.5.210
Mark Cooke
alert ID: 132952
GE CIRT Malicious Behaviour Detected
MEDIUM
TLP:RED
SLA:
Owner
Select...
Set Status
New
Activity
Guidance
Timeline
HUD
ACTION
PLAYBOOK
ARTIFACT
Recent Activity
All
get domain frequency
find blocked domain
reverse email
display cirt widget
gecirt_triage_domain_score
gecirt_triage_ip_reputation
whois ip
reverse ip
ip reputation
geolocate ip
find blocked domain
1 action failed for app
reverse email
display cirt widget
gecirt_triage_domain_score
gecirt_triage_hash_score
run query
file reputation
hunt file
get process by hash
gecirt_utility_merge_related_alerts
gecirt_utility_extract_artifact_iocs
gecirt_triage_asset_info
get lake client info
lookup employee by sso
check vip by sso
gecirt_utility_template_picker
Comment
ID
LABEL
1967814
user:autogen
- User Info
0 minutes ago
0 minutes ago
LOW
None
Name
Label
Source ID
Start Time
Details
userAssignmentStatus
userBusinessSegment
userCompany
userDepartment
userEmail
userEmployeeType
userFullName
userId
userIndustrySegment
userLocationCode
userStartDate
userStreet
userSupervisorId
userSupervisorName
userTitle
userWorldRegion
1967813
1967812
1967811
Name
- User Info
Created
0 minutes ago
Label
user:autogen
Type
user
Source ID
823f7974-430d-4467-bf34-4a51a8cb4c56
Severity
low
Start Time
0 minutes ago
Details
userAssignmentStatus
userBusinessSegment
userCompany
userDepartment
userEmail
userEmployeeType
userFullName
userId
userIndustrySegment
userLocationCode
userStartDate
userStreet
userSupervisorId
userSupervisorName
userTitle
userWorldRegion
Show
50
COLLAPSE
Widgets
Notes
MANAGE WIDGETS

Demo – Alerting

Triaging our enriched alerts



Phantom | Analyst Queue

Phantom

version 3.5.210

Mark Cooke

Sources

Show alert_view

+ EVENT

IMPORT

Top Events	Severity			Status			Top Owners
1 alert	0 Low	1 Medium	0 High	1 New	0 Open	0 Resolved	

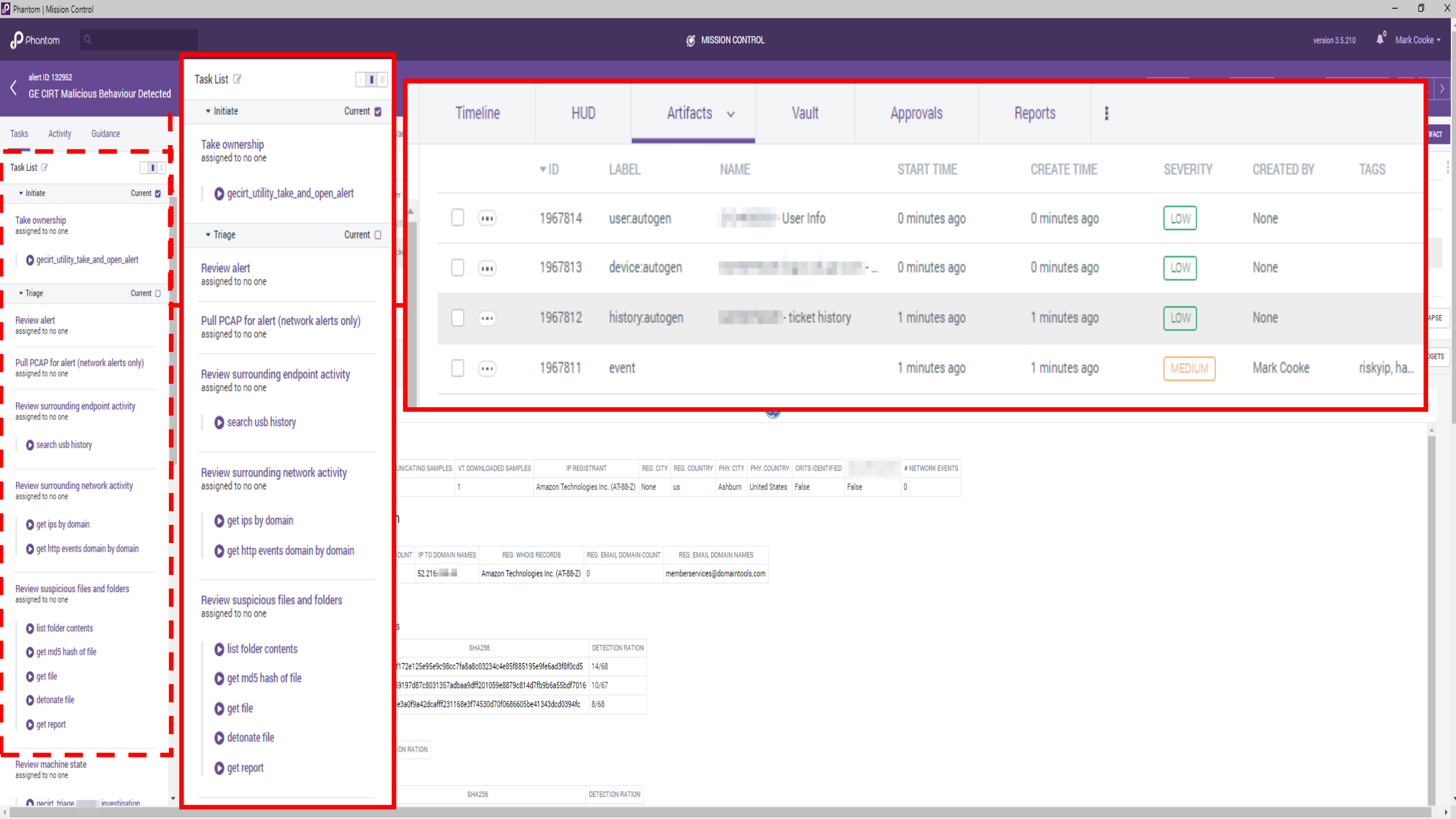
Label: alert Status: New CLEAR EDIT

Dynamic Updates Show Stats

ID	STATUS	NAME	ARTIFACTS	CREATED	TAGS	DESTINATIONADDRESS	DEVICEHOSTNAME	DISPOSITION	DESTINATIONUSER	FILEHASH	DESTINATIONDNSDOMAIN	SOURCEADDRESS
132952	New	GE CIRT Malicious Behaviour Detected	4	2 minutes ago		52.216				542a98fba74f08d3c71bff11b7d71475	artist com	41.190.

1

Show 50


Phantom | Mission Control
Phantom
MISSION CONTROL
version 3.5.210
Mark Cooke
alert ID: 132952
GE CIRT Malicious Behaviour Detected
Tasks
Activity
Guidance
Task List
Initiate
Current
Take ownership
assigned to no one
gecirt_utility_take_and_open_alert
Triage
Current
Review alert
assigned to no one
Pull PCAP for alert (network alerts only)
assigned to no one
Review surrounding endpoint activity
assigned to no one
search usb history
Review surrounding network activity
assigned to no one
get ips by domain
get http events domain by domain
Review suspicious files and folders
assigned to no one
list folder contents
get md5 hash of file
get file
detonate file
get report
Review machine state
assigned to no one
Timeline
HUD
Artifacts
Vault
Approvals
Reports
ID
LABEL
NAME
START TIME
CREATE TIME
SEVERITY
CREATED BY
TAGS
1967814
user:autogen
User Info
0 minutes ago
0 minutes ago
LOW
None
1967813
device:autogen
0 minutes ago
0 minutes ago
LOW
None
1967812
history:autogen
ticket history
1 minutes ago
1 minutes ago
LOW
None
1967811
event
1 minutes ago
1 minutes ago
MEDIUM
Mark Cooke
riskyip, ha...
VT DOWNLOADED SAMPLES
IP REGISTRANT
REG. CITY
REG. COUNTRY
PHY. CITY
PHY. COUNTRY
CRITS IDENTIFIED
NETWORK EVENTS
1
Amazon Technologies Inc. (AT-88-Z)
None
us
Ashburn
United States
False
False
0
IP TO DOMAIN NAMES
REG. WHOIS RECORDS
REG. EMAIL DOMAIN COUNT
REG. EMAIL DOMAIN NAMES
Amazon Technologies Inc. (AT-88-Z)
0
memberservices@domaintools.com
SHA256
DETECTION RATION
14/68
10/67
8/68

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

alert ID: 132952
GE CIRT Malicious Behaviour Detected
MEDIUM | TLP:RED | More

Owner: Mark Cooke | Set Status: Resolved | Current Phase: Initiate

Tasks | Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports | ACTION | PLAYBOOK

Task List

assigned to no one

terminate process

Escalate — Current

Page the On-call
assigned to no one

gecirt_response_page_on_call

1
Escalation(s) - Success

PINNED ITEMS (4)

DATE	MESSAGE	DATA	BY

PINNED ITEMS (4)

DATE	MESSAGE	DATA	BY
5 minutes ago	vt score: 55/67, [redacted]confidence: no results, [redacted]impact: no results, [redacted] system count: 0, [redacted]system count: 0, risk score: 10, risk_tag:hash-ma...	542a98fba74f08d3c71bff11b7[redacted]	automation
5 minutes ago	52.216.230.42	RISK: Low User Count,RISK: Low Event Count,Threat Score: 0	automation
6 minutes ago	artist[redacted].com	RISK: Moderate Domaintools Score,RISK: URLVoid Detections,RISK: Low Alexa Ranking,RISK: Blocked Domain,RISK: VT Samples,RIS...	automation

gecirt_utility_resolve_alert_tp_trivial

gecirt_utility_resolve_alert_fp

gecirt_utility_resolve_alert_tp_unable_to_track

gecirt_utility_resolve_alert_tp_already_ticketed

Report — Current

Detection tuning
assigned to no one

Identify Indicators for Intel
assigned to no one

intel_ews_send_to_intel

domain_reputation [cirtwi

VT DETECTED URLS	VT COMMUNICATING SAMPLES	VT DOWNLOADED SAMPLES	IP REGISTRANT	REG. CITY	REG. COUNTRY	PHY. CITY	PHY. COUNTRY	CRITS IDENTIFIED	[redacted]	# NETWORK EVENTS
9	3	1	Amazon Technologies Inc. (AT-88-Z)	None	us	Ashburn	United States	False	False	0

Passive Information

IP ADDRESS	IP TO DOMAIN COUNT	IP TO DOMAIN NAMES	REG. WHOIS RECORDS	REG. EMAIL DOMAIN COUNT	REG. EMAIL DOMAIN NAMES
52.216[redacted]	21	52.216.[redacted]	Amazon Technologies Inc. (AT-88-Z)	0	memberservices@domaintools.com

Associated Files

Communicating Samples

SCAN DATE	SHA256	DETECTION RATION
2018-06-20 13:03:15	be84152f172e125e95e9c98cc7fa8a8c03234c4e85f885195e9fe6ad3f8f0cd5	14/68
2017-12-15 23:14:13	cc8b3df59197d87c8031357adbaa9dff201059e8879c814d7fb9b6a55bdf7016	10/67
2017-11-19 03:02:10	96f68f54e3a0f9a42dcafff231168e3f74530d70f0686605be41343dcd0394fc	8/68

Phantom | Mission Control

Phantom

MISSION CONTROL

version 3.5.210

Mark Cooke

alert ID: 132952

GE CIRT Malicious Behaviour Detected

MEDIUM

TLP:RED

More

Owner Select...

Set Status New

Current Phase Initiate

Tasks Activity Guidance

Task List

Initiate Current

Take ownership
assigned to no one

gecirt_utility_take_and_open_alert

Confirm Run Playbook

Cancel RUN PLAYBOOK

Review

Pull PCAP for alert (network alerts only)
assigned to no one

Review surrounding endpoint activity
assigned to no one

search usb history

Review surrounding network activity
assigned to no one

get ips by domain

get http events domain by domain

Review suspicious files and folders
assigned to no one

list folder contents

get md5 hash of file

get file

detonate file

get report

Review machine state
assigned to no one

Back to case

Take ownership

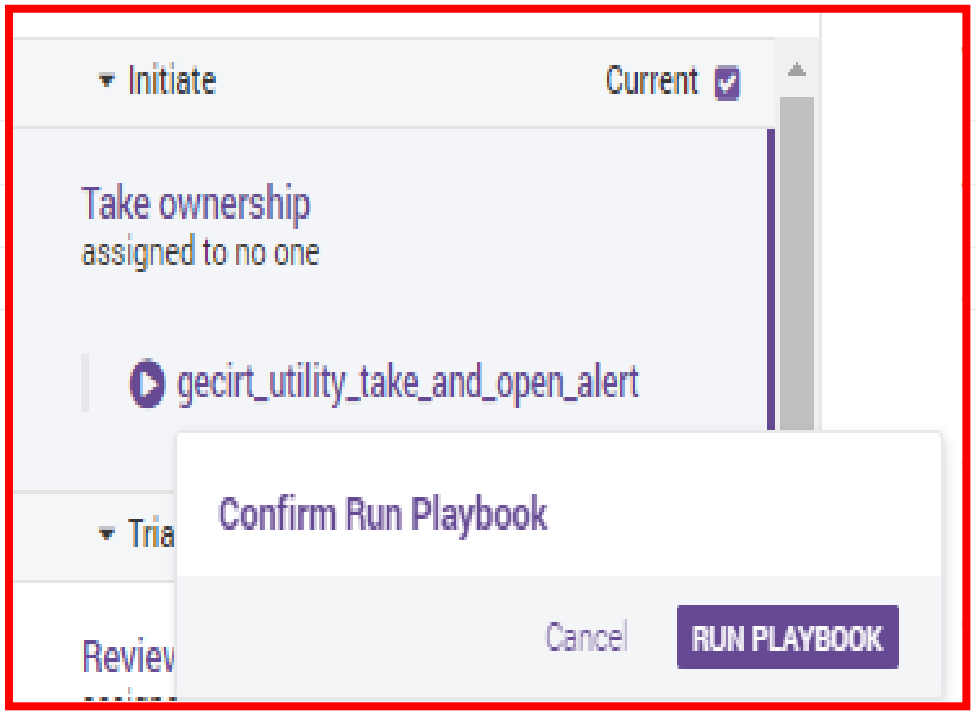
assigned to no one

DESCRIPTION

NOTES (0)

