ESET for Enterprise

ENJOY SAFER TECHNOLOGY™

Agenda

1. Our vision for Enterprises
2. Technologies
3. Solutions
4. Summary

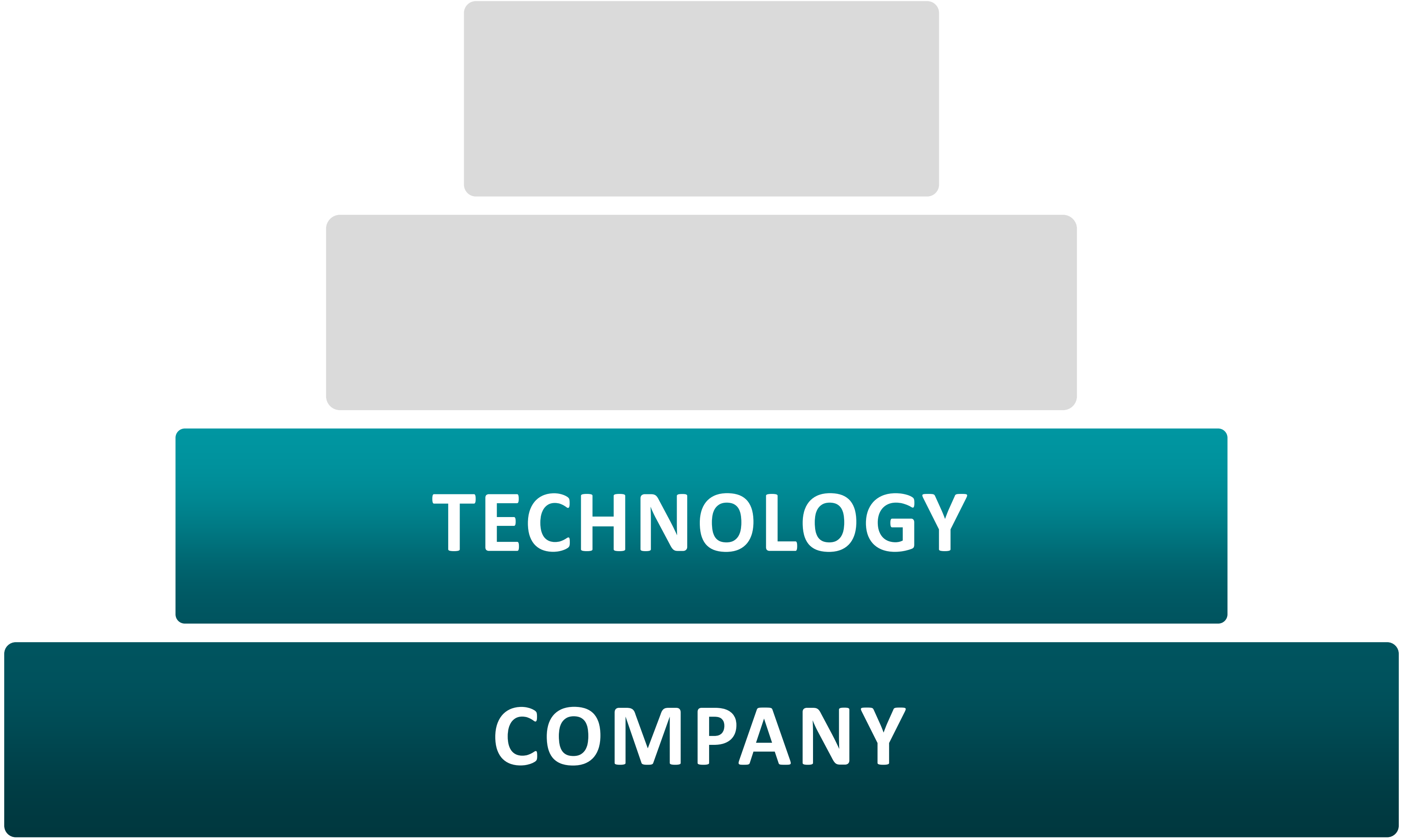
Vision for Enterprises

Be a trusted IT security partner by providing cutting edge technology and knowledge that integrates with and enables key areas of security, and by offering top quality security and professional services.