FILES (0)

MARK COMPLETE



Phantom | Mission Control

Phantom

MISSION CONTROL

Playbook gecirt_utility_take_and_open_alert started successfully.

alert ID: 132952

GE CIRT Malicious Behaviour Detected

MEDIUM | TLP:RED | More

Owner Mark Cooke | Set Status Open | Current Phase Initiate

Tasks | Activity | Guidance

Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK | ARTIFACT

Task List

Initiate — Current

Take ownership
assigned to no one

gecirt_utility_take_and_open_alert

Triage — Current

Review alert
assigned to no one

Pull PCAP for alert (network alerts only)
assigned to no one

Review surrounding endpoint activity
assigned to no one

search usb history

Review surrounding network activity
assigned to no one

get ips by domain

get http events domain by domain

Review suspicious files and folders
assigned to no one

list folder contents

get md5 hash of file

get file

detonate file

get report

Review machine state
assigned to no one

gecirt_triag[redacted]tigation

ID	LABEL	NAME	START TIME	CREATE TIME	SEVER
1967814	user:autogen	[redacted] - User Info	1 minutes ago	1 minutes ago	LOW
1967813	device:autogen	[redacted]	1 minutes ago	1 minutes ago	LOW
1967812	history:autogen	[redacted] - ticket history	2 minutes ago	2 minutes ago	LOW
1967811	event		3 minutes ago	3 minutes ago	MED

Show 50 | COLLAPSE

Owner Mark Cooke | Set Status Open | Cu

Widgets | Notes

MANAGE WIDGETS

GE Imagination at work

display cirt widget
ip_reputation [cirtwidget]
domain_reputation [cirtwid

Domain Summary

VT DETECTED URLS	VT COMMUNICATING SAMPLES	VT DOWNLOADED SAMPLES	IP REGISTRANT	REG. CITY	REG. COUNTRY	PHY. CITY	PHY. COUNTRY	CRITS IDENTIFIED	[redacted]	# NETWORK EVENTS
9	3	1	Amazon Technologies Inc. (AT-88-Z)	None	us	Ashburn	United States	False	False	0

Passive Information

IP ADDRESS	IP TO DOMAIN COUNT	IP TO DOMAIN NAMES	REG. WHOIS RECORDS	REG. EMAIL DOMAIN COUNT	REG. EMAIL DOMAIN NAMES
52.216.[redacted]	21	52.216.[redacted]	Amazon Technologies Inc. (AT-88-Z)	0	memberservices@domaintools.com

Associated Files

Communicating Samples

SCAN DATE	SHA256	DETECTION RATION
2018-06-20 13:03:15	be84152f172e125e95e9c98cc7fa8a8c03234c4e85f8851[redacted]	14/68
2017-12-15 23:14:13	cc8b3df59197d87c8031357adbaa9dff201059e8879c814[redacted]	10/67
2017-11-19 03:02:10	96f68f54e3a0f9a42dcafff231168e3f74530d70f0686605[redacted]	8/68

Refferred Samples

SCAN DATE	SHA256	DETECTION RATION

Downloaded Samples

SCAN DATE	SHA256	DETECTION RATION
2018-02-12 04:02:21	b71f469f83e172131270c181b243afe753c9b4e98f0efa8db69[redacted]	11/56

Phantom | Mission Control

Phantom

MISSION CONTROL

Playbook gecirt_utility_take_and_open_alert started successfully.

alert ID: 132952

GE CIRT Malicious Behaviour Detected

MEDIUM | TLP:RED | More

Owner Mark Cooke | Set Status Open | Current Phase Initiate

Tasks | Activity | Guidance

Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK | ARTIFACT

Task List

Initiate — Current

Take ownership
assigned to no one

gecirt_utility_take_and_open_alert

Triage — Current

Review alert
assigned to no one

Pull PCAP for alert (network alerts only)
assigned to no one

Review surrounding endpoint activity
assigned to no one

search usb history

Review surrounding network activity
assigned to no one

get ips by domain

get http events domain by domain

Review suspicious files and folders
assigned to no one

list folder contents

get md5 hash of file

get file

detonate file

get report

Review machine state
assigned to no one

gecirt_triag[redacted]tigation

ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY	TAGS
1967814	user:autogen	[redacted] - User Info	1 minutes ago	1 minutes ago	LOW	None	
1967813	device:autogen	[redacted]	1 minutes ago	1 minutes ago	LOW	None	
1967812	history:autogen	[redacted] - ticket history	2 minutes ago	2 minutes ago	LOW	None	
1967811	event		3 minutes ago	3 minutes ago	MEDIUM	Mark Cooke	riskyip, ha...

Show 50 | COLLAPSE

Widgets | Notes

MANAGE WIDGETS

GE Imagination at work

display cirt widget
ip_reputation [cirtwidget]
domain_reputation [cirtwid

Domain Summary

VT DETECTED URLS	VT COMMUNICATING SAMPLES	VT DOWNLOADED SAMPLES	IP REGISTRANT	REG. CITY	REG. COUNTRY	PHY. CITY	PHY. COUNTRY	CRITS IDENTIFIED	[redacted]	# NETWORK EVENTS
9	3	1	Amazon Technologies Inc. (AT-88-Z)	None	us	Ashburn	United States	False	False	0

Passive Information

IP ADDRESS	IP TO DOMAIN COUNT	IP TO DOMAIN NAMES	REG. WHOIS RECORDS	REG. EMAIL DOMAIN COUNT	REG. EMAIL DOMAIN NAMES
52.216.[redacted]	21	52.216.[redacted]	Amazon Technologies Inc. (AT-88-Z)	0	memberservices@domaintools.com

Associated Files

Communicating Samples

SCAN DATE	SHA256	DETECTION RATION
2018-06-20 13:03:15	be84152f172e125e95e9c98cc7fa8a8c03234c4e85f8851[redacted]	14/68
2017-12-15 23:14:13	cc8b3df59197d87c8031357adbaa9dff201059e8879c814[redacted]	10/67
2017-11-19 03:02:10	96f68f54e3a0f9a42dcafff231168e3f74530d70f0686605[redacted]	8/68

Refferred Samples

SCAN DATE	SHA256	DETECTION RATION

Downloaded Samples

SCAN DATE	SHA256	DETECTION RATION
2018-02-12 04:02:21	b71f469f83e172131270c181b243afe753c9b4e98f0efa8db69[redacted]	11/56

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

alert ID: 132952
GE CIRT Malicious Behaviour Detected
MEDIUM | TLP:RED | More

Owner: Mark Cooke | Set Status: Open | Current Phase: Initiate

Tasks | Activity | Guidance

Task List

Review suspicious files and folders
assigned to no one

- list folder contents
- get md5 hash of file
- get file
- detonate file
- get report

Review machine state
assigned to no one

- gecirt_triage_investigation

Mitigate — Current

Block domains and IPs
assigned to no one

- gecirt_response_proxy_block

Confirm Run Playbook
Cancel | RUN PLAYBOOK

Stop n
assigne

- terminate process

Escalate — Current

Page the On-call
assigned to no one

- gecirt_response_page_on_call

Disposition — Current

Create incident and resolve as TP
assigned to no one

- gecirt_utility_create_incident_from_alert

Back to case

Block domains and IPs
Assigned to: no one

MARK COMPLETE

DESCRIPTION

NOTES (0)

FILES (0)

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

alert ID: 132952
GE CIRT Malicious Behaviour Detected
MEDIUM | TLP:RED | More

Owner: Mark Cooke | Set Status: Open | Current Phase: Initiate

Tasks | Activity | Guidance

Task List

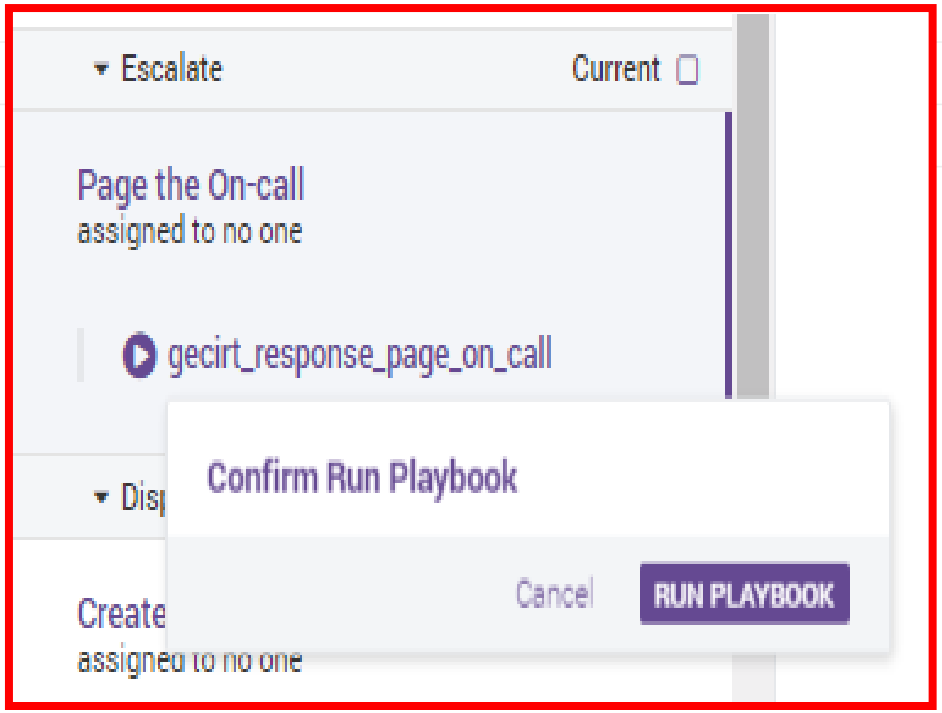
- Initiate — Current
  - Take ownership
    assigned to no one
    - gecirt_utility_take_and_open_alert
- Triage — Current
- Mitigate — Current
  - Block domains and IPs
    assigned to no one
    - gecirt_response_proxy_block
  - Stop malicious processes
    assigned to no one
    - terminate process
- Escalate — Current
  - Page the On-call
    assigned to no one
    - gecirt_response_page_on_call
  - Confirm Run Playbook
    Cancel | RUN PLAYBOOK
  - Create
    assigned to no one
    - gecirt_utility_create_incident_from_alert
  - Add disposition notes
    assigned to no one
  - Resolve alert
    assigned to no one
    - gecirt_utility_resolve_alert_tp_trivial

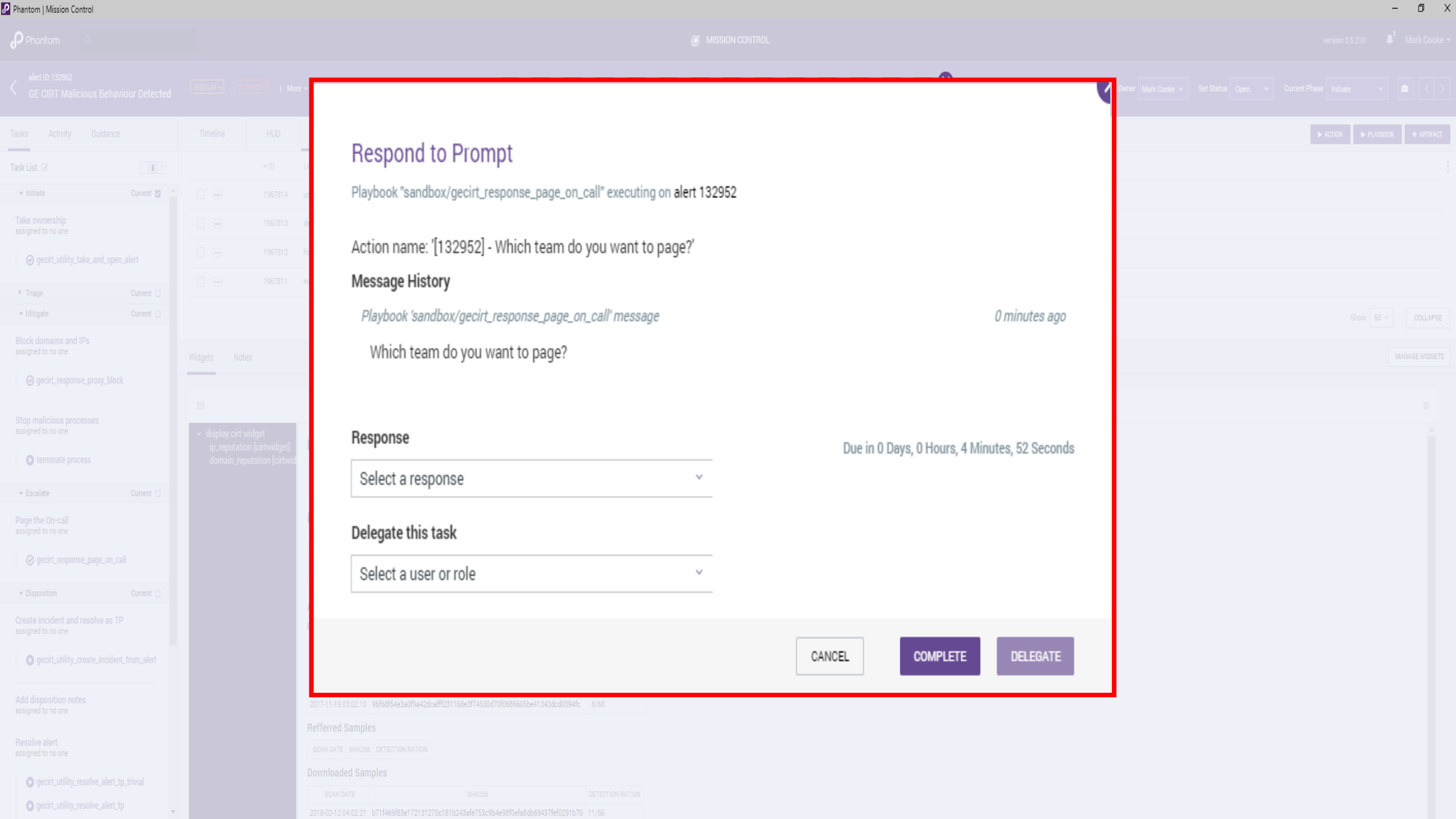
Back to case

Page the On-call
Assigned to: no one

MARK COMPLETE

DESCRIPTION
NOTES (0)
FILES (0)




Phantom | Mission Control
Phantom
MISSION CONTROL
version 3.5.210
Mark Cooke
alert ID: 132952
GE CIRT Malicious Behaviour Detected
MEDIUM
TLP:RED
More
Owner
Mark Cooke
Set Status
Open
Current Phase
Initiate
Tasks
Activity
Guidance
Timeline
HUD
ACTION
PLAYBOOK
ARTIFACT
Task List
Initiate
Current
Take ownership
assigned to no one
gecirt_utility_take_and_open_alert
Triage
Current
Mitigate
Current
Block domains and IPs
assigned to no one
gecirt_response_proxy_block
Stop malicious processes
assigned to no one
terminate process
Escalate
Current
Page the On-call
assigned to no one
gecirt_response_page_on_call
Disposition
Current
Create incident and resolve as TP
assigned to no one
gecirt_utility_create_incident_from_alert
Add disposition notes
assigned to no one
Resolve alert
assigned to no one
gecirt_utility_resolve_alert_tp_trivial
gecirt_utility_resolve_alert_fp
Widgets
Notes
display cirt widget
ip_reputation [cirtwidget]
domain_reputation [cirtwid
Show
50
COLLAPSE
MANAGE WIDGETS
Respond to Prompt
Playbook "sandbox/gecirt_response_page_on_call" executing on alert 132952
Action name: '[132952] - Which team do you want to page?'
Message History
Playbook 'sandbox/gecirt_response_page_on_call' message
0 minutes ago
Which team do you want to page?
Response
Select a response
Due in 0 Days, 0 Hours, 4 Minutes, 52 Seconds
Delegate this task
Select a user or role
CANCEL
COMPLETE
DELEGATE
2017-11-19 03:02:10
96f68f54e3a0f9a42dcafff231168e3f74530d70f0686605be41343dcd0394fc
8/68
Refferred Samples
SCAN DATE
SHA256
DETECTION RATION
Downloaded Samples
SCAN DATE
SHA256
DETECTION RATION
2018-02-12 04:02:21
b71f469f83e172131270c181b243afe753c9b4e98f0efa8db69437fef0291b70
11/56

Phantom | Mission Control

Phantom

MISSION CONTROL

version 3.5.210

Mark Cooke

alert ID: 132952

GE CIRT Malicious Behaviour Detected

MEDIUM | TLP:RED | More

Owner Mark Cooke | Set Status Open | Current Phase Initiate

Tasks | Activity | Guidance

Timeline | HUD | Ar

▶ ACTION | ▶ PLAYBOOK | ✚ ARTIFACT

Task List

- Initiate — Current
  - Take ownership
    assigned to no one
    - gecirt_utility_take_and_open_alert
- Triage — Current
- Mitigate — Current
- Escalate — Current
- Disposition — Current
  - Create incident and resolve as TP
    assigned to no one
    - gecirt_utility_create_incident_from_alert
  - Add disposition notes
    assigned to no one
  - Resolve alert
    assigned to no one
    - gecirt_utility_resolve_alert_tp_trivial
    - gecirt_utility_resolve_alert_fp
    - gecirt_utility_resolve_alert_tp_unable_to_track
    - gecirt_utility_resolve_alert_tp_already_ticketed
- Report — Current
  - Detection tuning
    assigned to no one
  - Identify Indicators for Intel
    assigned to no one
    - intel_ews_send_to_intel

ID	LABEL	CREATED BY	TAGS
1967814	user:autc	one	
1967813	device:au	one	
1967812	history:a	one	
1967811	event	ark Cooke	riskyip, ha...

Show 50 | COLLAPSE

Widgets | Notes

MANAGE WIDGETS

GE Imagination at work

display cirt widget
ip_reputation [cirtwidget]
domain_reputation [cirtwid

Dom

VT DE	G. COUNTRY	PHY. CITY	PHY. COUNTRY	CRITS IDENTIFIED	# NETWORK EVENTS
9		Ashburn	United States	False	False	0

Pass

IP AD	REG. EMAIL DOMAIN NAMES
52.216	berservices@domaintools.com

Assc

Comn

S	
2018-0	
2017-1	
2017-1	

Reffe

SCAN

Downloaded Samples

SCAN DATE	SHA256	DETECTION RATION

Disposition Current

Create incident and resolve as TP
assigned to no one
- gecirt_utility_create_incident_from_alert

Add disposition notes
assigned to no one

Resolve alert
assigned to no one
- gecirt_utility_resolve_alert_tp_trivial
- gecirt_utility_resolve_alert_fp
- gecirt_utility_resolve_alert_tp_unable_to_track
- gecirt_utility_resolve_alert_tp_already_ticketed

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

alert ID: 132952
GE CIRT Malicious Behaviour Detected
MEDIUM | TLP:RED | More

Owner: Mark Cooke | Set Status: Resolved | Current Phase: Initiate

Tasks | Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK | ARTIFACT

Recent Activity — All

- gecirt_triage_domain_score
- gecirt_triage_hash_score
- gecirt_utility_merge_related_alerts
- gecirt_utility_extract_artifact_iocs
- gecirt_triage_asset_info
- gecirt_utility_template_picker

Mark Cooke — 3 minutes ago
promoted to case "GE CIRT Malicious Behaviour Detected" (id: 132952)

- gecirt_utility_take_and_open_alert
- gecirt_utility_take_and_open_alert
- gecirt_response_proxy_block
  - block domain
  - add listitem

The following domains will not be blocked in [redacted] because they are already actively being blocked. Domains: artist[redacted]

All IP's that were tagged as "RISKY IPs" have been blocked. IP(s): 52.216.[redacted]

- gecirt_response_page_on_call

Please respond to the prompt to provide which team you want to page!

Successfully escalated to on-call.

- gecirt_utility_create_incident_from_al...
  - create container
  - no op

Incident created in container at https://[redacted]/mission/132954

Comment

ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY	TAGS
1967814	user:autogen	[redacted] - User Info	1 minutes ago	1 minutes ago	LOW	None	
1967813	device:autogen	[redacted] - ...	1 minutes ago	1 minutes ago	LOW	None	
1967812	history:autogen	[redacted] - ticket history	2 minutes ago	2 minutes ago	LOW	None	
1967811	event		3 minutes ago	3 minutes ago	MEDIUM	Mark Cooke	riskyip, ha...

Show 50 | COLLAPSE

Widgets | Notes | MANAGE WIDGETS

Incident created in container at https://[redacted]/mission/132954

display cirt widget
ip_reputation [cirtwidget]
domain_reputation [cirtwid

Domain [redacted]

VT DETECTED
9

Passive [redacted]

IP ADDRESS
52.216.[redacted]

Associated Files

Communicating Samples

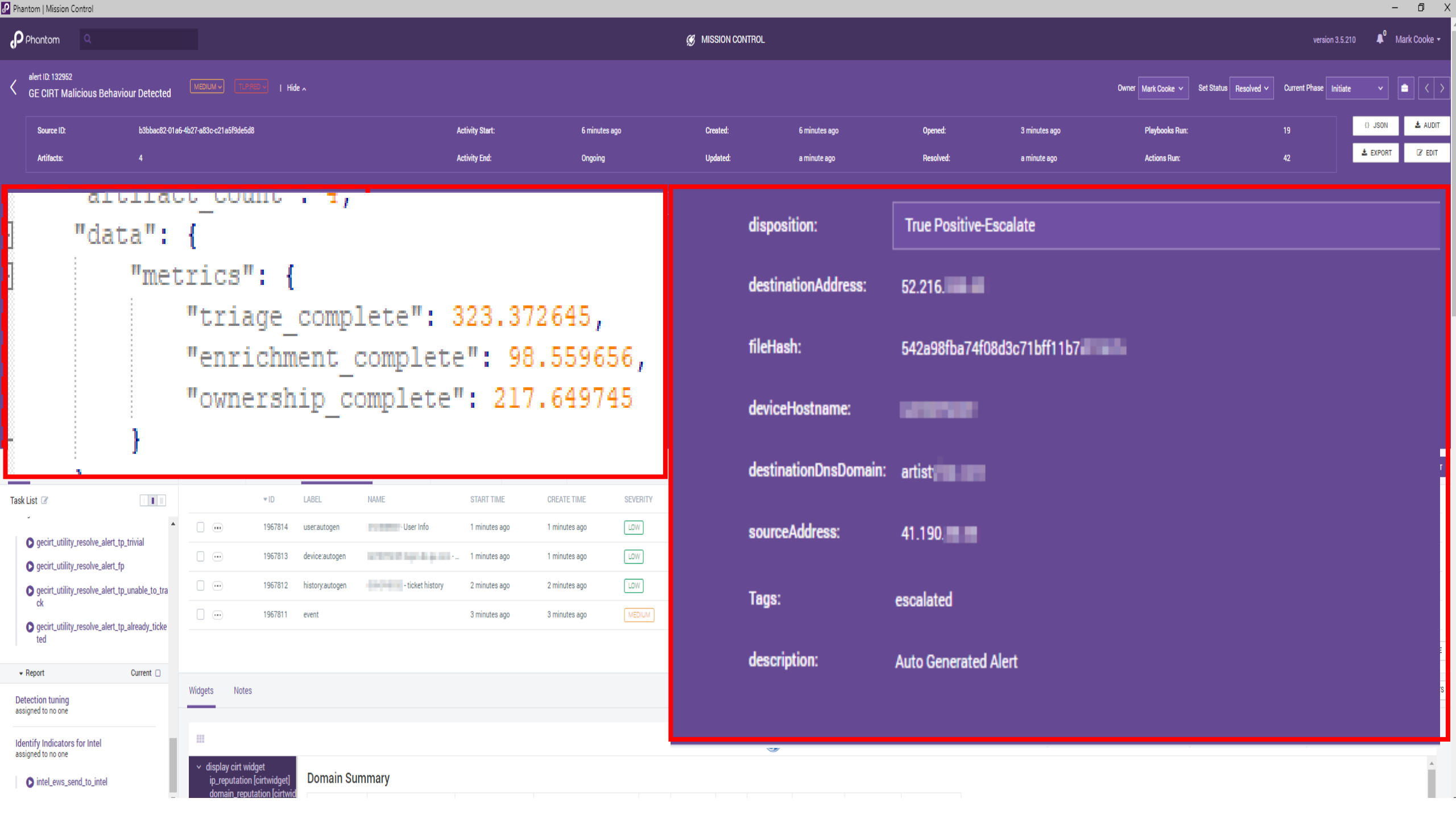
SCAN DATE	SHA256	DETECTION RATION
2018-06-20 13:03:15	be84152f172e125e95e9c98cc7fa8a8c03234c4e85f885195e9fe6a[redacted]	14/68
2017-12-15 23:14:13	cc8b3df59197d87c8031357adbaa9dff201059e8879c814d7fb9b6[redacted]	10/67
2017-11-19 03:02:10	96f68f54e3a0f9a42dcafff231168e3f74530d70f0686605be41343d[redacted]	8/68