ESET Vision for Enterprises

COMPANY

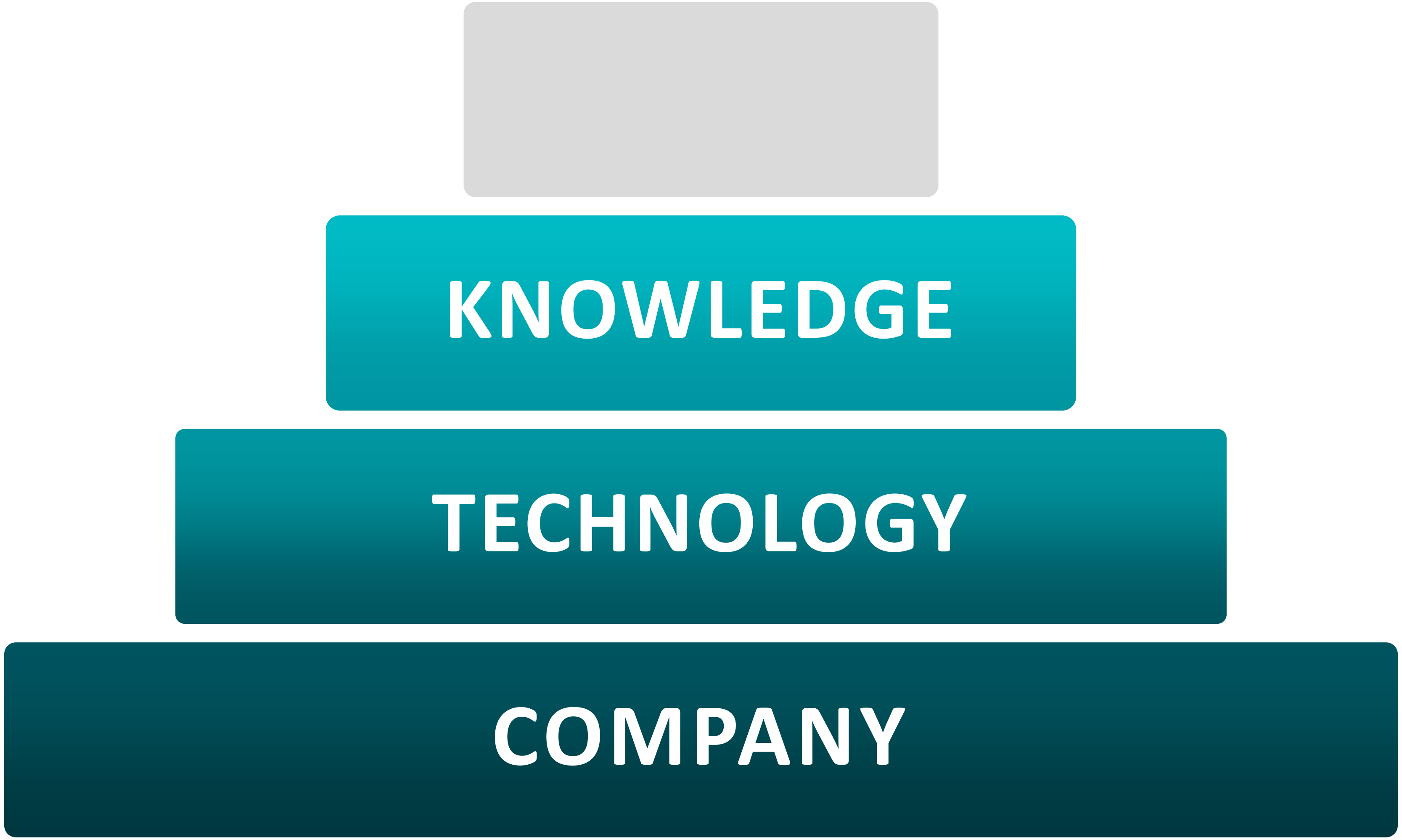
ESET Vision for Enterprises



TECHNOLOGY

COMPANY

ESET Vision for Enterprises

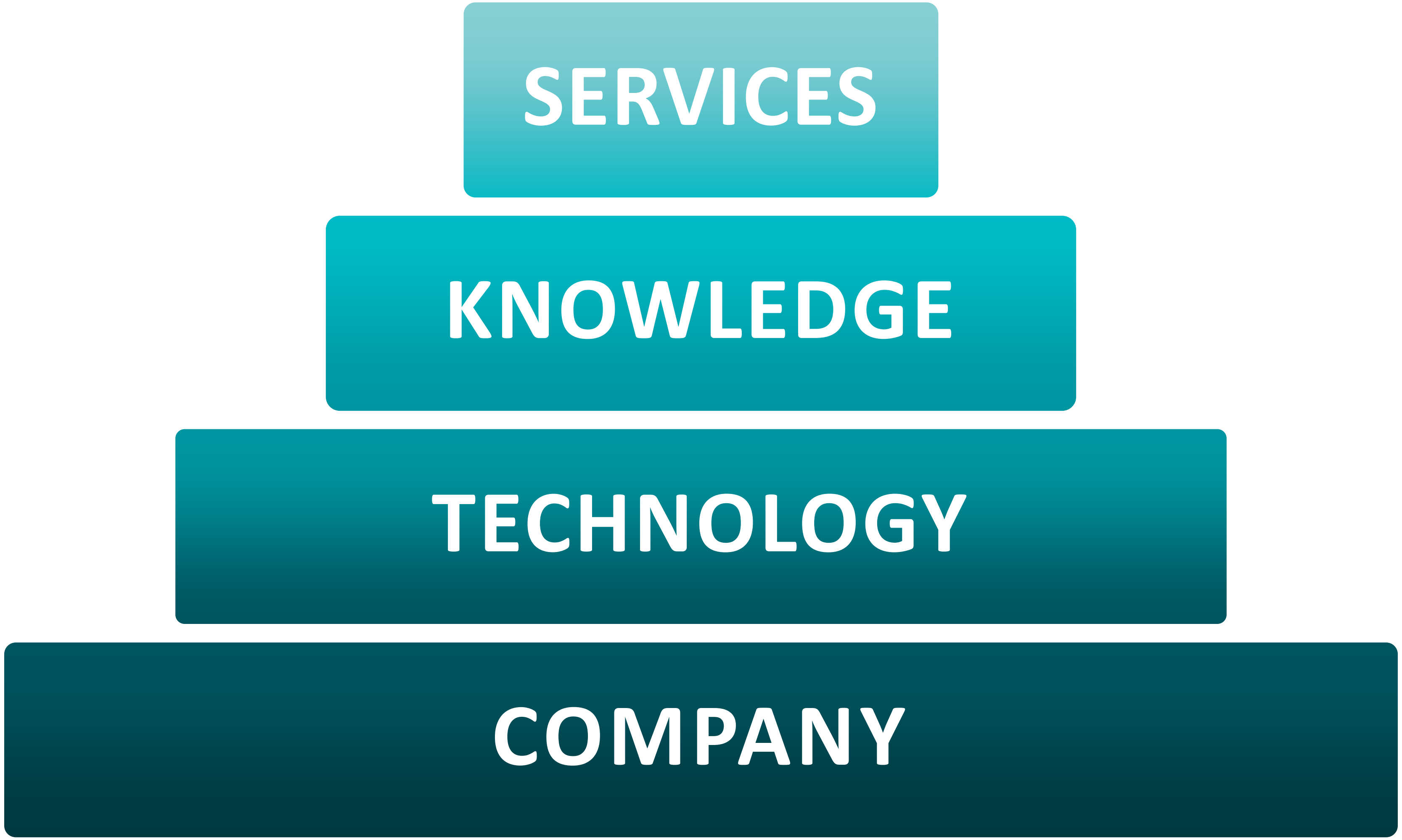


KNOWLEDGE

TECHNOLOGY

COMPANY

ESET Vision for Enterprises



SERVICES

KNOWLEDGE

TECHNOLOGY

COMPANY

Technologies

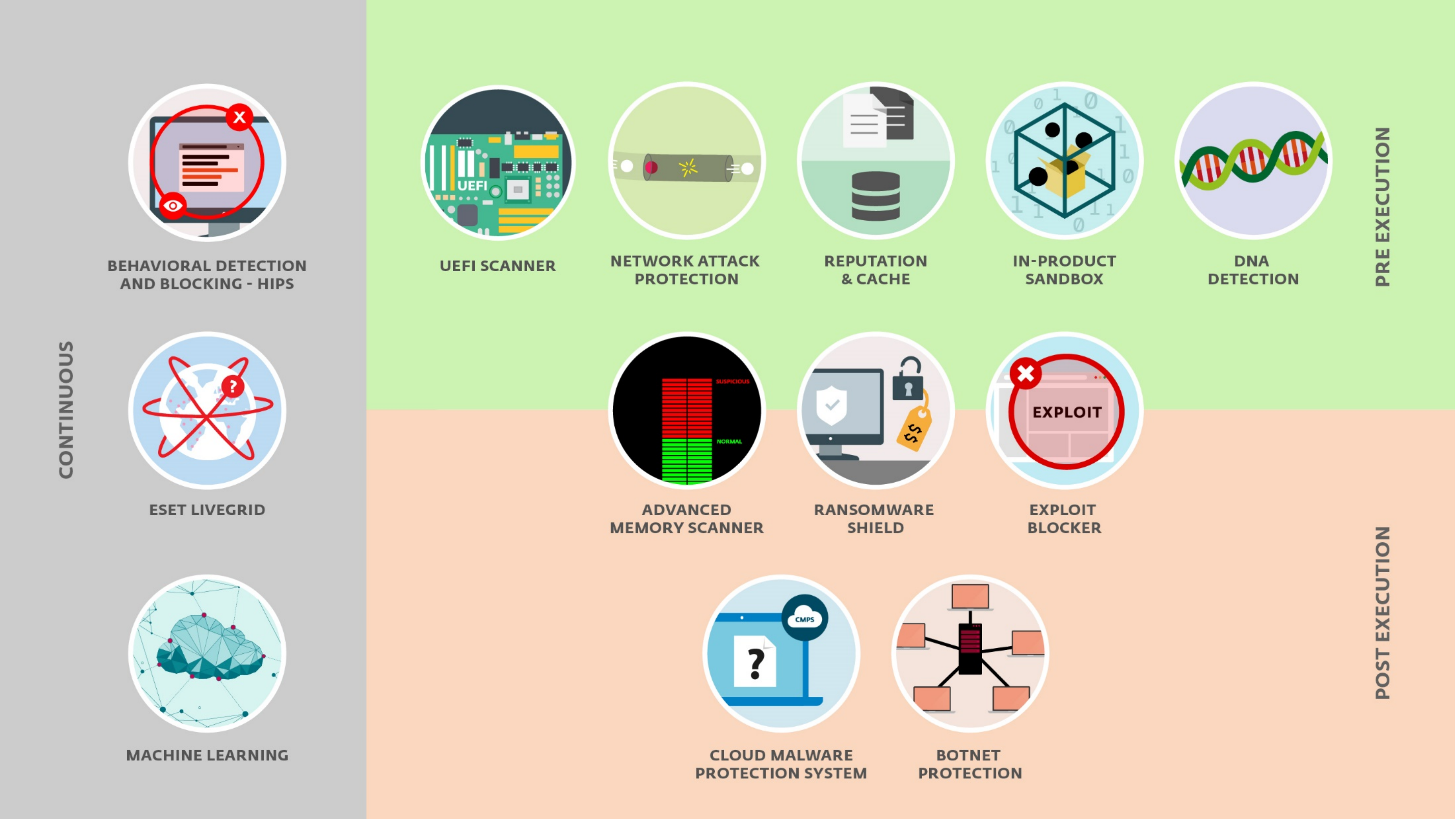
Technology principles

Reliability

High Detection

Low Performance Impact

Ease of Use



CONTINUOUS

BEHAVIORAL DETECTION AND BLOCKING - HIPS

ESET LIVEGRID

MACHINE LEARNING

PRE EXECUTION

UEFI SCANNER

NETWORK ATTACK PROTECTION

REPUTATION & CACHE

IN-PRODUCT SANDBOX

DNA DETECTION

POST EXECUTION

ADVANCED MEMORY SCANNER

RANSOMWARE SHIELD

EXPLOIT BLOCKER

CLOUD MALWARE PROTECTION SYSTEM

BOTNET PROTECTION

Base for new Enterprise Products

ESET
LiveGrid

Machine
Learning

Human
Expertise

Solutions

BUSINESS SEGMENT

SMB

Enterprise

Adaptive Security Architecture

POLICY

PREDICT

Risk-prioritized exposure assesment

Anticipate threats / attacks

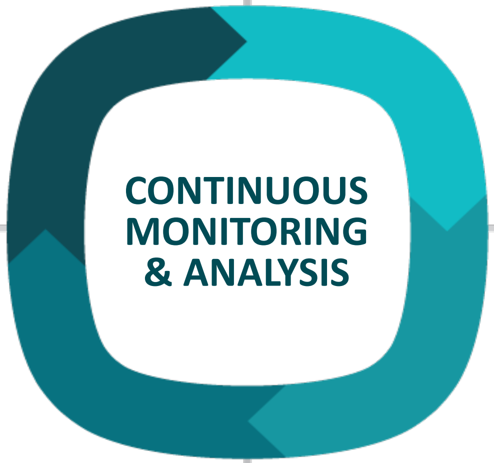
Baseline systems and security posture

PREVENT

Harden Systems

Isolate Systems

Prevent Attacks



CONTINUOUS MONITORING & ANALYSIS

RESPOND

Remediate

Design / Model policy change

Investigate incidents / retrospective analysis

DETECT

Detect Incidents

Confirm and prioritize risk

Contain Incidents

COMPLIANCE

How ESET fits in Adaptive Security Architecture

POLICY

PREDICT

ESET Threat Intelligence

ESET Virus Radar

WeLive Security

PREVENT

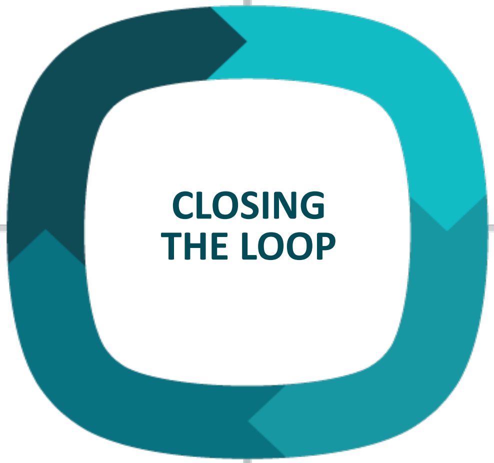
ESET Endpoint Security

ESET Virtualization Security

ESET Security Management Center

ESET Secure Authentication

ESET Endpoint Encryption



RESPOND

ESET Security Management Center

NEW ESET Enterprise Inspector

NEW ESET Dynamic Threat Defense

DETECT

ESET Endpoint Security

ESET Security Management Center

ESET Enterprise Inspector NEW

ESET Dynamic Threat Defense NEW

COMPLIANCE

eset® THREAT INTELLIGENCE

Problem: not enough context over data

- Organizations seek multi-layered defenses
- Second pair of eyes, with vendor with local presence is always good
- Multiple layers are more efficient

How does it work?

- Shares ESET’s actionable threat intelligence with customers
- Early Warning System
- Exposes/predicts next steps of attackers
- Provides IOCs (IP, URL, file hash…)
- Automated Malware Analysis portal
- Incident Response Management via SOCs
- Also available to users who are not ESET customers

ESET Threat Intelligence offers 3 different tiers

Use Case	Tier
“Found a suspicious sample (file/code). Is it a targeted attack?”	Automated Sample Analysis