Refferred Samples

SCAN DATE	SHA256	DETECTION RATION

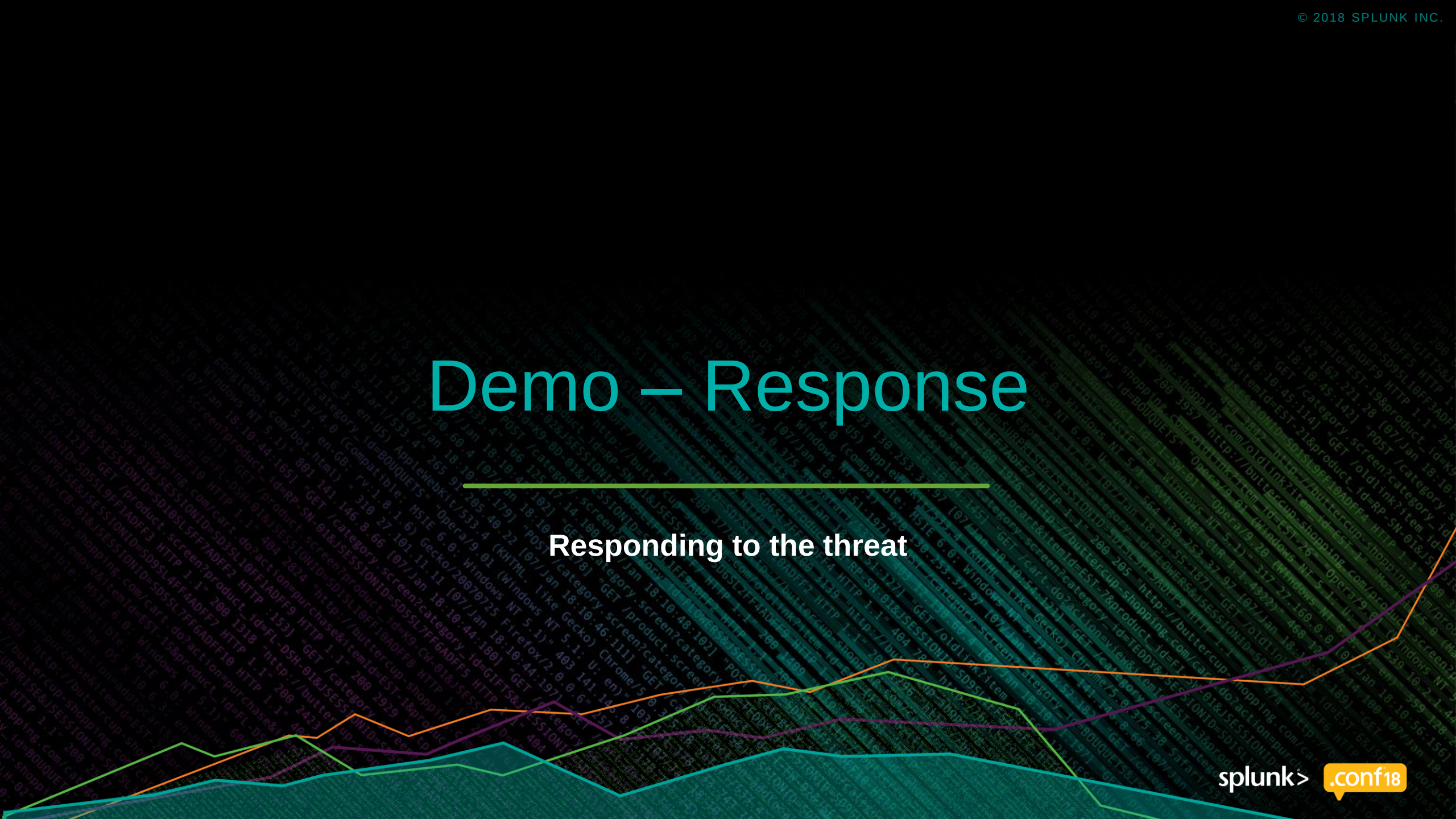
Downloaded Samples

SCAN DATE	SHA256	DETECTION RATION


Phantom | Mission Control
Phantom
MISSION CONTROL
version 3.5.210
Mark Cooke
alert ID: 132952
GE CIRT Malicious Behaviour Detected
MEDIUM
TLP:RED
Hide
Owner Mark Cooke
Set Status Resolved
Current Phase Initiate
Source ID: b3bbac82-01a6-4b27-a83c-c21a5f9de5d8
Activity Start: 6 minutes ago
Created: 6 minutes ago
Opened: 3 minutes ago
Playbooks Run: 19
Artifacts: 4
Activity End: Ongoing
Updated: a minute ago
Resolved: a minute ago
Actions Run: 42
JSON
AUDIT
EXPORT
EDIT
"artifact_count": 4,
"data": {
"metrics": {
"triage_complete": 323.372645,
"enrichment_complete": 98.559656,
"ownership_complete": 217.649745
}
disposition: True Positive-Escalate
destinationAddress: 52.216.
fileHash: 542a98fba74f08d3c71bff11b7
deviceHostname:
destinationDnsDomain: artist
sourceAddress: 41.190.
Tags: escalated
description: Auto Generated Alert
Task List
gecirt_utility_resolve_alert_tp_trivial
gecirt_utility_resolve_alert_fp
gecirt_utility_resolve_alert_tp_unable_to_track
gecirt_utility_resolve_alert_tp_already_ticketed
ID
LABEL
NAME
START TIME
CREATE TIME
SEVERITY
1967814 user:autogen User Info 1 minutes ago 1 minutes ago LOW
1967813 device:autogen 1 minutes ago 1 minutes ago LOW
1967812 history:autogen - ticket history 2 minutes ago 2 minutes ago LOW
1967811 event 3 minutes ago 3 minutes ago MEDIUM
Report
Current
Detection tuning
assigned to no one
Identify Indicators for Intel
assigned to no one
intel_ews_send_to_intel
Widgets
Notes
display cirt widget
ip_reputation [cirtwidget]
Domain Summary

Demo – Response

Responding to the threat



incident ID: 133711

GE CIRT Malicious Behavior Detected

HIGH | TLP:RED | More

Owner: Mark Cooke | Set Status: Open | Current Phase: Report

Tasks | Activity | Guidance

Timeline | HUD | Artifacts | Vault | Approvals | Reports

▶ ACTION | ▶ PLAYBOOK | + ARTIFACT

Task List

Report — Current

Create RT incident ticket
assigned to no one

- gecirt_response_create_ticket

Notify affected user
assigned to no one

- gecirt_response_employee_notification

Containment — Current

Contain system
assigned to no one

- gecirt_response_[redacted]_isolate
- gecirt_response_[redacted]_quarantine

Contain affected user
assigned to no one

Collection — Current

Review machine state
assigned to no one

- gecirt_triage_[redacted]_investigation

Collect malicious content
assigned to no one

- get file
- list file details

	ID	TAGS	NAME	LABEL	FILEHASH
	1970505		[redacted] - D...	device:autogen	None
	1970504		event	event	542a98fba74f08d3c71bff1[redacted]
	1970503		[redacted] - User Info	user:autogen	None
	1970502		[redacted] - ticket history	history:autogen	None

Show 50 | COLLAPSE

Widgets | Notes

MANAGE WIDGETS

No widgets to display

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

incident ID: 133711
GE CIRT Malicious Behavior Detected
HIGH | TLP:RED | More

Owner Mark Cooke | Set Status Open | Current Phase Report

Tasks | Activity | Guidance

Task List

Report — Current

Create RT incident ticket
assigned to no one

gecirt_response_create_ticket

Confirm Run Playbook
Cancel | RUN PLAYBOOK

Notify
assigne

gecirt_response_employee_notification

Containment — Current

Contain system
assigned to no one

gecirt_response_[redacted]solate

gecirt_response_[redacted]_quarantine

Contain affected user
assigned to no one

Collection — Current

Review machine state
assigned to no one

gecirt_triage_[redacted]_investigation

Collect malicious content
assigned to no one

get file

list file details

list folder contents

Back to case

Create RT incident ticket

Assigned to no one

DESCRIPTION

NOTES (0)

FILES (0)

MARK COMPLETE

Report — Current

Create RT incident ticket
assigned to no one

gecirt_response_create_ticket

Confirm Run Playbook
Cancel | RUN PLAYBOOK

Notify
assigne

gecirt_response_employee_notification

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

incident ID: 133711
GE CIRT Malicious Behavior Detected
HIGH | TLP:RED | More

Owner: Mark Cooke | Set Status: Open | Current Phase: Report

Tasks | Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK | ARTIFACT

Task List

Report — Current

Create RT incident ticket
assigned to no one
gecirt_response_create_ticket

Notify affected user
assigned to no one
gecirt_response_employee_notification

Containment — Current

Contain system
assigned to no one
gecirt_response_[redacted]_isolate
gecirt_response_[redacted]_quarantine

Contain affected user
assigned to no one

Collection — Current

Review machine state
assigned to no one
gecirt_triage_[redacted]_investigation

Collect malicious content
assigned to no one
get file
list file details

ID
1970506
1970505
1970504
1970503
1970502

Show 50 | COLLAPSE

Widgets | Notes | MANAGE WIDGETS

widgets to display

Report — Current

Create RT incident ticket
assigned to no one
gecirt_response_create_ticket

Notify affected user
assigned to no one
gecirt_response_employee_notification

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

incident ID: 133711
GE CIRT Malicious Behavior Detected
HIGH | TLP:RED | More

Owner: Mark Cooke | Set Status: Open | Current Phase: Report

Tasks | Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK | ARTIFACT

Task List

Report — Current
- Create RT incident ticket
  assigned to no one
  - gecirt_response_create_ticket
- Notify affected user
  assigned to no one
  - gecirt_response_employee_notification

Containment — Current
- Contain system
  assigned to no one
  - gecirt_response_[redacted]isolate
  - gecirt_response_[redacted]quarantine
- Contain affected user
  assigned to no one

Collection — Current
- Review machine state
  assigned to no one
  - gecirt_triage_[redacted]investigation
- Collect malicious content
  assigned to no one
  - get file
  - list file details

ID	TAGS	NAME	LABEL	FILEHASH
1970506		[redacted] - T...	ticket:autogen	
1970505		[redacted] - D...	device:autogen	
1970504		event	event	
1970503		[redacted] - User Info	user:autogen	
1970502		[redacted] - ticket history	history:autogen	

Name: [redacted] - Ticket Details
Label: ticket:autogen
Source ID: 2791f885-c79e-4757-a241-1e277f0bc403
Start Time: 0 minutes ago

Details

deviceHostname: [redacted]
rt: 712975

Show 50 | COLLAPSE

Widgets | Notes | MANAGE WIDGETS

[redacted]
- create incident ticket
- get ticket
- list tickets

incident ID: 133711

GE CIRT Malicious Behavior Detected

HIGH | TLP:RED | Hide

Owner: Mark Cooke | Set Status: Open | Current Phase: Report

Source ID:	df87de88-fc0c-4045-9552-54cc02c9cd6e	Activity Start:	5 minutes ago	Created:	3 minutes ago	Opened:	3 minutes ago	Playbooks Run:	16
Artifacts:	5	Activity End:	Ongoing	Updated:	a minute ago	Resolved:	Not resolved	Actions Run:	39

JSON | AUDIT | EXPORT | EDIT

Incident Type: Malware Infection

KC Detection Phase: KC 5: Installation

Detection Source: [redacted]

Detection Time: 2018-08-29 23:36:44.049551+00

Detection Indicator: GE CIRT Malicious Behavior Detected

Earliest Compromise Time: 2018-08-29 23:36:44.049551+00

description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Tortor at risus viverra adipiscing. Ultrices dui sapien eget mi proin sed libero enim. Consequat semper viverra nam libero justo laoreet sit amet cursus. Neque sodales ut etiam sit amet nisl purus. Ultricies mi quis hendrerit dolor magna eget. Condimentum id venenatis a condimentum vitae sapien pellentesque. Viverra suspendisse potenti nullam ac tortor vitae purus. Ut ornare lectus sit amet est. Ultricies mi eget mauris pharetra et ultrices. Eu scelerisque felis imperdiet proin fermentum leo vel orci. Egestas congue quisque egestas diam in arcu cursus euismod quis.

Tasks | Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK | ARTIFACT

Task List

Report — Current

Create RT incident ticket
assigned to no one

gecirt_response_create_ticket

Notify affected user
assigned to no one

gecirt_response_employee_notification

Containment — Current

Contain system
assigned to no one

	ID	TAGS	NAME	LABEL	FILEHASH
	1970506		[redacted] - T...	ticket:autogen	None

Name: [redacted] - Ticket Details
Label: ticket:autogen
Source ID: 2791f885-c79e-4757-a241-1e277f0bc403
Start Time: 0 minutes ago
Created: 0 minutes ago
Type: ticket
Severity: low

Details

deviceHostname: [redacted]
rt: 712975

	1970505		[redacted] - D...	device:autogen	None
	1970504		event	event	542a98fba74f08d3c71bf[redacted]

Ticket metadata

The Basics

Id: 712975
Status: open
Priority: 0/
Queue: Incident

Host Information

Asset Type: [redacted]
Asset Name (Hostname/Account Name): [redacted]
IP Address: [redacted]
Environment: [redacted]
Domain List: [redacted]

User Information

Owner SSO: [redacted]
Owner Name: [redacted]
Owner Email: [redacted]
Location (City): [redacted]
Country Name: [redacted]

Incident Response

Priority: [redacted]
Splunk ES Alert Urgency: [redacted]
Incident Type: [redacted]
Incident Ticket Reporter: [redacted]
Earliest Compromise Date/Time (UTC): [redacted]
Console Alert Date/Time (UTC): [redacted]
Detection Source: [redacted]
Detection Indicator: [redacted]
KC Phase Detected: [redacted]

ServiceNow

ServiceNow Ticket: *(no value)*
ServiceNow Type: *(no value)*
ServiceNow Ticket #: *(no value)*
ServiceNow Ticket Link: *(no value)*

Reminders

New reminder:
Subject:
Owner: [redacted]
Due:
Save

Dates

Created: 2018-08-29 23:40:25
Starts: Not set
Started: 2018-08-29 23:40:25
Last Contact: Not set
Due: Not set
Closed: Not set
Updated: 2018-08-29 23:40:25 by The RT System itself

Links

Graph

Depends on: (Create)
Depended on by: (Create)
Parents: (Create)
Children: (Create)
Refers to: (Create)
Referred to by: (Create)

Create | Depends on | Ticket in | Analyze

VIP: *(no value)*
EventID: *(no value)*
iReport Ticket #: *(no value)*
Message ID: *(no value)*
RCA Status: *(no value)*
RCA Confidence: *(no value)*
RCA Toolkit: *(no value)*
Delivery Method: *(no value)*
Delivery Method Other: *(no value)*
Application Other: *(no value)*
CVE(s): *(no value)*
Exploit Layer: *(no value)*
Exploit Layer Other: *(no value)*
Unmanaged Asset: *(no value)*
Exploited Software: *(no value)*
Exploited Software Other: *(no value)*
Exploited Software Version: *(no value)*
Phantom Data: *(no value)*

People

Owner: [redacted]
Requestors:
Cc:
AdminCc:

History

Show all quoted text — Show full headers

2018-08-29 23:40:25 **Service phantom_rt - Ticket created**

Reply Comment Forward

From: [redacted]

Subject: [redacted] - GE CIRT Malicious Behavior Detected

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Tortor at risus viverra adipiscing. Ultrices dui sapien eget mi proin sed libero enim. Consequat semper viverra nam libero justo laoreet sit amet cursus. Neque sodales ut etiam sit amet nisl purus. Ultricies mi quis hendrerit dolor magna eget. Condimentum id venenatis a condimentum vitae sapien pellentesque. Viverra suspendisse potenti nullam ac tortor vitae purus. Ut ornare lectus sit amet est. Ultricies mi eget mauris pharetra et ultrices. Eu scelerisque felis imperdiet proin fermentum leo vel orci. Egestas congue quisque egestas diam in arcu cursus euismod quis.

Download (untitled) / with headers
text/plain 745B

Added by Phantom for container id: 133711

2018-08-29 23:40:25 **The RT System itself - Cc group @CORP Security Operations Center All added**

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

incident ID: 133711
GE CIRT Malicious Behavior Detected
HIGH | TLP:RED | More

Owner Mark Cooke | Set Status Open | Current Phase Report

Tasks | Activity | Guidance

Task List

Report — Current

Create RT incident ticket
assigned to no one

gecirt_response_create_ticket

Notify affected user
assigned to no one

gecirt_response_employee_notification

Confirm Run Playbook

Cancel | RUN PLAYBOOK

Contai
assigned to no one

gecirt_response_ isolate

gecirt_response_ quarantine

Contain affected user
assigned to no one

Collection — Current

Review machine state
assigned to no one

gecirt_triage_ investigation

Collect malicious content
assigned to no one

get file

list file details

list folder contents

Back to case

Notify affected user

Assigned to no one

MARK COMPLETE

DESCRIPTION

NOTES (0)

FILES (0)

Notify affected user
assigned to no one

gecirt_response_employee_notification

Confirm Run Playbook

Cancel | RUN PLAYBOOK

Contai
assigned to no one

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

incident ID: 133711
GE CIRT Malicious Behavior Detected
HIGH | TLP:RED | More

Owner: Mark Cooke | Set Status: Open | Current Phase: Report

Tasks | Activity | Guidance

Task List

- Report — Current
  - Create RT incident ticket
    assigned to no one
    - gecirt_response_create_ticket
  - Notify affected user
    assigned to no one
    - gecirt_response_employee_notification
- Containment — Current
  - Contain system
    assigned to no one
    - gecirt_response_[redacted]isolate
  - Contai
    assigned to no one
- Collection — Current
  - Review machine state
    assigned to no one
    - gecirt_triag[redacted]investigation
  - Collect malicious content
    assigned to no one
    - get file
    - list file details
    - list folder contents

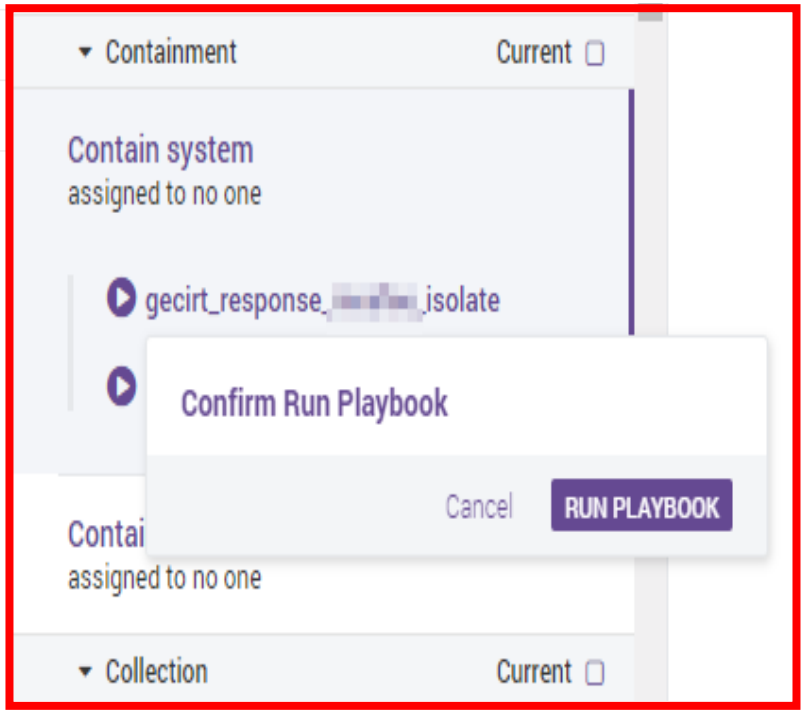
Confirm Run Playbook
Cancel | RUN PLAYBOOK

Back to case

Contain system
Assigned to: no one

MARK COMPLETE

DESCRIPTION
NOTES (0)
FILES (0)



Phantom | Mission Control

Phantom

MISSION CONTROL

Playbook gecirt_triage_tanium_investigation started successfully.

incident ID: 133711

GE CIRT Malicious Behavior Detected

HIGH TLP:RED | More

Owner Mark Cooke Set Status Open Current Phase Report

Tasks Activity Guidance

Task List

gecirt_response_employee_notification

Containment Current

Contain system
assigned to no one

gecirt_response_[redacted]isolate

gecirt_response_[redacted]quarantine

Contain affected user
assigned to no one

Collection Current

Review machine state
assigned to no one

gecirt_triage_[redacted]investigation

Collect malicious content
assigned to no one

get file

list file details

list folder contents

gecirt_response_[redacted]bup_collection

Analyze malicious content
assigned to no one

detonate file

detonate url

Back to case

Review machine state

Assigned to no one

MARK COMPLETE

DESCRIPTION

NOTES (0)

FILES (0)

Phantom | Mission Control

Phantom

MISSION CONTROL

version 3.5.210

Mark Cooke

incident ID: 133711

GE CIRT Malicious Behavior Detected

HIGH

TLP:RED

More

Owner Mark Cooke

Set Status Open

Current Phase Report

Tasks Activity Guidance

Recent Activity All

gecirt_triage_asset_info

gecirt_utility_template_picker

Mark Cooke 6 minutes ago

gecirt_utility_take_and_open_alert

promoted to case "GE CIRT Malicious Behavior Detected" (id: 133711)

added event "GE CIRT Malicious Behavior Detected" (id: 133710)

gecirt_response_create_ticket

gecirt_response_create_ticket_main

gecirt_response_employee_notificati...

gecirt_response_ isolate

The following hosts were successfully isolated and their agent woke up.

Hosts:

gecirt_triage_ investigation

get lake client info

list processes with md5

list open ports

list listen ports

list installed applications

list autoruns

list scheduled tasks

list shim cache

Comment

	1970503	User Info	user:autogen	None
	1970502	ticket history	history:autogen	None

Show 50

COLLAPSE

Widgets Notes

MANAGE WIDGETS

gecirt_triage_ investigation

get lake client info

list processes with md5

list open ports

list listen ports

list installed applications

list autoruns

list scheduled tasks

list shim cache

create incident ticket

cirt rt

get ticket

list tickets

update ticket

update incident ticket

GE Imagination at work

display.irt.widget
irtwidget]

Malicious Processes

PATH	MD5 HASH	VT SCORE	VT LINK

Suspicious Processes

PATH	MD5 HASH	VT LINK
c:\lr\win32\tools_regdump7.exe	7cb9018c53741d90578c77820a0b308a	LINK
c:\program files\opsware\agent\pylibs\watchdog\watchdog.exe	5f7ba383d812433078e012ec203921dc	LINK
\msg711.acm		LINK
\imaadp32.acm		LINK
\msyuv.dll		LINK
C:\Windows\SysWOW64\Wow64cpu.dll		LINK
C:\windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe		LINK
C:\WINDOWS\System32\Drivers\mfeavfk01.sys		LINK
\msgsm32.acm		LINK
c:\scheduledtask\fixwsus_regset_labclient.bat	BD4CB0660CCE8DF28C59BC015B70F711	LINK
c:\lr\win32\startlr.bat	F2A6EB9E655209DDE317423CA423CFCB	LINK
C:\windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe		LINK
c:\program files\opsware\agent\pylibs\watchdog\watchdog.exe	5F7BA383D812433078E012EC203921DC	LINK
\midimap.dll		LINK
\msyuv.dll		LINK
\tsbyuv.dll		LINK
C:\Windows\SysWoW64\Wow64.dll		LINK
\iyuv_32.dll		LINK
C:\Program Files (x86)\Windows Mail\WinMail.exe		LINK
\msyuv.dll		LINK
\msrle32.dll		LINK
C:\Windows\SysWoW64\Wow64win.dll		LINK
\msadp32.acm		LINK
c:\program files\actividentity\activclient\actsinit.exe	F3F601ED07BC90BB93D4277363051E5F	LINK
\iyuv_32.dll		LINK
C:\Program Files\Windows Mail\WinMail.exe		LINK
\msacm32.drv		LINK
\msvidc32.dll		LINK

Running Processes

\iyuv_32.dll	LINK
C:\Program Files\Windows Mail\WinMail.exe	LINK
\msacm32.drv	LINK
\msvidc32.dll	LINK

Running Processes

PATH	MD5 HASH	VT SCORE	VT LINK
c:\windows\system32\conhost.exe	[redacted]d5685ba7	0/68	LINK
c:\lr\win32\tools_regdump7.exe	[redacted]20a0b308a	unknown	LINK
c:\program files\splunkuniversalforwarder\bin\splunk-winevtlog.exe	[redacted]eb799f01	0/62	LINK
c:\windows\system32\lsass.exe	[redacted]c6ceffad	0/67	LINK
c:\windows\system32\svchost.exe	[redacted]cb38ec47	0/66	LINK
c:\program files\opsware\agent\lcpython15\python.exe	[redacted]a5dfbdb3	0/56	LINK
c:\windows\system32\wininit.exe	[redacted]8faf3948	0/68	LINK
c:\program files\common files[redacted]systemcore\mcshield.exe	[redacted]a3d61b8f	0/68	LINK
c:\lr\win32\tools_fget.exe	[redacted]db2c9fc7	0/66	LINK
c:\windows\syswow64\cscript.exe	[redacted]0125740d	0/67	LINK
c:\windows\system32\mfevtps.exe	[redacted]fe74b32b	0/65	LINK
c:\windows\system32\wbem\wmiprvse.exe	[redacted]61e9ae33	0/68	LINK
c:\windows\system32\dwm.exe	[redacted]03ebf03	0/68	LINK
c:\program files\common files[redacted]systemcore\mfefire.exe	[redacted]51b0a67	0/59	LINK
c:\program files\veritas\netbackup\bin\nbdisco.exe	[redacted]0e2ce8eb	0/56	LINK
c:\program files\vmware\vmware tools\vmtoolsd.exe	[redacted]28100022	0/67	LINK
c:\program files\veritas\netbackup\bin\vnetd.exe	[redacted]53d3bbfb	0/55	LINK
c:\lr\win32\tools_tee.exe	[redacted]76bcd492	0/68	LINK
c:\windows\system32\dllhost.exe	[redacted]2d10e9de	0/67	LINK
c:\program files (x86)\[redacted]	[redacted]cf283f9a	0/62	LINK
c:\windows\syswow64\wbem\wmiprvse.exe	[redacted]59d260e78	0/68	LINK
c:\program files\veritas\netbackup\bin\bpinetd.exe	[redacted]767c58b3	0/56	LINK
c:\program files\vmware\vmware tools\vmware vgauth\vgauthservice.exe	[redacted]e744a8be	0/68	LINK
c:\windows\system32\spoolsv.exe	[redacted]	0/67	LINK

Tasks Activity Guidance

Task List

- Report Current
- Containment Current
- Collection Current
- Eradication Current

Proxy block malicious domains
assigned to no one

gecirt_response_proxy_block

Remove malicious content
assigned to no one

terminate process

Launch AV scan
assigned to no one

gecirt_remediation_[redacted]_full_scan

Confirm Run Playbook

Cancel RUN PLAYBOOK

Identif
assigne

- Recovery Current

Re-image affected systems
assigned to no one

gecirt_remediate_reimage_device

Validate restoration
assigned to no one

Remove containment
assigned to no one

Back to case

Launch AV scan

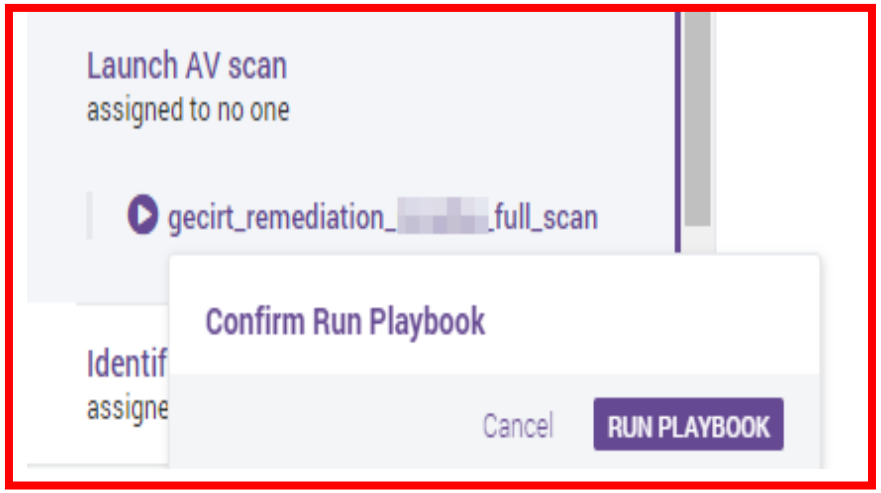
Assigned to no one

MARK COMPLETE

DESCRIPTION

NOTES (0)

FILES (0)



Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

incident ID: 133711
GE CIRT Malicious Behavior Detected
HIGH | TLP:RED | More

Owner: Mark Cooke | Set Status: Open | Current Phase: Report

Tasks | Activity | Guidance

Task List

- Report — Current
- Containment — Current
- Collection — Current
- Eradication — Current
- Recovery — Current
- Closing Tasks — Current

Determine root cause
assigned to no one

Identify Indicators for Intel
assigned to no one

intel_ews_send_to_intel

Sync key incident data to RT
assigned to no one

Create detection request tickets
assigned to no one

Close ServiceNow ticket
assigned to no one

Close RT ticket
assigned to no one

Resolve container
assigned to no one

Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK

1 Full Scan(s) - Success
1 Isolation(s) - Success
1 Notification(s) - Success
1 Ticket(s) - Success

PINNED ITEMS (4)

Widgets | Notes

MANAGE WIDGETS

Approvals | Reports

1 Full Scan(s) - Success
1 Isolation(s) - Success
1 Notification(s) - Success
1 Ticket(s) - Success

People

Owner: Mark Cooke
Requestors:
Cc:
AdminCc:

History

Show all quoted text — Show full headers

2018-08-29 23:40:25 Service phantom_rt - Ticket created
From:
Subject: - GE CIRT Malicious

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor in
venenatis a condimentum vitae sapien pellentesque. Viverra suspendisse potenti

---
Added by Phantom for container id: 133711

Reply Comment Forward

Download (untitled) / with headers
text/plain 745B

2018-08-29 23:40:25 The RT System itself - Cc group added

2018-08-29 23:43:56 Service phantom_rt - Comments added

Phantom has successfully sent the quarantine/scan notification template to the user. Container /mission/133711

2018-08-29 23:44:07 Service phantom_rt - Contain Date/Time (UTC) 2018-08-29 23:44:05 added

2018-08-29 23:44:07 Service phantom_rt - Contain Method Virtual Isolation added

2018-08-29 23:44:07 Service phantom_rt - Comments added

Phantom has applied isolation and awoke the agent successfully for at 2018-08-29 23:44:05. Container nission/133711

2018-08-29 23:45:18 Service phantom_rt - Comments added

Phantom has applied a Full Scan for . Container /mission/133711

2018-08-29 23:40:25 The RT System itself - Cc group
2018-08-29 23:43:56 Service phantom_rt - Comments added
Phantom has successfully sent the quarantine/scan notification template to the us
2018-08-29 23:44:07 Service phantom_rt - Contain Date/Time (UTC) 2018-08
2018-08-29 23:44:07 Service phantom_rt - Contain Method Virtual Isolation
2018-08-29 23:44:07 Service phantom_rt - Comments added
Phantom has applied isolation and awoke the agent successfully for
2018-08-29 23:45:18 Service phantom_rt - Comments added
Phantom has applied a Full Scan for