NEW

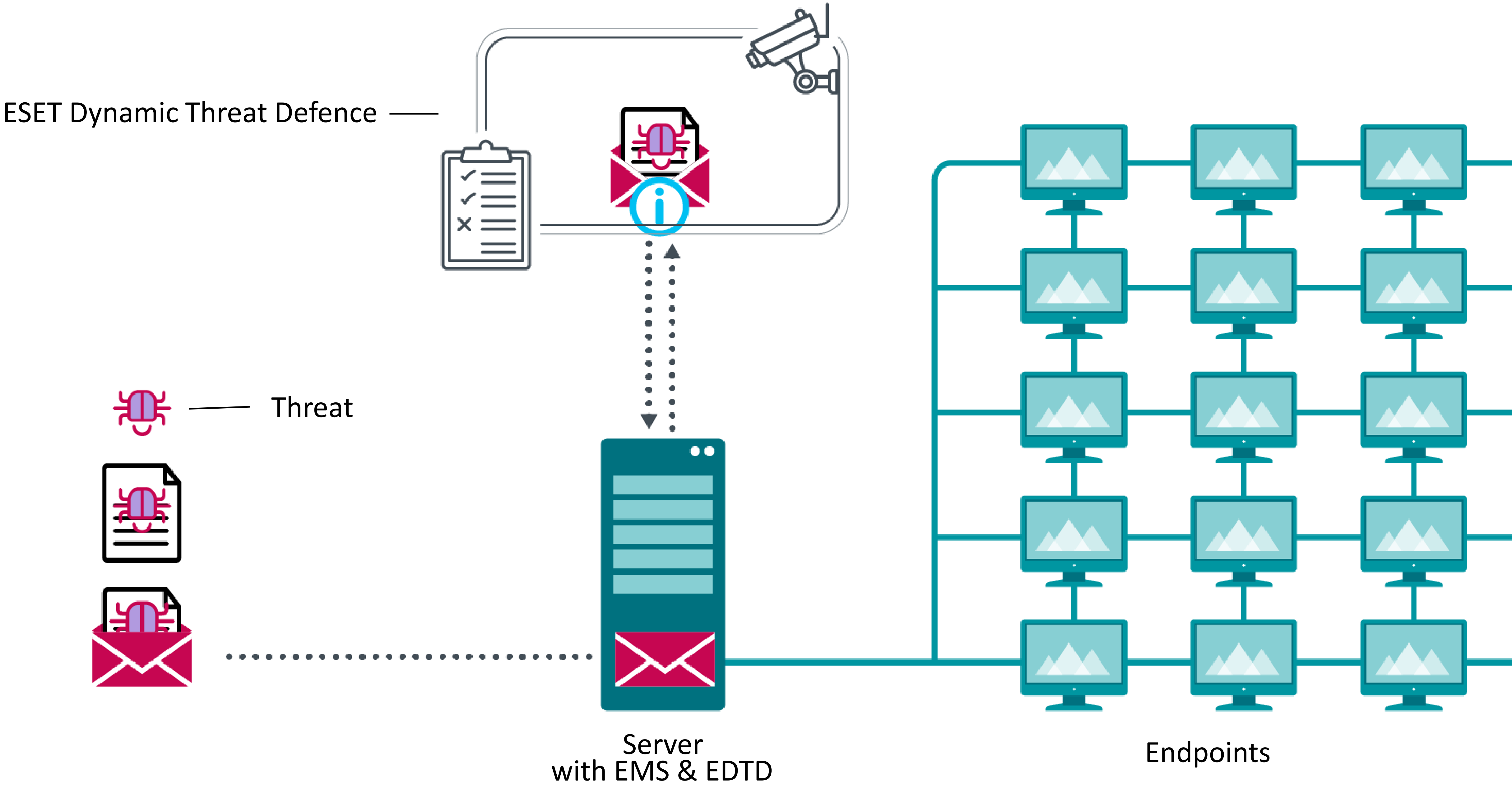
ESET DYNAMIC THREAT DEFENSE

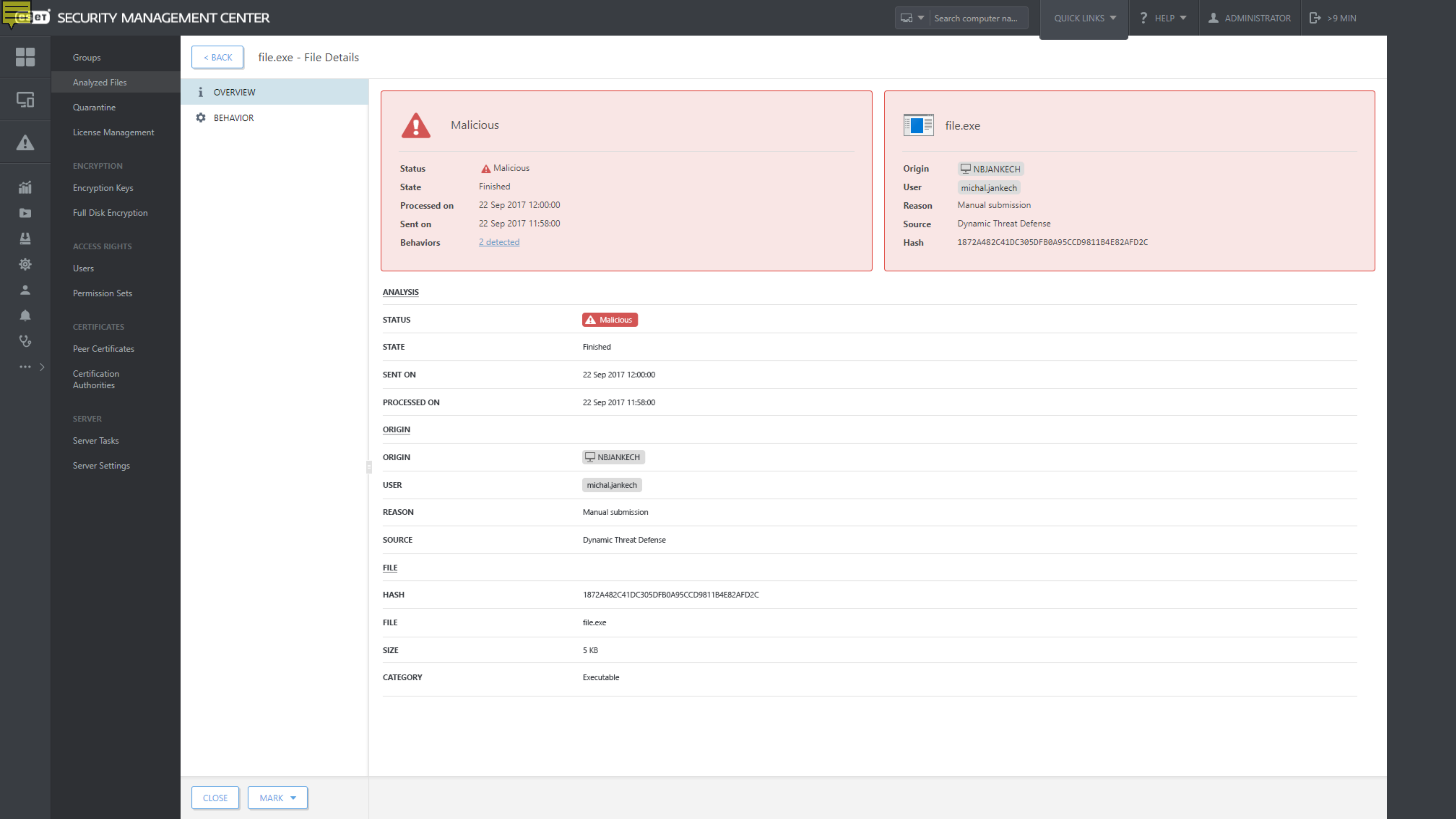
Problem: Ransomware

- E-mail is still used as a common delivery method
- Conventional antispam is not effective
- Multiple layers are more efficient

Key features

1. ESET LiveGrid® Visibility
2. Advanced & Dynamic Threat Analysis
3. Detailed results of Submission / Analysis
4. Affects detections on Endpoints
5. Integrates with Enterprise Inspector
6. Adds another manageable layer of protection to ESET Endpoint & Server security products


ESET Dynamic Threat Defence
Threat
Server
with EMS & EDTD
Endpoints



file.exe - File Details

Malicious

Status	Malicious
State	Finished
Processed on	22 Sep 2017 12:00:00
Sent on	22 Sep 2017 11:58:00
Behaviors	2 detected

file.exe

Origin	NBJANKECH
User	michal.jankech
Reason	Manual submission
Source	Dynamic Threat Defense
Hash	1872A482C41DC305DFB0A95CCD9811B4E82AFD2C

ANALYSIS

STATUS	Malicious
STATE	Finished
SENT ON	22 Sep 2017 12:00:00
PROCESSED ON	22 Sep 2017 11:58:00

ORIGIN

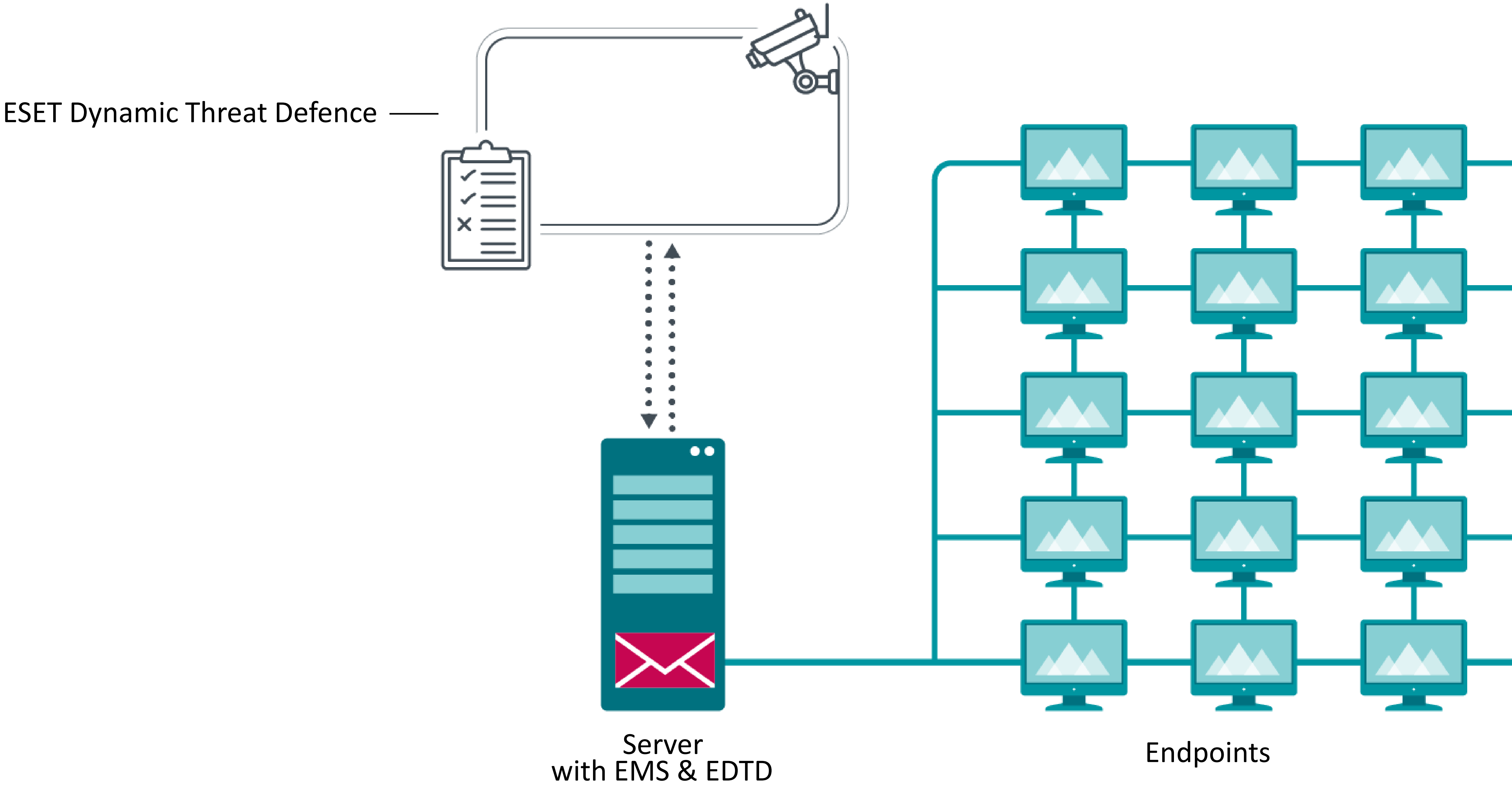
ORIGIN	NBJANKECH
USER	michal.jankech
REASON	Manual submission
SOURCE	Dynamic Threat Defense

FILE

HASH	1872A482C41DC305DFB0A95CCD9811B4E82AFD2C
FILE	file.exe
SIZE	5 KB
CATEGORY	Executable

NEW

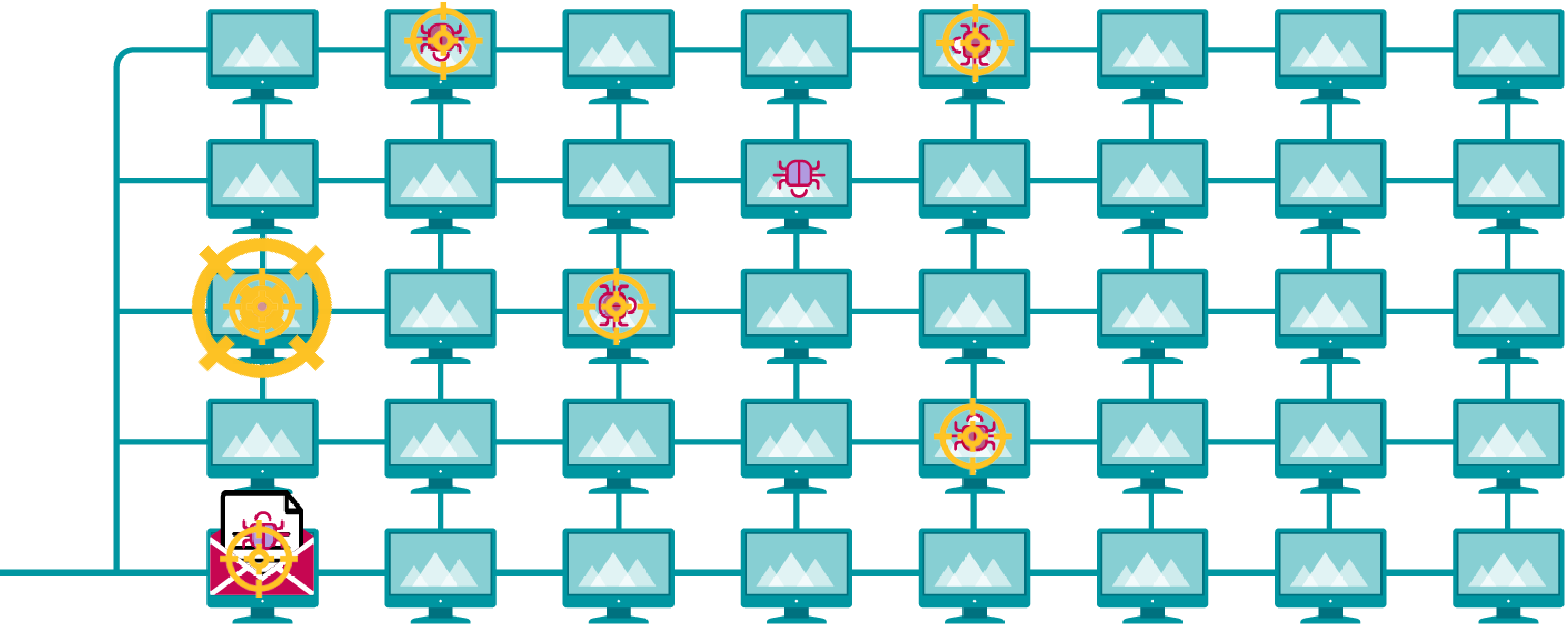
ESET ENTERPRISE INSPECTOR



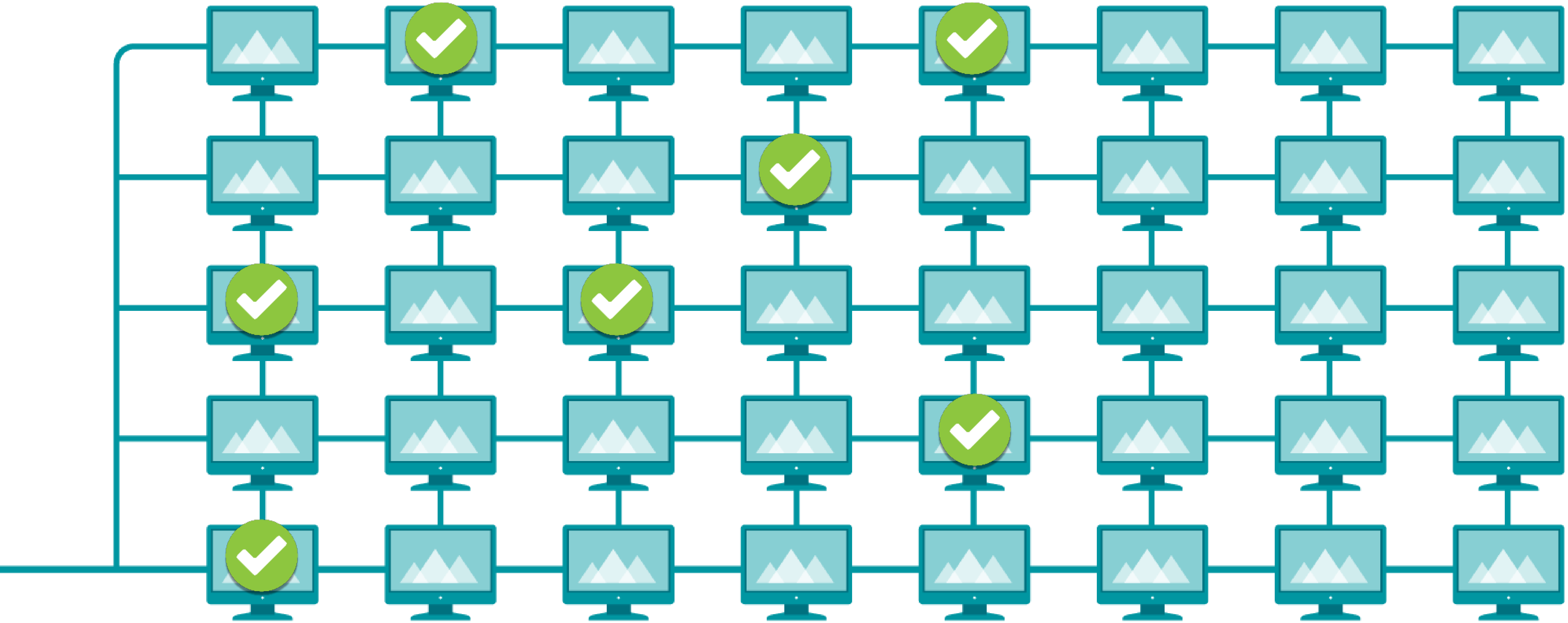
ESET Dynamic Threat Defence

Server
with EMS & EDTD

Endpoints



Endpoints



Endpoints

Problem: Targeted attacks & APTs

- Threats are modified to evade detection
- Dwell time until detection is long
- Attackers don’t just use executable files

Solution for targeted attacks & APTs

Detection

Find malicious anomaly

Visibility

What is affected?
When did it happen?
How did it happen?