Reply Comment Forward

Download (untitled) / with headers
text/plain 145B

Reply Comment Forward

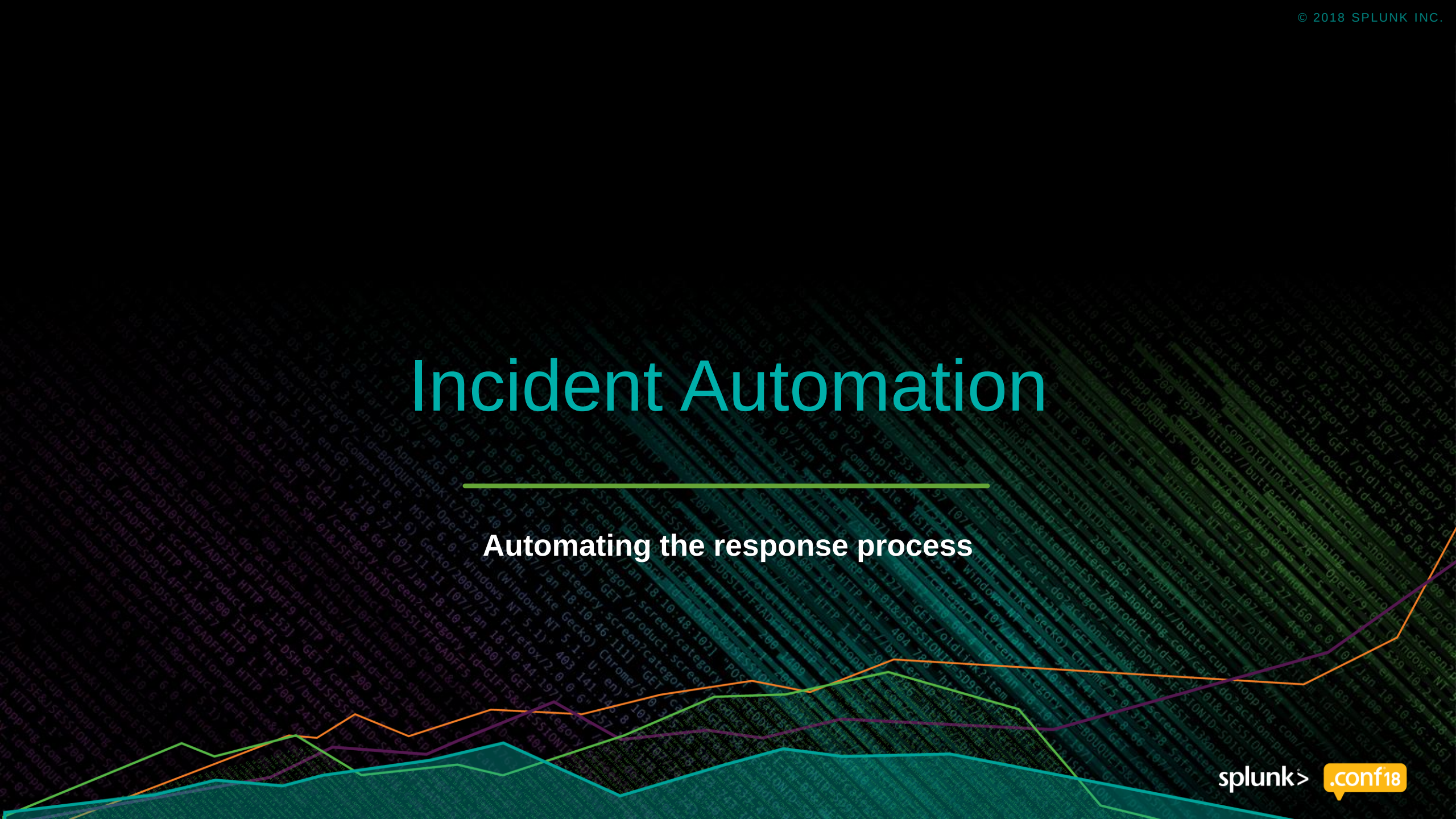
Download (untitled) / with headers
text/plain 177B

Reply Comment Forward

Download (untitled) / with headers
text/plain 146B

Incident Automation

Automating the response process



Phantom | Analyst Queue

Phantom

version 3.5.210

Mark Cooke

Sources

Show Select a filter EVENT IMPORT

Label: incident_auto Status: New Open CLEAR SAVE

Dynamic Updates Show Stats

ID	STATUS	NAME	ARTIFACTS	CREATED	TAGS
133716	Open	GE CIRT Malicious Behavior Detected	1	0 minutes ago	running

Show 50

Label: incident_auto Status: New Open CLEAR SAVE

ID STATUS NAME

133716 Open GE CIRT Malicious Behavior Detected

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

incident_auto ID: 133716

GE CIRT Malicious Behavior Detected

HIGH | TLP:RED | SLA: an hour remaining | More

Owner: Select... | Set Status: Open

Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK | ARTIFACT

Recent Activity | All

ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY	TAGS
1970518	event	event	0 minutes ago	0 minutes ago	MEDIUM	Mark Cooke	

Show 50 | COLLAPSE

Widgets | Notes | MANAGE WIDGETS

BEST PRACTICAL™

list tickets
Incident [cirt rt]

ID	QUEUE	SUBJECT
712911	Incident	[redacted] - Malicious Activity Discovered in the Registry
712947	Incident	[redacted] - Endpoint - CIRT - Crowd Strike Alert - 20768 - Rule - A

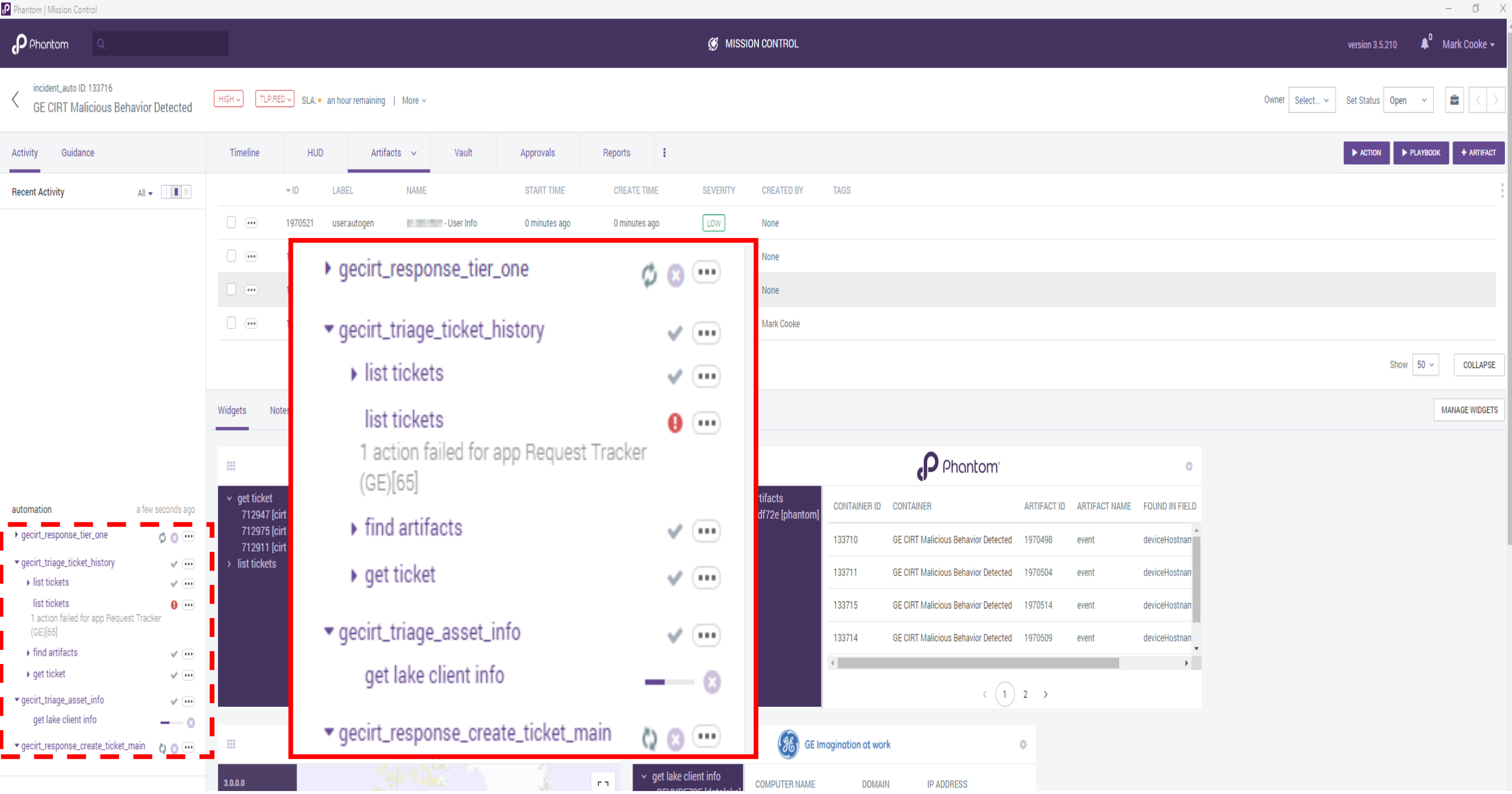
automation — a few seconds ago

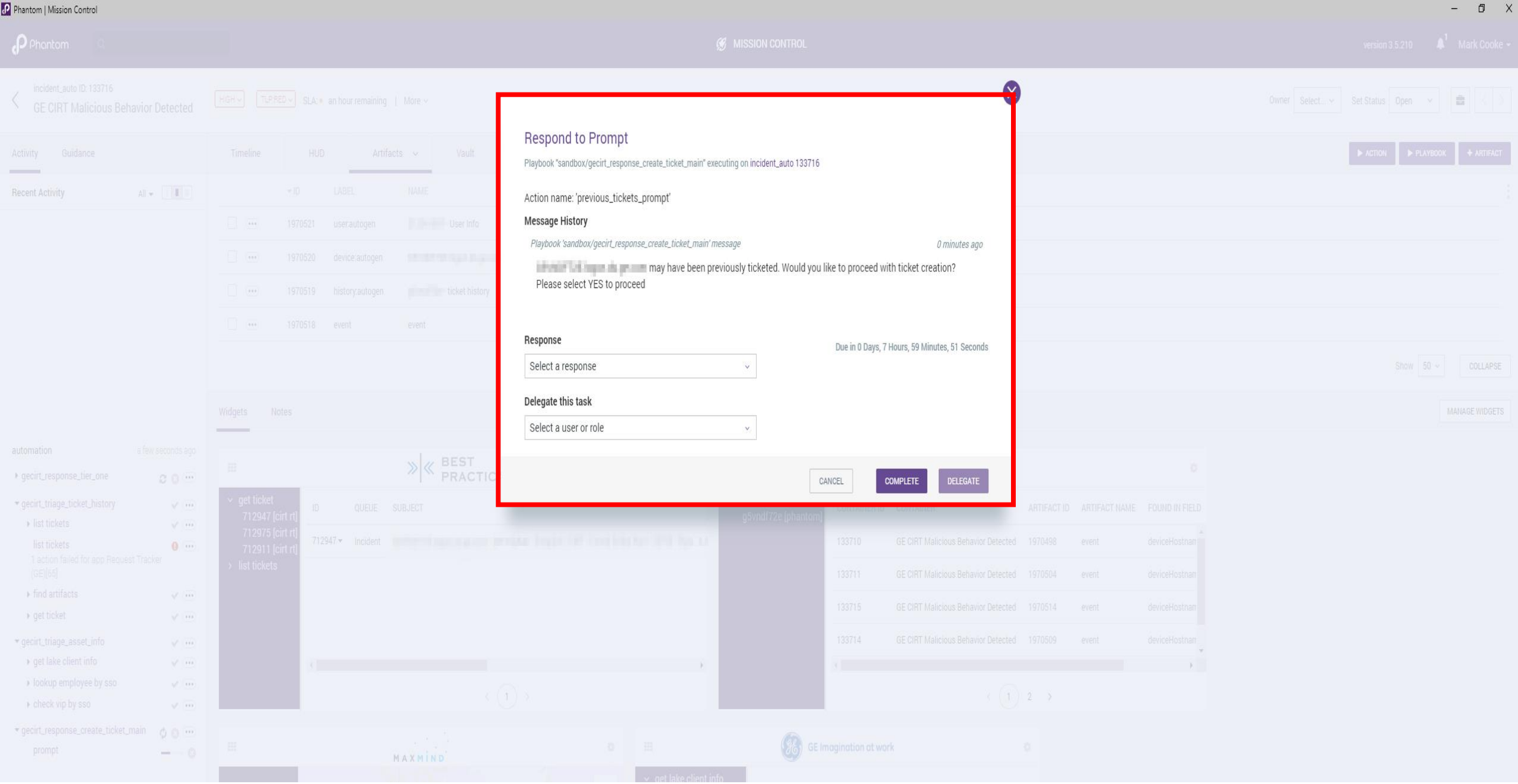
- gecirt_response_tier_one
- gecirt_triage_ticket_history
  - list tickets
  - list tickets