Response

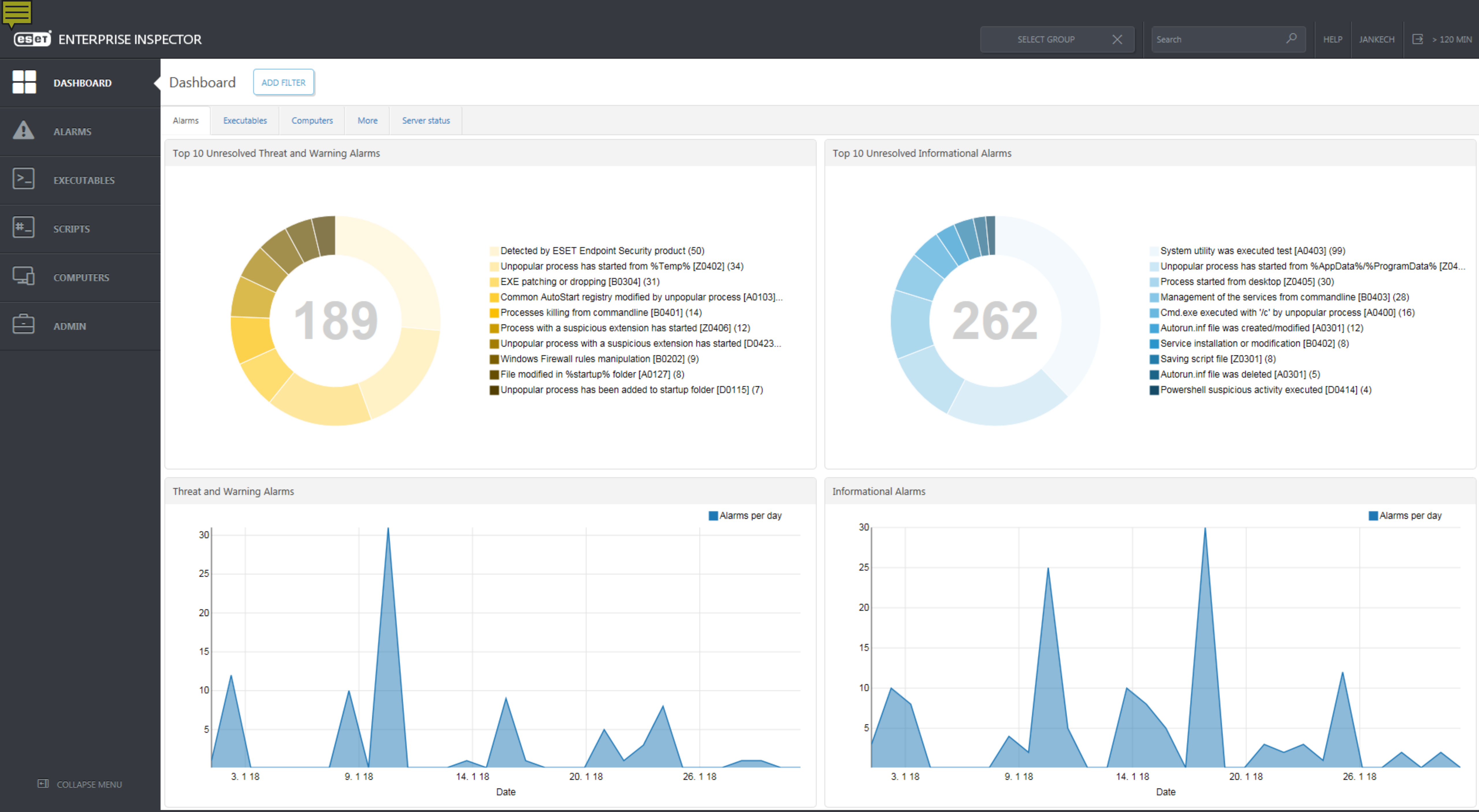
Block it
Remove it

How does it work?

- Collects real-time events
- Provides extensive filtering and sorting
- Uses ESET reputation systems
- Gives customers the ability to create their own notification rules
- Offers blocking and remediation

	Other EDR solutions	ESET Enterprise Inspector
Ease of use	Hard	Easy – focuses on the workflow

	Other EDR solutions	ESET Enterprise Inspector
Openess	The same detection methods for all the assets and users	Ability to adjust detection for different assets in the company



Top 10 Unresolved Threat and Warning Alarms

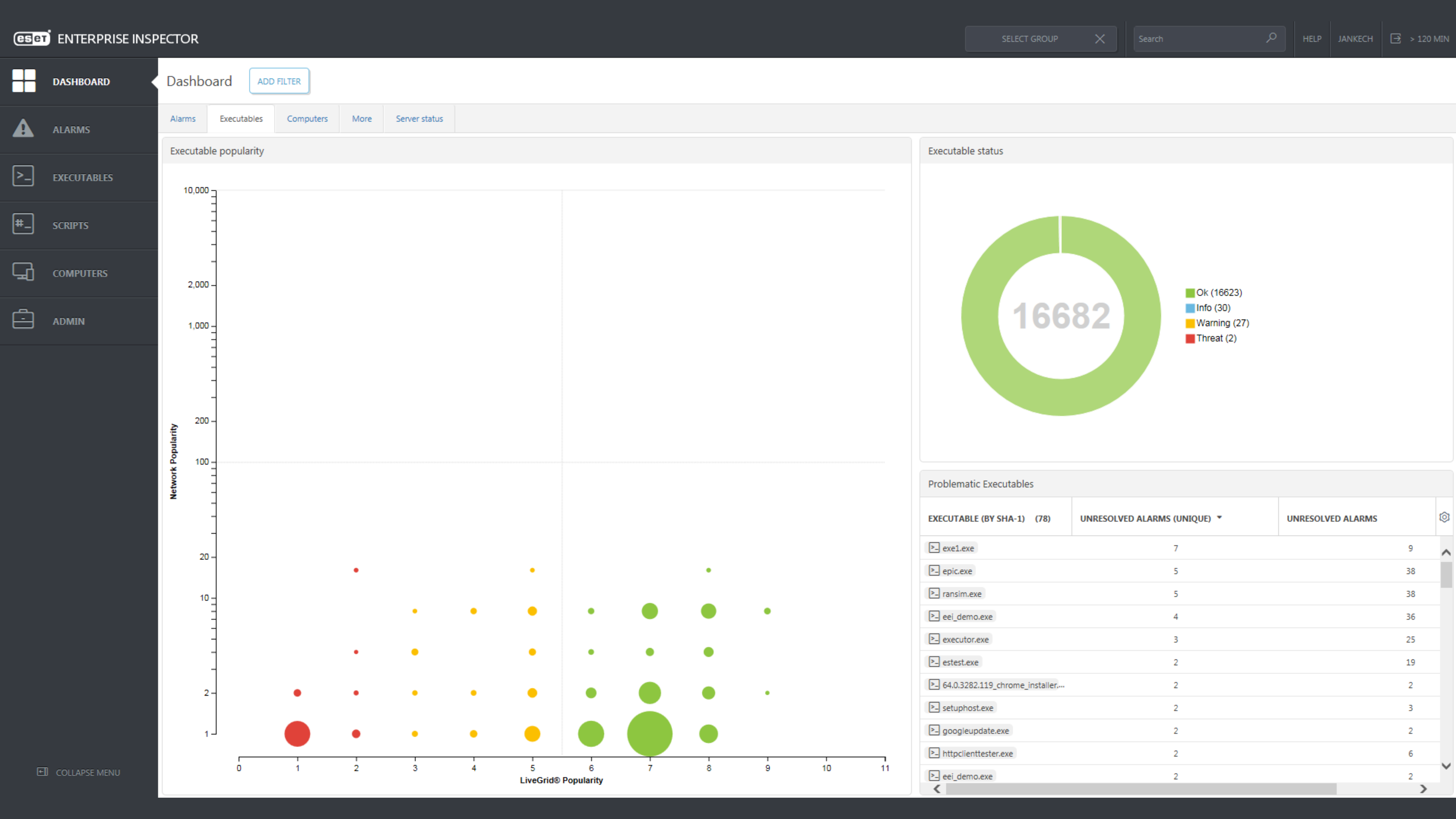
- Detected by ESET Endpoint Security product (50)
- Unpopular process has started from %Temp% [Z0402] (34)
- EXE patching or dropping [B0304] (31)
- Common AutoStart registry modified by unpopular process [A0103]...
- Processes killing from commandline [B0401] (14)
- Process with a suspicious extension has started [Z0406] (12)
- Unpopular process with a suspicious extension has started [D0423...
- Windows Firewall rules manipulation [B0202] (9)
- File modified in %startup% folder [A0127] (8)
- Unpopular process has been added to startup folder [D0115] (7)

Top 10 Unresolved Informational Alarms

- System utility was executed test [A0403] (99)
- Unpopular process has started from %AppData%/%ProgramData% [Z04...
- Process started from desktop [Z0405] (30)
- Management of the services from commandline [B0403] (28)
- Cmd.exe executed with '/c' by unpopular process [A0400] (16)
- Autorun.inf file was created/modified [A0301] (12)
- Service installation or modification [B0402] (8)
- Saving script file [Z0301] (8)
- Autorun.inf file was deleted [A0301] (5)
- Powershell suspicious activity executed [D0414] (4)

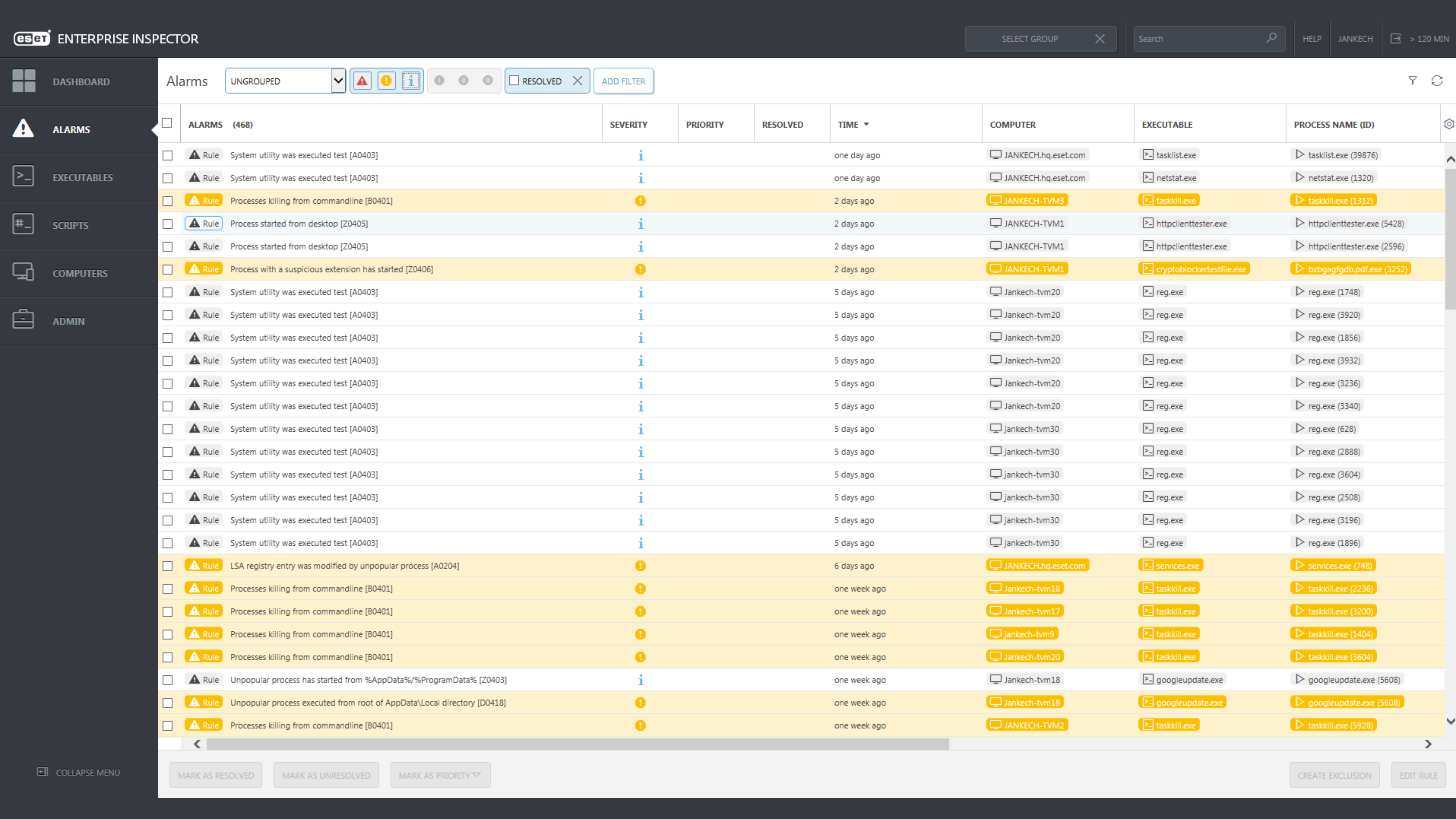
Threat and Warning Alarms

Informational Alarms

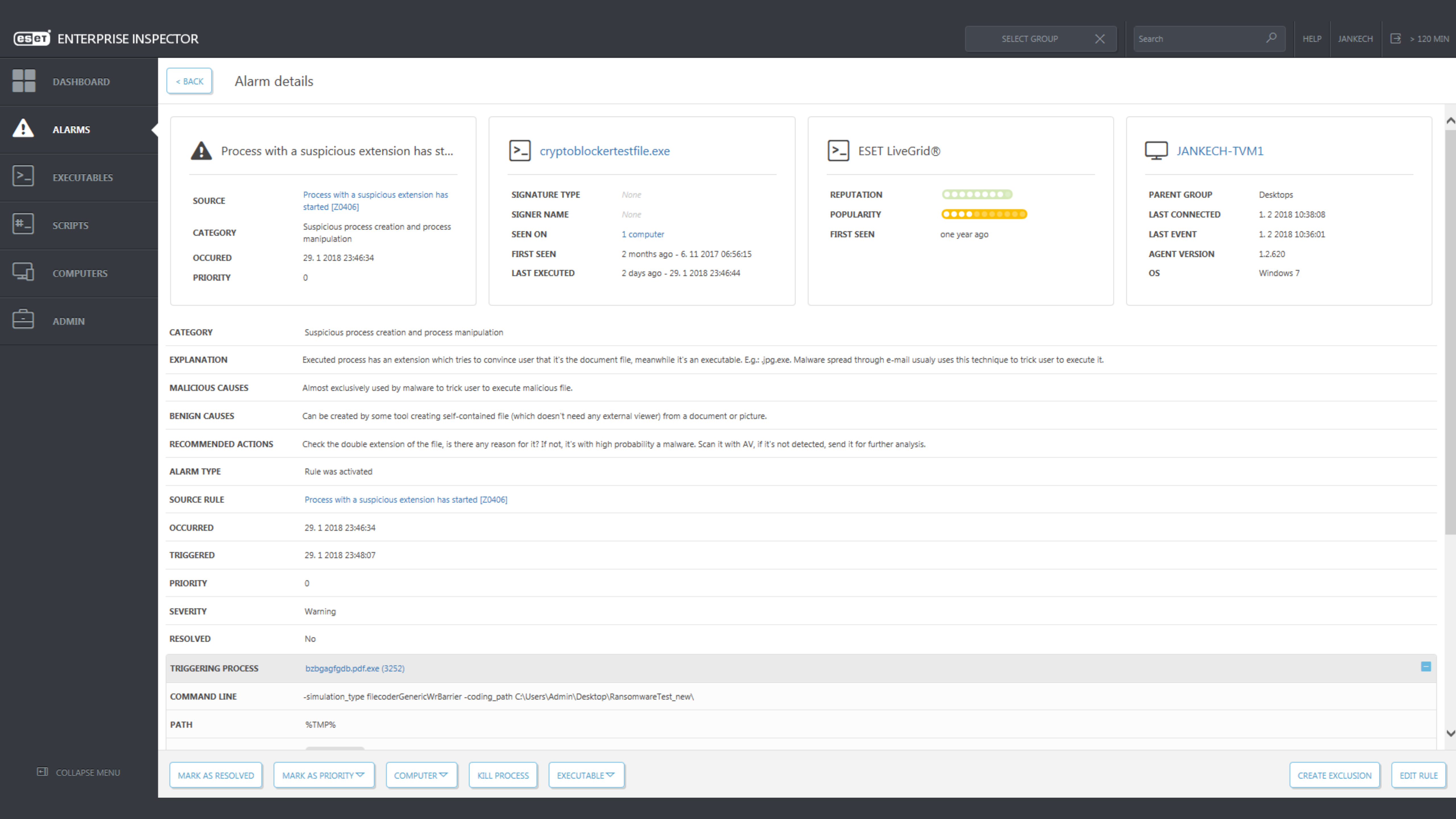


Problematic Executables

EXECUTABLE (BY SHA-1) (78)	UNRESOLVED ALARMS (UNIQUE)	UNRESOLVED ALARMS
exe1.exe	7	9
epic.exe	5	38
ransim.exe	5	38
eei_demo.exe	4	36
executor.exe	3	25
estest.exe	2	19
64.0.3282.119_chrome_installer....	2	2
setuphost.exe	2	3
googleupdate.exe	2	2
httpclienttester.exe	2	6
eei_demo.exe	2	2



□	ALARMS (468)	SEVERITY	PRIORITY	RESOLVED	TIME	COMPUTER	EXECUTABLE	PROCESS NAME (ID)
□	Rule System utility was executed test [A0403]	i			one day ago	JANKECH.hq.eset.com	tasklist.exe	tasklist.exe (39876)
□	Rule System utility was executed test [A0403]	i			one day ago	JANKECH.hq.eset.com	netstat.exe	netstat.exe (1320)
□	Rule Processes killing from commandline [B0401]	!			2 days ago	JANKECH-TVM3	taskkill.exe	taskkill.exe (1312)
□	Rule Process started from desktop [Z0405]	i			2 days ago	JANKECH-TVM1	httpclienttester.exe	httpclienttester.exe (5428)
□	Rule Process started from desktop [Z0405]	i			2 days ago	JANKECH-TVM1	httpclienttester.exe	httpclienttester.exe (2596)
□	Rule Process with a suspicious extension has started [Z0406]	!			2 days ago	JANKECH-TVM1	cryptoblockertestfile.exe	bzbgagfgdb.pdf.exe (3252)
□	Rule System utility was executed test [A0403]	i			5 days ago	Jankech-tvm20	reg.exe	reg.exe (1748)
□	Rule System utility was executed test [A0403]	i			5 days ago	Jankech-tvm20	reg.exe	reg.exe (3920)
□	Rule System utility was executed test [A0403]	i			5 days ago	Jankech-tvm20	reg.exe	reg.exe (1856)
□	Rule System utility was executed test [A0403]	i			5 days ago	Jankech-tvm20	reg.exe	reg.exe (3932)
□	Rule System utility was executed test [A0403]	i			5 days ago	Jankech-tvm20	reg.exe	reg.exe (3236)
□	Rule System utility was executed test [A0403]	i			5 days ago	Jankech-tvm20	reg.exe	reg.exe (3340)
□	Rule System utility was executed test [A0403]	i			5 days ago	jankech-tvm30	reg.exe	reg.exe (628)
□	Rule System utility was executed test [A0403]	i			5 days ago	jankech-tvm30	reg.exe	reg.exe (2888)
□	Rule System utility was executed test [A0403]	i			5 days ago	jankech-tvm30	reg.exe	reg.exe (3604)
□	Rule System utility was executed test [A0403]	i			5 days ago	jankech-tvm30	reg.exe	reg.exe (2508)
□	Rule System utility was executed test [A0403]	i			5 days ago	jankech-tvm30	reg.exe	reg.exe (3196)
□	Rule System utility was executed test [A0403]	i			5 days ago	jankech-tvm30	reg.exe	reg.exe (1896)
□	Rule LSA registry entry was modified by unpopular process [A0204]	!			6 days ago	JANKECH.hq.eset.com	services.exe	services.exe (748)
□	Rule Processes killing from commandline [B0401]	!			one week ago	Jankech-tvm18	taskkill.exe	taskkill.exe (2236)
□	Rule Processes killing from commandline [B0401]	!			one week ago	Jankech-tvm17	taskkill.exe	taskkill.exe (3200)
□	Rule Processes killing from commandline [B0401]	!			one week ago	jankech-tvm9	taskkill.exe	taskkill.exe (1404)
□	Rule Processes killing from commandline [B0401]	!			one week ago	Jankech-tvm20	taskkill.exe	taskkill.exe (3604)
□	Rule Unpopular process has started from %AppData%/%ProgramData% [Z0403]	i			one week ago	Jankech-tvm18	googleupdate.exe	googleupdate.exe (5608)
□	Rule Unpopular process executed from root of AppData\Local directory [D0418]	!			one week ago	Jankech-tvm18	googleupdate.exe	googleupdate.exe (5608)
□	Rule Processes killing from commandline [B0401]	!			one week ago	JANKECH-TVM2	taskkill.exe	taskkill.exe (5928)



Alarm details

Process with a suspicious extension has st...

SOURCE	Process with a suspicious extension has started [Z0406]
CATEGORY	Suspicious process creation and process manipulation
OCCURED	29. 1 2018 23:46:34
PRIORITY	0

cryptoblockertestfile.exe

SIGNATURE TYPE	None
SIGNER NAME	None
SEEN ON	1 computer
FIRST SEEN	2 months ago - 6. 11 2017 06:56:15
LAST EXECUTED	2 days ago - 29. 1 2018 23:46:44