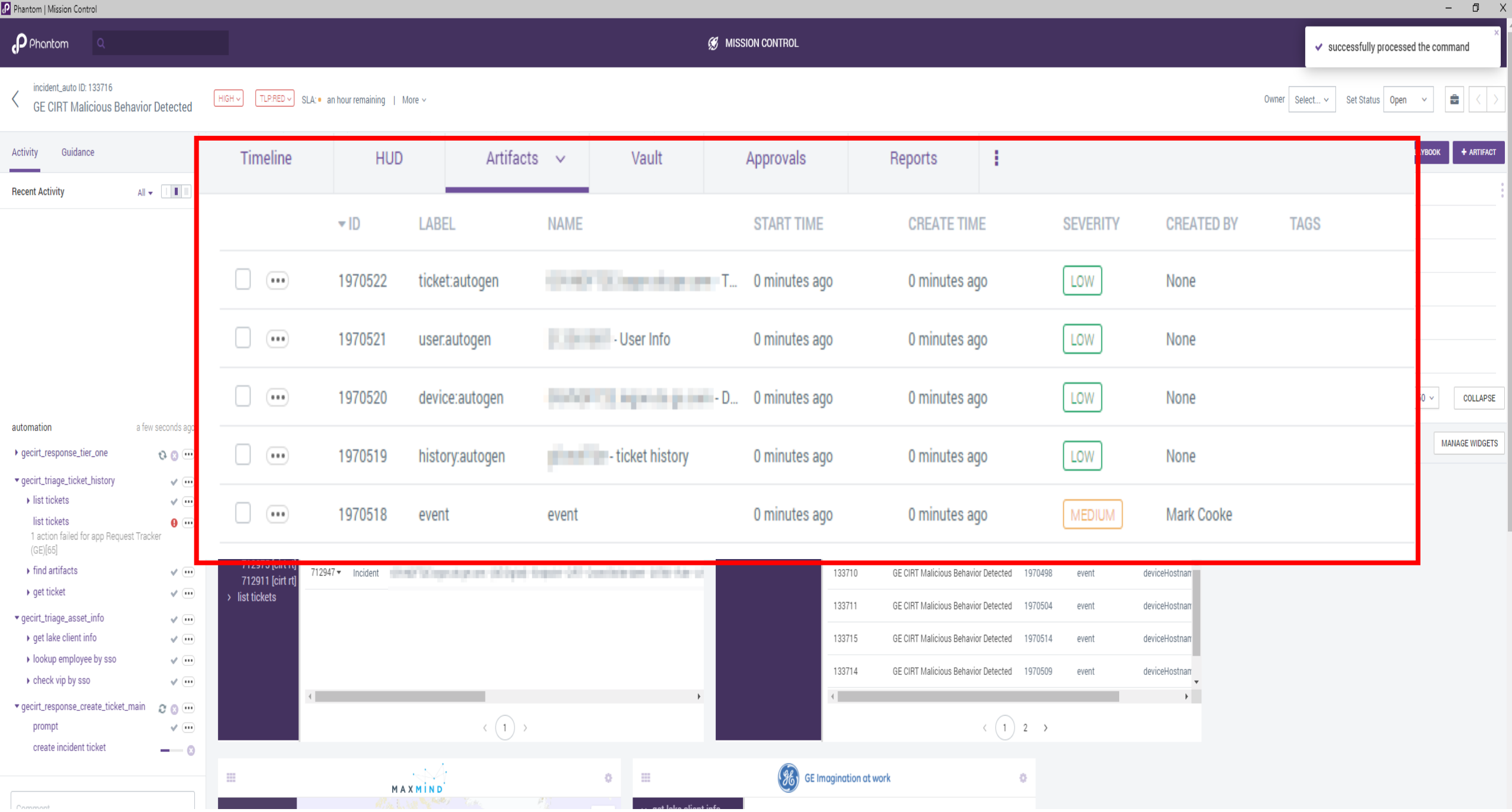
automation — a few seconds ago

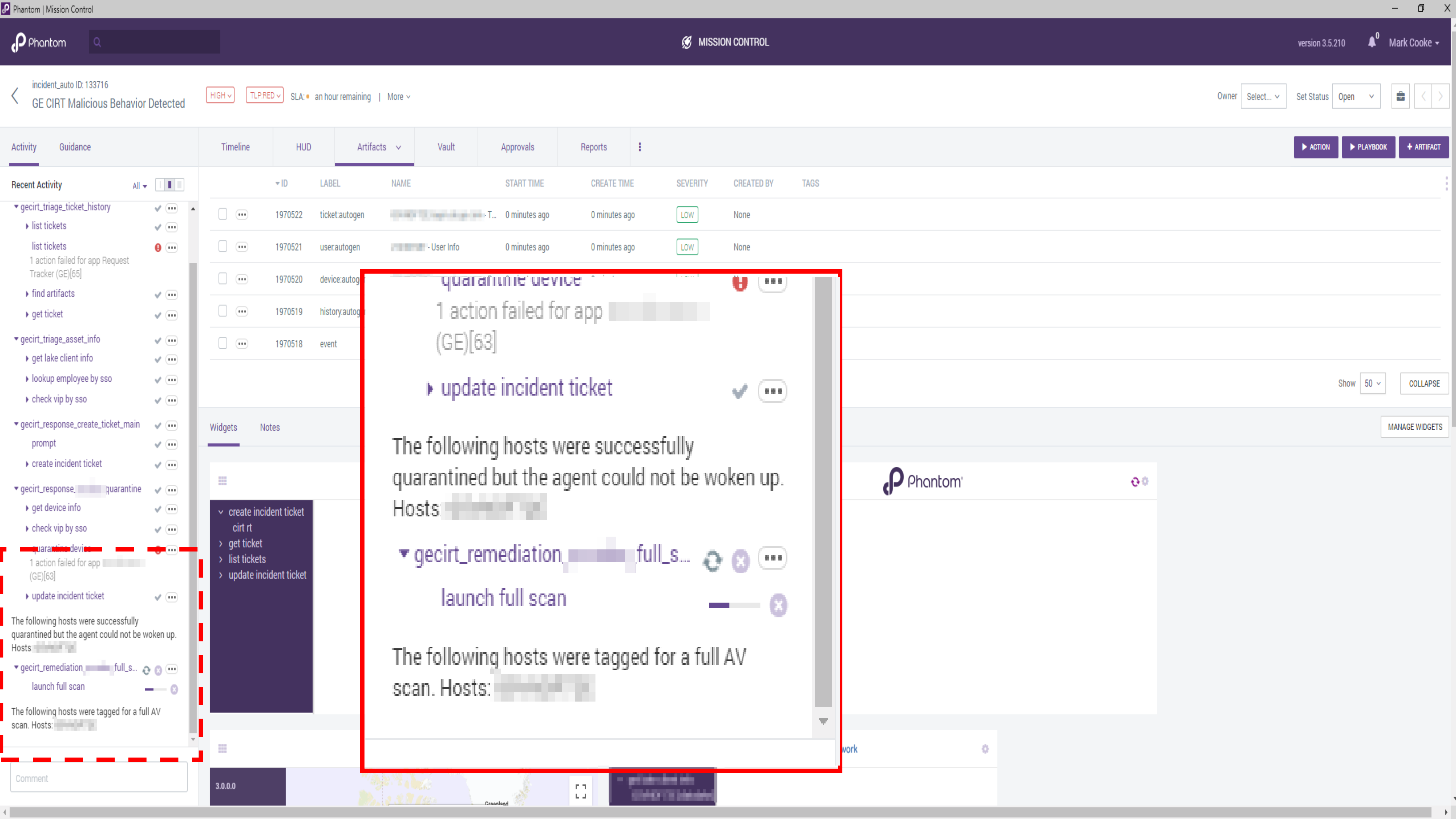
- gecirt_response_tier_one
- gecirt_triage_ticket_history
  - list tickets
  - list tickets

Comment


Phantom | Mission Control
Phantom
MISSION CONTROL
version 3.5.210
Mark Cooke
incident_auto ID: 133716
GE CIRT Malicious Behavior Detected
HIGH
TLP:RED
SLA: an hour remaining | More
Owner
Select...
Set Status
Open
Activity
Guidance
Timeline
HUD
Artifacts
Vault
Approvals
Reports
ACTION
PLAYBOOK
ARTIFACT
Recent Activity
All
ID
LABEL
NAME
START TIME
CREATE TIME
SEVERITY
CREATED BY
TAGS
1970521
user:autogen
- User Info
0 minutes ago
0 minutes ago
LOW
None
None
None
Mark Cooke
Show
50
COLLAPSE
Widgets
Notes
MANAGE WIDGETS
gecirt_response_tier_one
gecirt_triage_ticket_history
list tickets
list tickets
1 action failed for app Request Tracker (GE)[65]
find artifacts
get ticket
gecirt_triage_asset_info
get lake client info
gecirt_response_create_ticket_main
automation
a few seconds ago
gecirt_response_tier_one
gecirt_triage_ticket_history
list tickets
list tickets
1 action failed for app Request Tracker (GE)[65]
find artifacts
get ticket
gecirt_triage_asset_info
get lake client info
gecirt_response_create_ticket_main
get ticket
712947 [cirt
712975 [cirt
712911 [cirt
list tickets
Phantom
CONTAINER ID
CONTAINER
ARTIFACT ID
ARTIFACT NAME
FOUND IN FIELD
133710
GE CIRT Malicious Behavior Detected
1970498
event
133711
GE CIRT Malicious Behavior Detected
1970504
event
133715
GE CIRT Malicious Behavior Detected
1970514
event
133714
GE CIRT Malicious Behavior Detected
1970509
event
GE Imagination at work
get lake client info
COMPUTER NAME
DOMAIN
IP ADDRESS
3.0.0.0


Phantom | Mission Control
Phantom
MISSION CONTROL
version 3.5.210
Mark Cooke
incident_auto ID: 133716
GE CIRT Malicious Behavior Detected
HIGH
TLP:RED
SLA: an hour remaining | More
Owner
Select...
Set Status
Open
Activity
Guidance
Timeline
HUD
Artifacts
Vault
ACTION
PLAYBOOK
ARTIFACT
Recent Activity
All
ID
LABEL
NAME
1970521 user:autogen User Info
1970520 device:autogen
1970519 history:autogen ticket history
1970518 event event
Respond to Prompt
Playbook "sandbox/gecirt_response_create_ticket_main" executing on incident_auto 133716
Action name: 'previous_tickets_prompt'
Message History
Playbook 'sandbox/gecirt_response_create_ticket_main' message
0 minutes ago
may have been previously ticketed. Would you like to proceed with ticket creation?
Please select YES to proceed
Response
Due in 0 Days, 7 Hours, 59 Minutes, 51 Seconds
Select a response
Delegate this task
Select a user or role
CANCEL
COMPLETE
DELEGATE
Show
50
COLLAPSE
Widgets
Notes
MANAGE WIDGETS
automation
a few seconds ago
gecirt_response_tier_one
gecirt_triage_ticket_history
list tickets
list tickets
1 action failed for app Request Tracker (GE)(66)
find artifacts
get ticket
gecirt_triage_asset_info
get lake client info
lookup employee by sso
check vip by sso
gecirt_response_create_ticket_main
prompt
BEST PRACTIC
get ticket
712947 [cirt rt]
712975 [cirt rt]
712911 [cirt rt]
list tickets
ID
QUEUE
SUBJECT
712947
Incident
g5vndf72c [phantom]
ARTIFACT ID
ARTIFACT NAME
FOUND IN FIELD
133710 GE CIRT Malicious Behavior Detected 1970498 event deviceHostnan
133711 GE CIRT Malicious Behavior Detected 1970504 event deviceHostnan
133715 GE CIRT Malicious Behavior Detected 1970514 event deviceHostnan
133714 GE CIRT Malicious Behavior Detected 1970509 event deviceHostnan
MAXMIND
GE Imagination at work
get lake client info


Phantom | Mission Control
Phantom
MISSION CONTROL
successfully processed the command
incident_auto ID: 133716
GE CIRT Malicious Behavior Detected
HIGH
TLP:RED
SLA: an hour remaining | More
Owner Select...
Set Status Open
Activity
Guidance
Recent Activity
All
Timeline
HUD
Artifacts
Vault
Approvals
Reports
ID
LABEL
NAME
START TIME
CREATE TIME
SEVERITY
CREATED BY
TAGS
1970522 ticket:autogen T... 0 minutes ago 0 minutes ago LOW None
1970521 user:autogen - User Info 0 minutes ago 0 minutes ago LOW None
1970520 device:autogen - D... 0 minutes ago 0 minutes ago LOW None
1970519 history:autogen - ticket history 0 minutes ago 0 minutes ago LOW None
1970518 event event 0 minutes ago 0 minutes ago MEDIUM Mark Cooke
+ ARTIFACT
COLLAPSE
MANAGE WIDGETS
automation
a few seconds ago
gecirt_response_tier_one
gecirt_triage_ticket_history
list tickets
list tickets
1 action failed for app Request Tracker (GE)[65]
find artifacts
get ticket
gecirt_triage_asset_info
get lake client info
lookup employee by sso
check vip by sso
gecirt_response_create_ticket_main
prompt
create incident ticket
712911 [cirt rt]
list tickets
712947 Incident
133710 GE CIRT Malicious Behavior Detected 1970498 event deviceHostnan
133711 GE CIRT Malicious Behavior Detected 1970504 event deviceHostnan
133715 GE CIRT Malicious Behavior Detected 1970514 event deviceHostnan
133714 GE CIRT Malicious Behavior Detected 1970509 event deviceHostnan
MAXMIND
GE Imagination at work


Phantom | Mission Control
Phantom
MISSION CONTROL
version 3.5.210
Mark Cooke
incident_auto ID: 133716
GE CIRT Malicious Behavior Detected
HIGH
TLP:RED
SLA: an hour remaining | More
Owner Select...
Set Status Open
Activity
Guidance
Timeline
HUD
Artifacts
Vault
Approvals
Reports
ACTION
PLAYBOOK
ARTIFACT
Recent Activity All
ID
LABEL
NAME
START TIME
CREATE TIME
SEVERITY
CREATED BY
TAGS
1970522 ticket:autogen 0 minutes ago 0 minutes ago LOW None
1970521 user:autogen - User Info 0 minutes ago 0 minutes ago LOW None
1970520 device:autog
1970519 history:autog
1970518 event
gecirt_triage_ticket_history
list tickets
list tickets
1 action failed for app Request Tracker (GE)[65]
find artifacts
get ticket
gecirt_triage_asset_info
get lake client info
lookup employee by sso
check vip by sso
gecirt_response_create_ticket_main
prompt
create incident ticket
gecirt_response_ quarantine
get device info
check vip by sso
quarantine device
1 action failed for app
(GE)[63]
update incident ticket
The following hosts were successfully quarantined but the agent could not be woken up. Hosts
gecirt_remediation_ full_s...
launch full scan
The following hosts were tagged for a full AV scan. Hosts:
Comment
Show 50
COLLAPSE
Widgets
Notes
MANAGE WIDGETS
create incident ticket
cirt rt
get ticket
list tickets
update incident ticket
3.0.0.0
Greenland
work

Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

incident_auto ID: 133716

GE CIRT Malicious Behavior Detected

HIGH | TLP:RED | SLA: an hour remaining | More

Owner: Select... | Set Status: Open

Activity | Guidance

Recent Activity | All

- gecirt_response_create_ticket_main
  - prompt
  - create incident ticket
- gecirt_response_[redacted]quarantine
  - get device info
  - check vip by sso
  - quarantine device
    1 action failed for app[redacted] (GE)[63]
  - update incident ticket