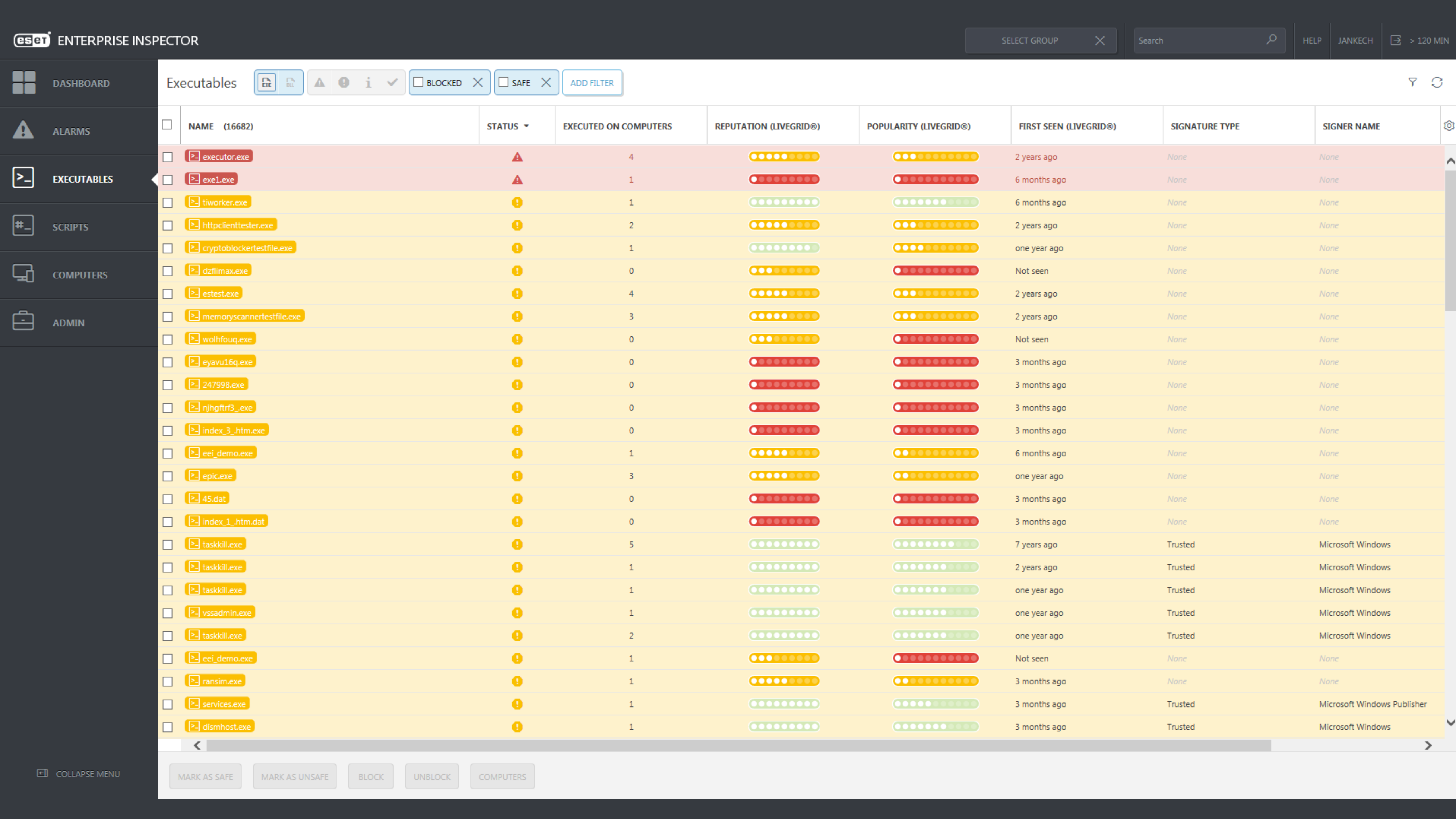
ESET LiveGrid®

REPUTATION	
POPULARITY	
FIRST SEEN	one year ago

JANKECH-TVM1

PARENT GROUP	Desktops
LAST CONNECTED	1. 2 2018 10:38:08
LAST EVENT	1. 2 2018 10:36:01
AGENT VERSION	1.2.620
OS	Windows 7

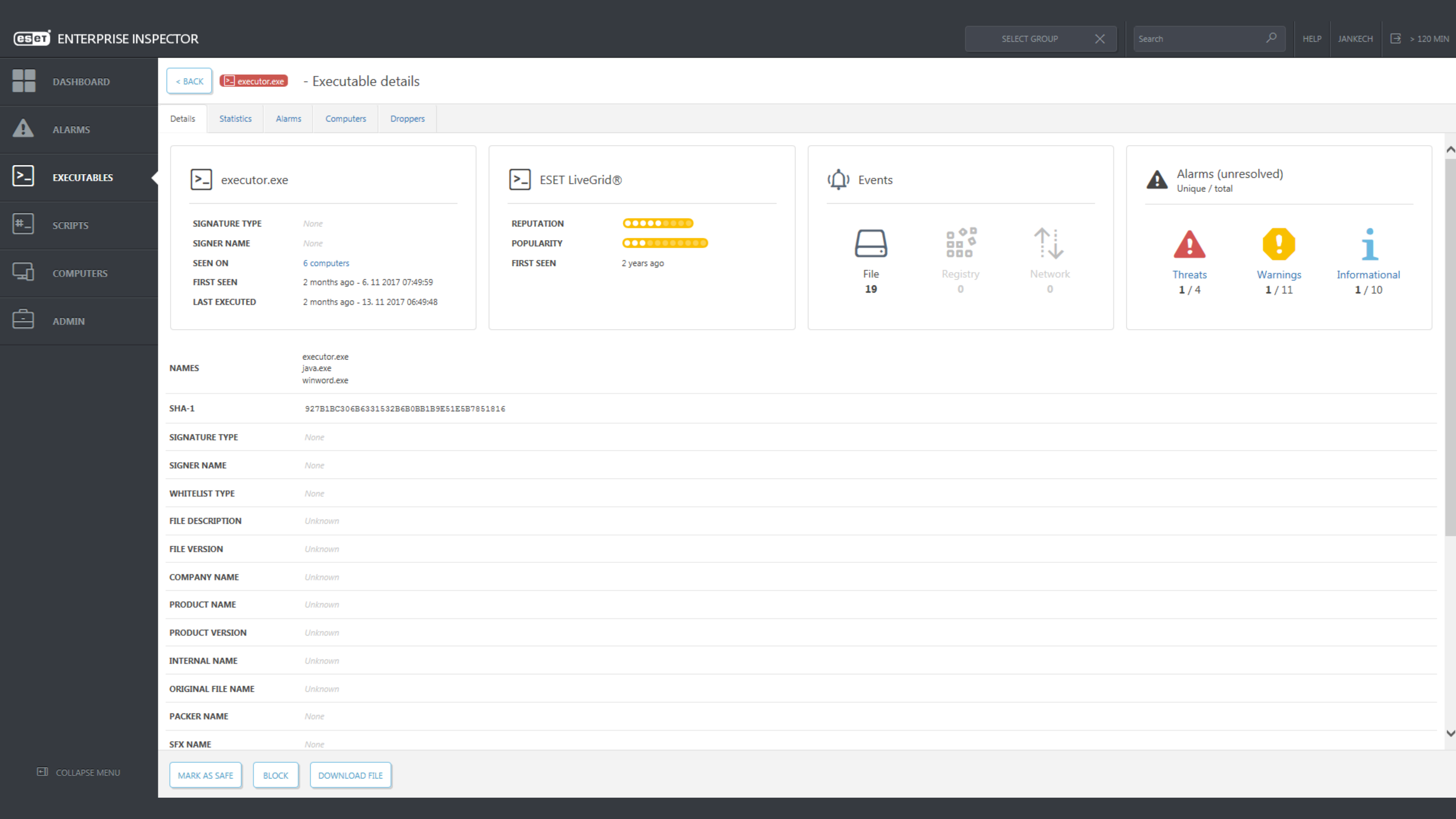
CATEGORY	Suspicious process creation and process manipulation
EXPLANATION	Executed process has an extension which tries to convince user that it's the document file, meanwhile it's an executable. E.g.: .jpg.exe. Malware spread through e-mail usualy uses this technique to trick user to execute it.
MALICIOUS CAUSES	Almost exclusively used by malware to trick user to execute malicious file.
BENIGN CAUSES	Can be created by some tool creating self-contained file (which doesn't need any external viewer) from a document or picture.
RECOMMENDED ACTIONS	Check the double extension of the file, is there any reason for it? If not, it's with high probability a malware. Scan it with AV, if it's not detected, send it for further analysis.
ALARM TYPE	Rule was activated
SOURCE RULE	Process with a suspicious extension has started [Z0406]
OCCURRED	29. 1 2018 23:46:34
TRIGGERED	29. 1 2018 23:48:07
PRIORITY	0
SEVERITY	Warning
RESOLVED	No
TRIGGERING PROCESS	bzbgagfgdb.pdf.exe (3252)
COMMAND LINE	-simulation_type filecoderGenericWrBarrier -coding_path C:\Users\Admin\Desktop\RansomwareTest_new\
PATH	%TMP%



Executables

□ BLOCKED ✕ □ SAFE ✕ ADD FILTER

NAME (16682)	STATUS	EXECUTED ON COMPUTERS	REPUTATION (LIVEGRID®)	POPULARITY (LIVEGRID®)	FIRST SEEN (LIVEGRID®)	SIGNATURE TYPE	SIGNER NAME
executor.exe	▲	4			2 years ago	None	None
exe1.exe	▲	1			6 months ago	None	None
tiworker.exe	!	1			6 months ago	None	None
httpclienttester.exe	!	2			2 years ago	None	None
cryptoblockertestfile.exe	!	1			one year ago	None	None
dzflimax.exe	!	0			Not seen	None	None
estest.exe	!	4			2 years ago	None	None
memoryscannertestfile.exe	!	3			2 years ago	None	None
wolhfouq.exe	!	0			Not seen	None	None
eyavu16q.exe	!	0			3 months ago	None	None
247998.exe	!	0			3 months ago	None	None
njhgftrf3_.exe	!	0			3 months ago	None	None
index_3_.htm.exe	!	0			3 months ago	None	None
eei_demo.exe	!	1			6 months ago	None	None
epic.exe	!	3			one year ago	None	None
45.dat	!	0			3 months ago	None	None
index_1_.htm.dat	!	0			3 months ago	None	None
taskkill.exe	!	5			7 years ago	Trusted	Microsoft Windows
taskkill.exe	!	1			2 years ago	Trusted	Microsoft Windows
taskkill.exe	!	1			one year ago	Trusted	Microsoft Windows
vssadmin.exe	!	1			one year ago	Trusted	Microsoft Windows
taskkill.exe	!	2			one year ago	Trusted	Microsoft Windows
eei_demo.exe	!	1			Not seen	None	None
ransim.exe	!	1			3 months ago	None	None
services.exe	!	1			3 months ago	Trusted	Microsoft Windows Publisher
dismhost.exe	!	1			3 months ago	Trusted	Microsoft Windows



executor.exe - Executable details

executor.exe

SIGNATURE TYPE	None
SIGNER NAME	None
SEEN ON	6 computers
FIRST SEEN	2 months ago - 6. 11 2017 07:49:59
LAST EXECUTED	2 months ago - 13. 11 2017 06:49:48

ESET LiveGrid®

REPUTATION	●●●●●○○○○
POPULARITY	●●●○○○○○○○○
FIRST SEEN	2 years ago

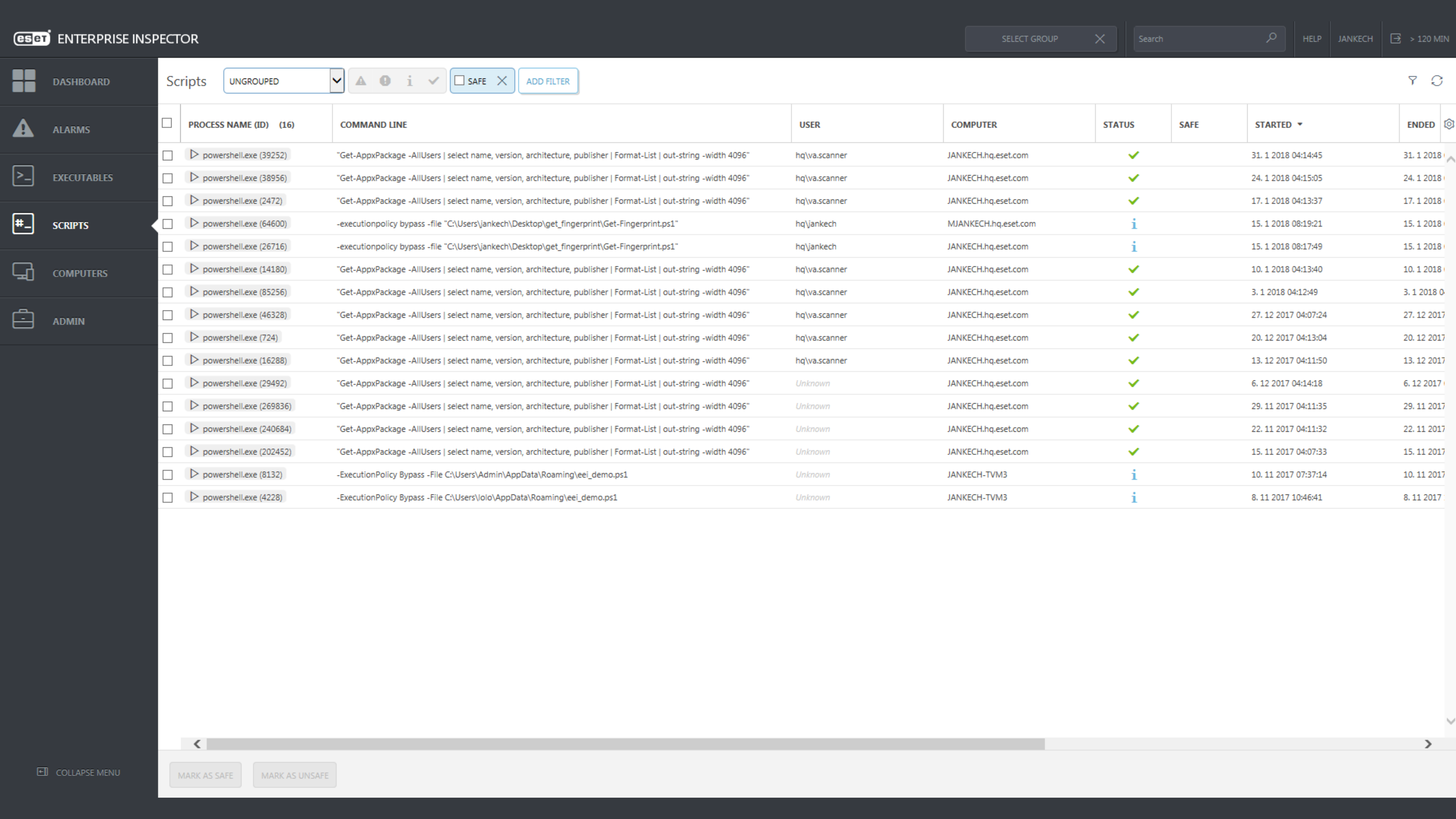
Events

File	Registry	Network
19	0	0

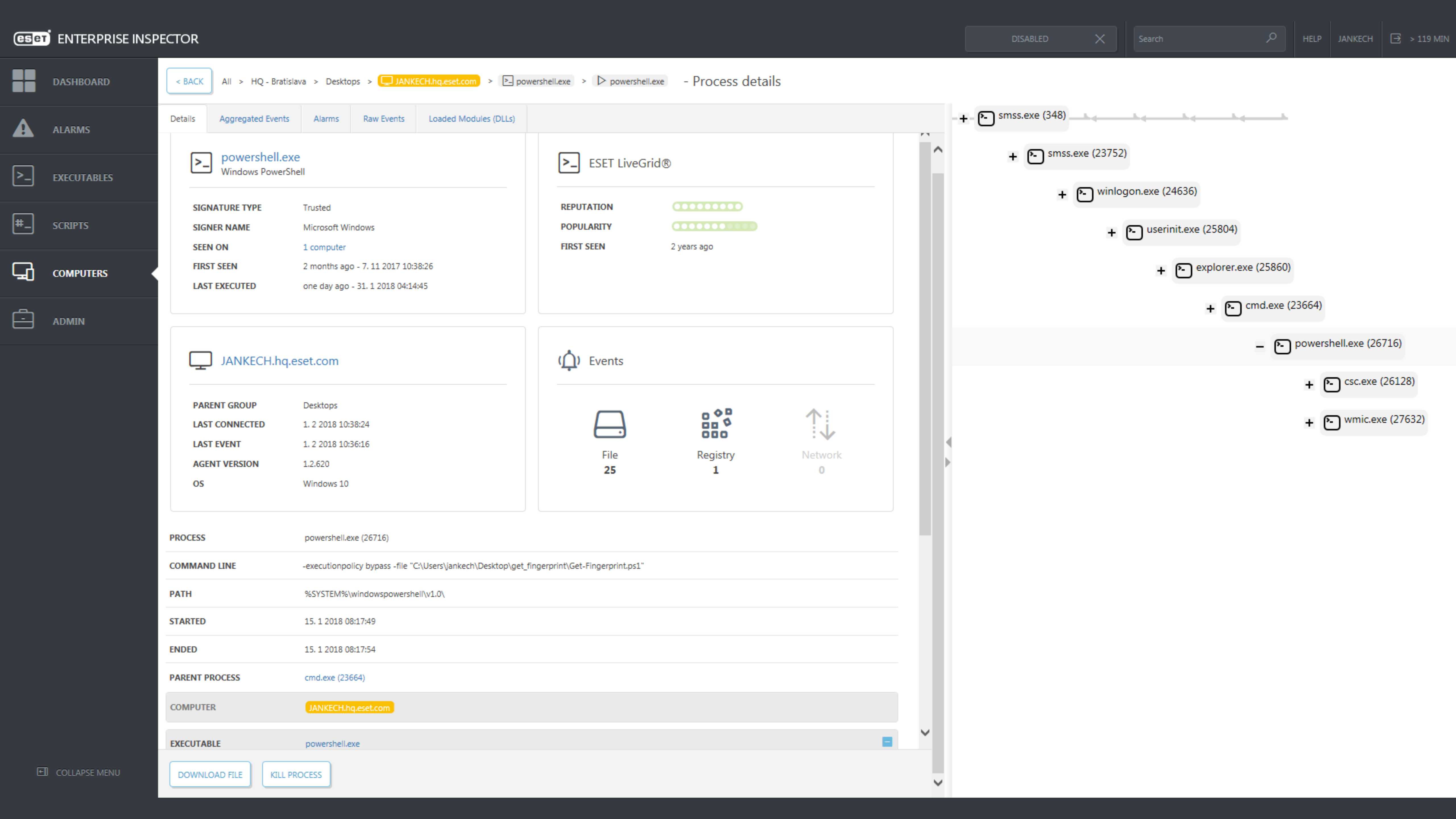
Alarms (unresolved)
Unique / total

Threats	Warnings	Informational
1 / 4	1 / 11	1 / 10

NAMES	executor.exe java.exe winword.exe
SHA-1	927B1BC306B6331532B6B0BB1B9E51E5B7851816
SIGNATURE TYPE	None
SIGNER NAME	None
WHITELIST TYPE	None
FILE DESCRIPTION	Unknown
FILE VERSION	Unknown
COMPANY NAME	Unknown
PRODUCT NAME	Unknown
PRODUCT VERSION	Unknown
INTERNAL NAME	Unknown
ORIGINAL FILE NAME	Unknown
PACKER NAME	None
SFX NAME	None



□	PROCESS NAME (ID) (16)	COMMAND LINE	USER	COMPUTER	STATUS	SAFE	STARTED	ENDED
□	powershell.exe (39252)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	hq\va.scanner	JANKECH.hq.eset.com	✓		31. 1 2018 04:14:45	31. 1 2018
□	powershell.exe (38956)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	hq\va.scanner	JANKECH.hq.eset.com	✓		24. 1 2018 04:15:05	24. 1 2018
□	powershell.exe (2472)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	hq\va.scanner	JANKECH.hq.eset.com	✓		17. 1 2018 04:13:37	17. 1 2018
□	powershell.exe (64600)	-executionpolicy bypass -file "C:\Users\jankech\Desktop\get_fingerprint\Get-Fingerprint.ps1"	hq\jankech	MJANKECH.hq.eset.com	i		15. 1 2018 08:19:21	15. 1 2018
□	powershell.exe (26716)	-executionpolicy bypass -file "C:\Users\jankech\Desktop\get_fingerprint\Get-Fingerprint.ps1"	hq\jankech	JANKECH.hq.eset.com	i		15. 1 2018 08:17:49	15. 1 2018
□	powershell.exe (14180)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	hq\va.scanner	JANKECH.hq.eset.com	✓		10. 1 2018 04:13:40	10. 1 2018
□	powershell.exe (85256)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	hq\va.scanner	JANKECH.hq.eset.com	✓		3. 1 2018 04:12:49	3. 1 2018 0
□	powershell.exe (46328)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	hq\va.scanner	JANKECH.hq.eset.com	✓		27. 12 2017 04:07:24	27. 12 2017
□	powershell.exe (724)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	hq\va.scanner	JANKECH.hq.eset.com	✓		20. 12 2017 04:13:04	20. 12 2017
□	powershell.exe (16288)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	hq\va.scanner	JANKECH.hq.eset.com	✓		13. 12 2017 04:11:50	13. 12 2017
□	powershell.exe (29492)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	Unknown	JANKECH.hq.eset.com	✓		6. 12 2017 04:14:18	6. 12 2017
□	powershell.exe (269836)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	Unknown	JANKECH.hq.eset.com	✓		29. 11 2017 04:11:35	29. 11 2017
□	powershell.exe (240684)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	Unknown	JANKECH.hq.eset.com	✓		22. 11 2017 04:11:32	22. 11 2017
□	powershell.exe (202452)	"Get-AppxPackage -AllUsers | select name, version, architecture, publisher | Format-List | out-string -width 4096"	Unknown	JANKECH.hq.eset.com	✓		15. 11 2017 04:07:33	15. 11 2017
□	powershell.exe (8132)	-ExecutionPolicy Bypass -File C:\Users\Admin\AppData\Roaming\eei_demo.ps1	Unknown	JANKECH-TVM3	i		10. 11 2017 07:37:14	10. 11 2017
□	powershell.exe (4228)	-ExecutionPolicy Bypass -File C:\Users\lolo\AppData\Roaming\eei_demo.ps1	Unknown	JANKECH-TVM3	i		8. 11 2017 10:46:41	8. 11 2017



- Process details

powershell.exe
Windows PowerShell

SIGNATURE TYPE	Trusted
SIGNER NAME	Microsoft Windows
SEEN ON	1 computer
FIRST SEEN	2 months ago - 7. 11 2017 10:38:26
LAST EXECUTED	one day ago - 31. 1 2018 04:14:45

ESET LiveGrid®

REPUTATION	●●●●●●●●●
POPULARITY	●●●●●●●●●●●●
FIRST SEEN	2 years ago

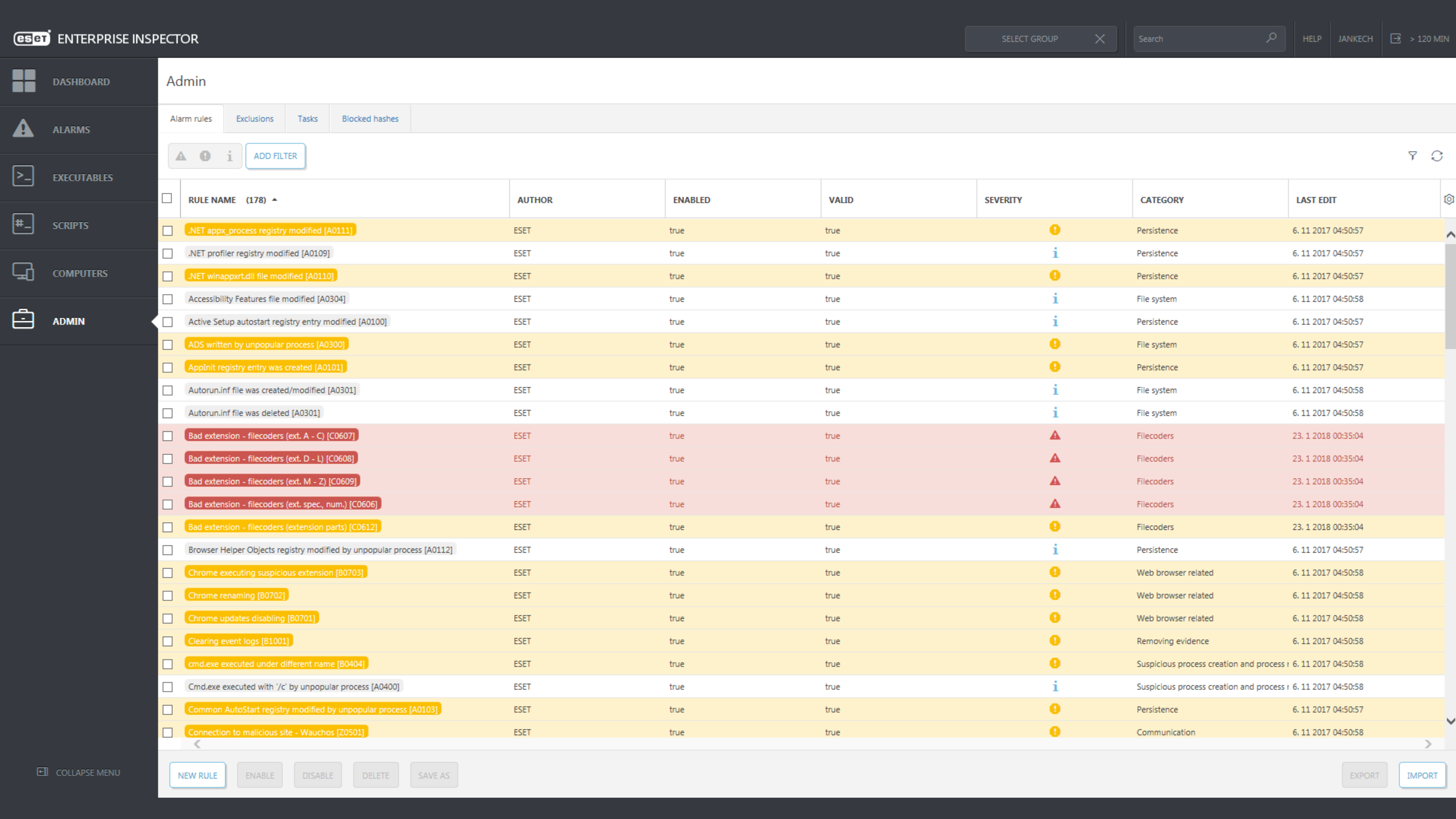
JANKECH.hq.eset.com

PARENT GROUP	Desktops
LAST CONNECTED	1. 2 2018 10:38:24
LAST EVENT	1. 2 2018 10:36:16
AGENT VERSION	1.2.620
OS	Windows 10