The following hosts were successfully quarantined but the agent could not be woken up. Hosts: [redacted]

- gecirt_remediation_[redacted]full_scan
  - launch full scan
  - update incident ticket
  - add listitem

The following hosts were tagged for a full AV scan. Hosts: [redacted]

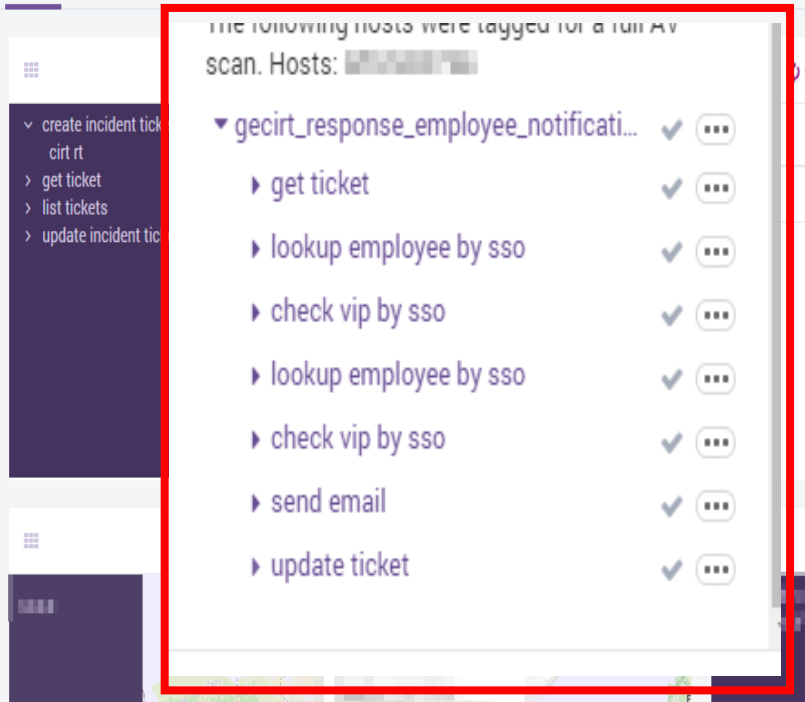
- gecirt_response_employee_notificati...
  - get ticket
  - lookup employee by sso
  - check vip by sso
  - lookup employee by sso
  - check vip by sso
  - send email
  - update ticket

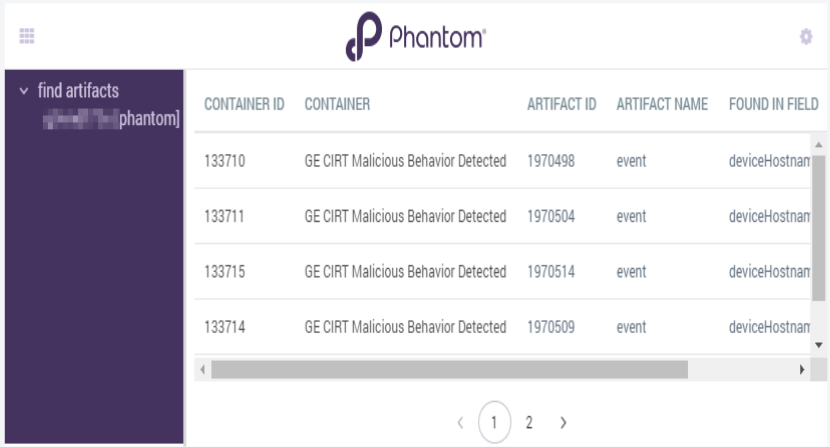
Comment

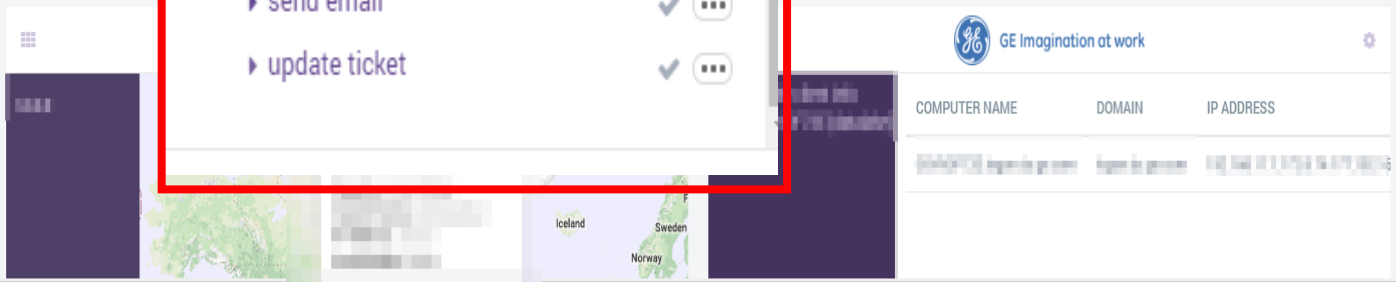
1970522	ticket:autogen	[redacted] T...	0 minutes ago	0 minutes ago	LOW	None
1970521	user:autogen	User Info	0 minutes ago	0 minutes ago	LOW	None
1970520	device:autogen	[redacted] D...	0 minutes ago	0 minutes ago	LOW	None
1970519	history:autogen	ticket history	0 minutes ago	0 minutes ago	LOW	None
1970518	event	event	0 minutes ago	0 minutes ago	MEDIUM	Mark Cooke

Show 50 | COLLAPSE

Widgets | Notes | MANAGE WIDGETS







Phantom | Mission Control

Phantom | MISSION CONTROL | version 3.5.210 | Mark Cooke

incident_auto ID: 133716

GE CIRT Malicious Behavior Detected

HIGH | TLP:RED | SLA: an hour remained | More

Owner: Select... | Set Status: Resolved

Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports | ACTION | PLAYBOOK

Recent Activity | All

- gecirt_response_create_ticket_main
  - prompt
  - create incident ticket
- gecirt_response quarantine
  - get device info
  - check vip by sso
  - quarantine device
    1 action failed for app (GE)[63]
  - update incident ticket

The following hosts were successfully quarantined but the agent could not be woken up. Hosts:

- gecirt_remediation full_scan
  - launch full scan
  - update incident ticket
  - add listitem

The following hosts were tagged for a full AV scan. Host

- gecirt_response_employee_notificati...
  - get ticket
  - lookup employee by sso
  - check vip by sso
  - lookup employee by sso
  - check vip by sso
  - send email
  - update ticket

Comment

1 Notification(s) - Success

1 Full Scan(s) - Success

1 Quarantine(s) - Success - Wake failed

1 Ticket(s) - Success

PINNED ITEMS (4)

It | Approvals | Reports

MANAGE WIDGETS

1 Notification(s) - Success

1 Full Scan(s) - Success

1 Quarantine(s) - Success - Wake failed

1 Ticket(s) - Success

3.0.0.0

City: Fairfield
Country: United States
State/Province: Connecticut
IP Address: 3.0.0.0

GE Imagination at work

COMPUTER NAME | DOMAIN | IP ADDRESS

incident_auto ID: 133716

GE CIRT Malicious Behavior Detected

HIGH | TLP:RED | SLA: an hour remained | Hide

Owner: Select... | Set Status: Resolved

Source ID:	0eae0280-9185-4406-922e-7aa7111f70d7	Activity Start:	2 minutes ago	Created:	2 minutes ago	Opened:	2 minutes ago	Playbooks Run:	7
Artifacts:	5	Activity End:	Ongoing	Updated:	a few seconds ago	Resolved:	a few seconds ago	Actions Run:	28

JSON | AUDIT | EXPORT | EDIT

Detection Indicator: GE CIRT Malicious Behavior Detected

Tags: autoresolve:res...

description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Tortor at risus viverra adipiscing. Ultrices dui sapien eget mi proin sed libero enim. Consequat semper viverra nam libero justo laoreet sit amet cursus. Neque sodales ut etiam sit amet nisl purus. Ultricies mi quis hendrerit dolor magna eget. Condimentum id venenatis a condimentum vitae sapien pellentesque. Viverra suspendisse potenti nullam ac tortor vitae purus. Ut ornare lectus sit amet est. Ultricies mi eget mauris pharetra et ultrices. Eu scelerisque felis imperdiet proin fermentum leo vel orci. Egestas congue quisque egestas diam in arcu cursus euismod quis.

Activity | Guidance

Timeline | HUD | Artifacts | Vault | Approvals | Reports

ACTION | PLAYBOOK | + ARTIFACT

Recent Activity — All

- gecirt_response_create_ticket_main
  - prompt
  - create incident ticket
- gecirt_response_[redacted]quarantine
  - get device info
  - check vip by sso
  - quarantine device
    1 action failed for app [redacted] (GE)[63]
  - update incident ticket

The following hosts were successfully quarantined but the agent could not be woken up. Hosts: [redacted]

- gecirt_remediation_[redacted]_full_scan
  - launch full scan
  - update incident ticket

Comment

	ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY	TAGS
	1970522	ticket:autogen	[redacted]logon.ds.ge.com - T...	0 minutes ago	0 minutes ago	LOW	None	

Name: [redacted] Ticket Details
Label: ticket:autogen
Source ID: 921422e9-b32e-407c-8753-c2ec70df265b
Start Time: 0 minutes ago
Created: 0 minutes ago
Type: ticket
Severity: low

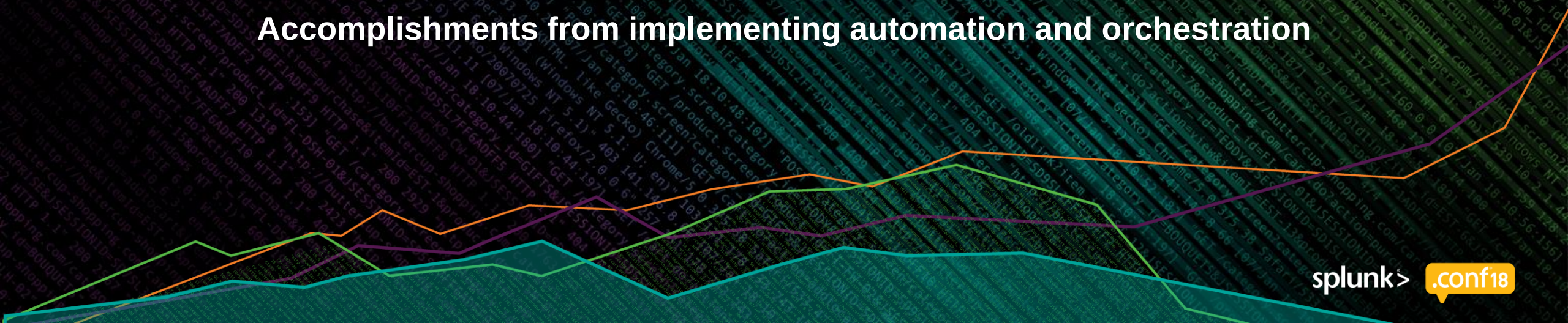
Details

deviceHostname: [redacted]
rt: 712976

	1970521	user:autogen	[redacted] - User Info	1 minutes ago	1 minutes ago	LOW	None
	1970520	device:autogen	[redacted] - D...	1 minutes ago	1 minutes ago	LOW	None
	1970519	history:autogen	[redacted] ticket history	1 minutes ago	1 minutes ago	LOW	None
	1970518	event	event	1 minutes ago	1 minutes ago	MEDIUM	Mark Cooke

Playbook Impacts

Accomplishments from implementing automation and orchestration



Playbook Impacts

Estimated hours saved per month

22 Hours

Ticket creator

30 Hours

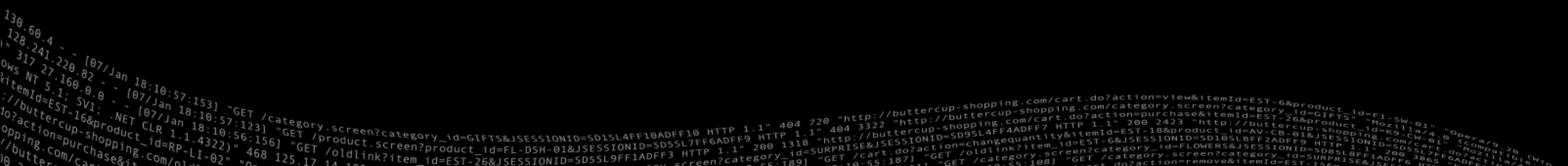
Network containment

30 Hours

Domain/IP blocks

32 Hours

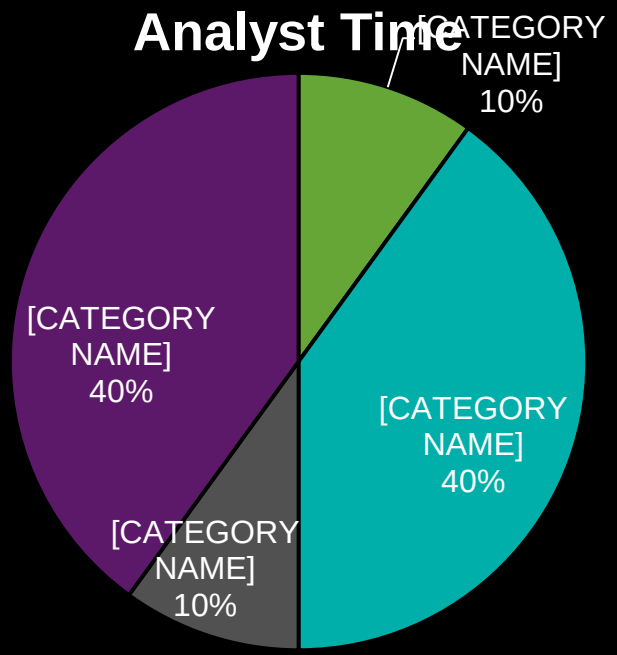
Alert history and auto categorization



Conclusion

Conclusion

Implementing automation and orchestration



By implementing automation and orchestration through Phantom we're aiming to:

- Focus analysts time on analysis
- Focus analysts time on finding threats
- Reduce risk through speed and consistency

splunk> .conf18

Thank You!

Don't forget to rate this session in the .conf18 mobile app