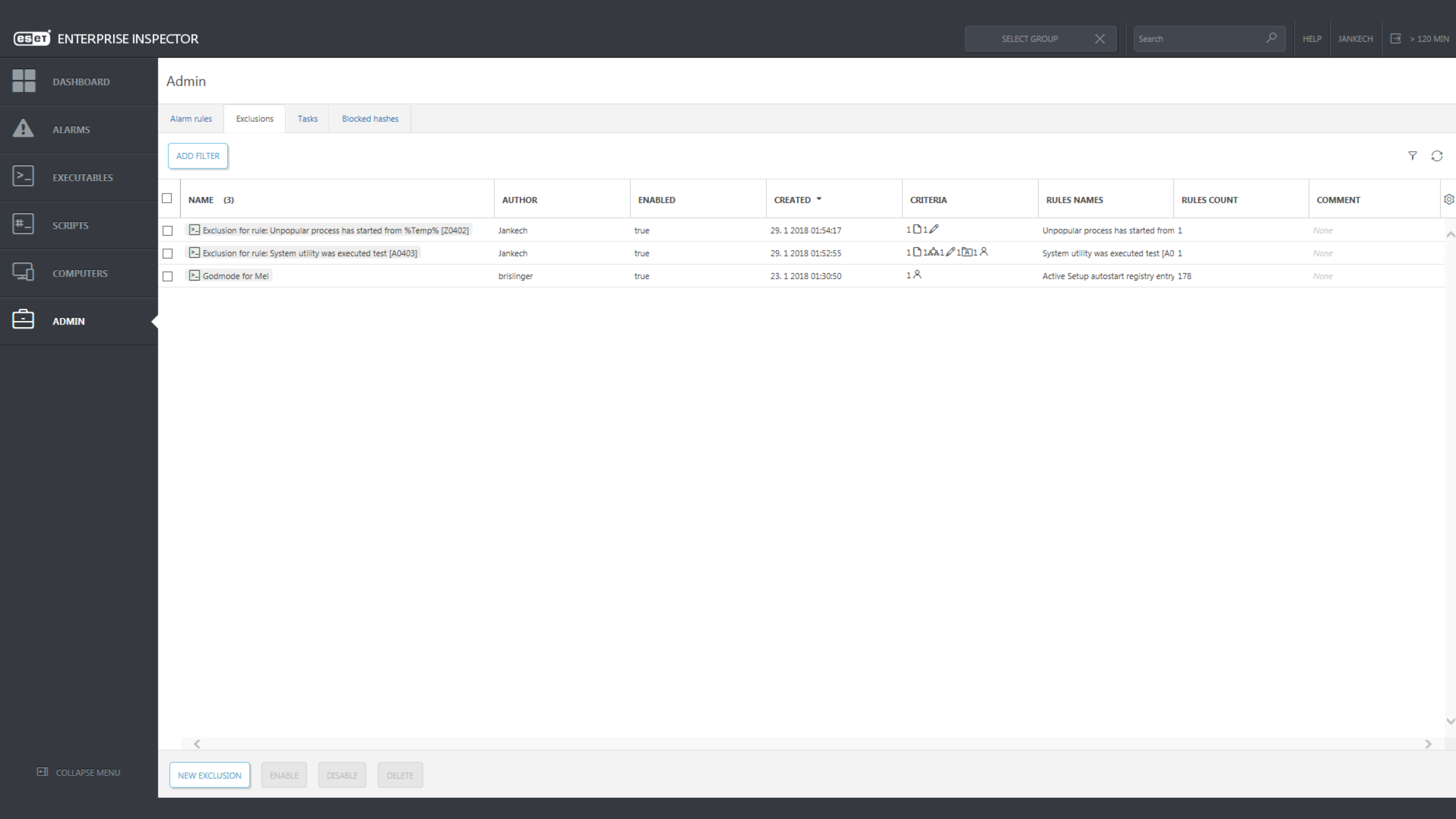
Events

File	Registry	Network
25	1	0

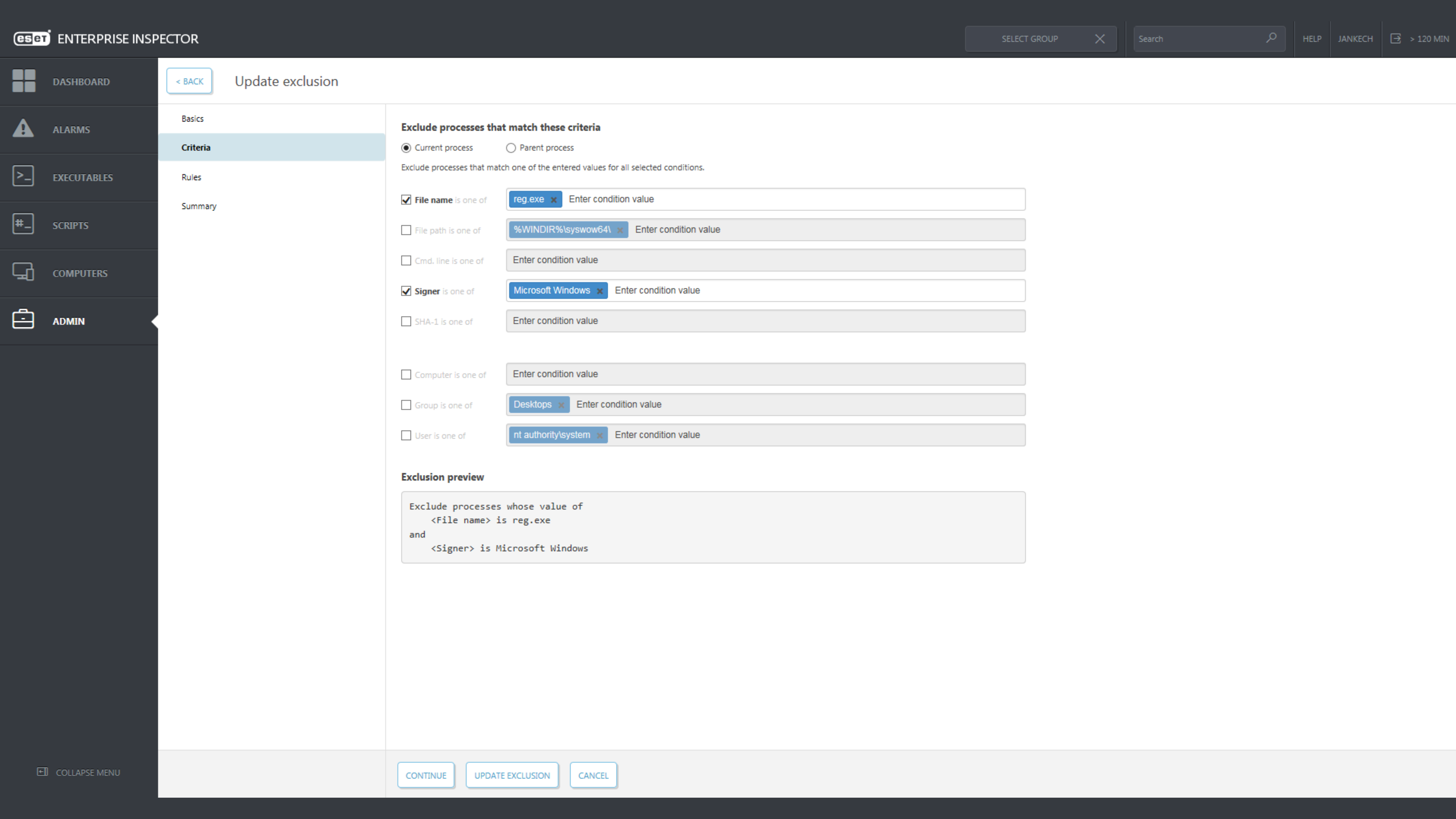
PROCESS	powershell.exe (26716)
COMMAND LINE	-executionpolicy bypass -file "C:\Users\jankech\Desktop\get_fingerprint\Get-Fingerprint.ps1"
PATH	%SYSTEM%\windowspowershell\v1.0\
STARTED	15. 1 2018 08:17:49
ENDED	15. 1 2018 08:17:54
PARENT PROCESS	cmd.exe (23664)
COMPUTER	JANKECH.hq.eset.com
EXECUTABLE	powershell.exe



□	RULE NAME (178) ▲	AUTHOR	ENABLED	VALID	SEVERITY	CATEGORY	LAST EDIT
□	.NET appx_process registry modified [A0111]	ESET	true	true	!	Persistence	6. 11 2017 04:50:57
□	.NET profiler registry modified [A0109]	ESET	true	true	i	Persistence	6. 11 2017 04:50:57
□	.NET winappxrt.dll file modified [A0110]	ESET	true	true	!	Persistence	6. 11 2017 04:50:57
□	Accessibility Features file modified [A0304]	ESET	true	true	i	File system	6. 11 2017 04:50:58
□	Active Setup autostart registry entry modified [A0100]	ESET	true	true	i	Persistence	6. 11 2017 04:50:57
□	ADS written by unpopular process [A0300]	ESET	true	true	!	File system	6. 11 2017 04:50:57
□	AppInit registry entry was created [A0101]	ESET	true	true	!	Persistence	6. 11 2017 04:50:57
□	Autorun.inf file was created/modified [A0301]	ESET	true	true	i	File system	6. 11 2017 04:50:58
□	Autorun.inf file was deleted [A0301]	ESET	true	true	i	File system	6. 11 2017 04:50:58
□	Bad extension - filecoders (ext. A - C) [C0607]	ESET	true	true	▲	Filecoders	23. 1 2018 00:35:04
□	Bad extension - filecoders (ext. D - L) [C0608]	ESET	true	true	▲	Filecoders	23. 1 2018 00:35:04
□	Bad extension - filecoders (ext. M - Z) [C0609]	ESET	true	true	▲	Filecoders	23. 1 2018 00:35:04
□	Bad extension - filecoders (ext. spec., num.) [C0606]	ESET	true	true	▲	Filecoders	23. 1 2018 00:35:04
□	Bad extension - filecoders (extension parts) [C0612]	ESET	true	true	!	Filecoders	23. 1 2018 00:35:04
□	Browser Helper Objects registry modified by unpopular process [A0112]	ESET	true	true	i	Persistence	6. 11 2017 04:50:57
□	Chrome executing suspicious extension [B0703]	ESET	true	true	!	Web browser related	6. 11 2017 04:50:58
□	Chrome renaming [B0702]	ESET	true	true	!	Web browser related	6. 11 2017 04:50:58
□	Chrome updates disabling [B0701]	ESET	true	true	!	Web browser related	6. 11 2017 04:50:58
□	Clearing event logs [B1001]	ESET	true	true	!	Removing evidence	6. 11 2017 04:50:58
□	cmd.exe executed under different name [B0404]	ESET	true	true	!	Suspicious process creation and process i	6. 11 2017 04:50:58
□	Cmd.exe executed with '/c' by unpopular process [A0400]	ESET	true	true	i	Suspicious process creation and process i	6. 11 2017 04:50:58
□	Common AutoStart registry modified by unpopular process [A0103]	ESET	true	true	!	Persistence	6. 11 2017 04:50:57
□	Connection to malicious site - Wauchos [Z0501]	ESET	true	true	!	Communication	6. 11 2017 04:50:58



☐	NAME (3)	AUTHOR	ENABLED	CREATED ▾	CRITERIA	RULES NAMES	RULES COUNT	COMMENT
☐	Exclusion for rule: Unpopular process has started from %Temp% [Z0402]	Jankech	true	29. 1 2018 01:54:17	1 🗋 1 ✎	Unpopular process has started from	1	None
☐	Exclusion for rule: System utility was executed test [A0403]	Jankech	true	29. 1 2018 01:52:55	1 🗋 1 ⁂ 1 ✎ 1 🗂 1 👤	System utility was executed test [A0	1	None
☐	Godmode for Me!	brislinger	true	23. 1 2018 01:30:50	1 👤	Active Setup autostart registry entry	178	None



Update exclusion

Exclude processes that match these criteria

● Current process ○ Parent process

Exclude processes that match one of the entered values for all selected conditions.

☑ **File name** is one of: reg.exe ×

□ File path is one of: %WINDIR%\syswow64\ ×

□ Cmd. line is one of: Enter condition value

☑ **Signer** is one of: Microsoft Windows ×

□ SHA-1 is one of: Enter condition value

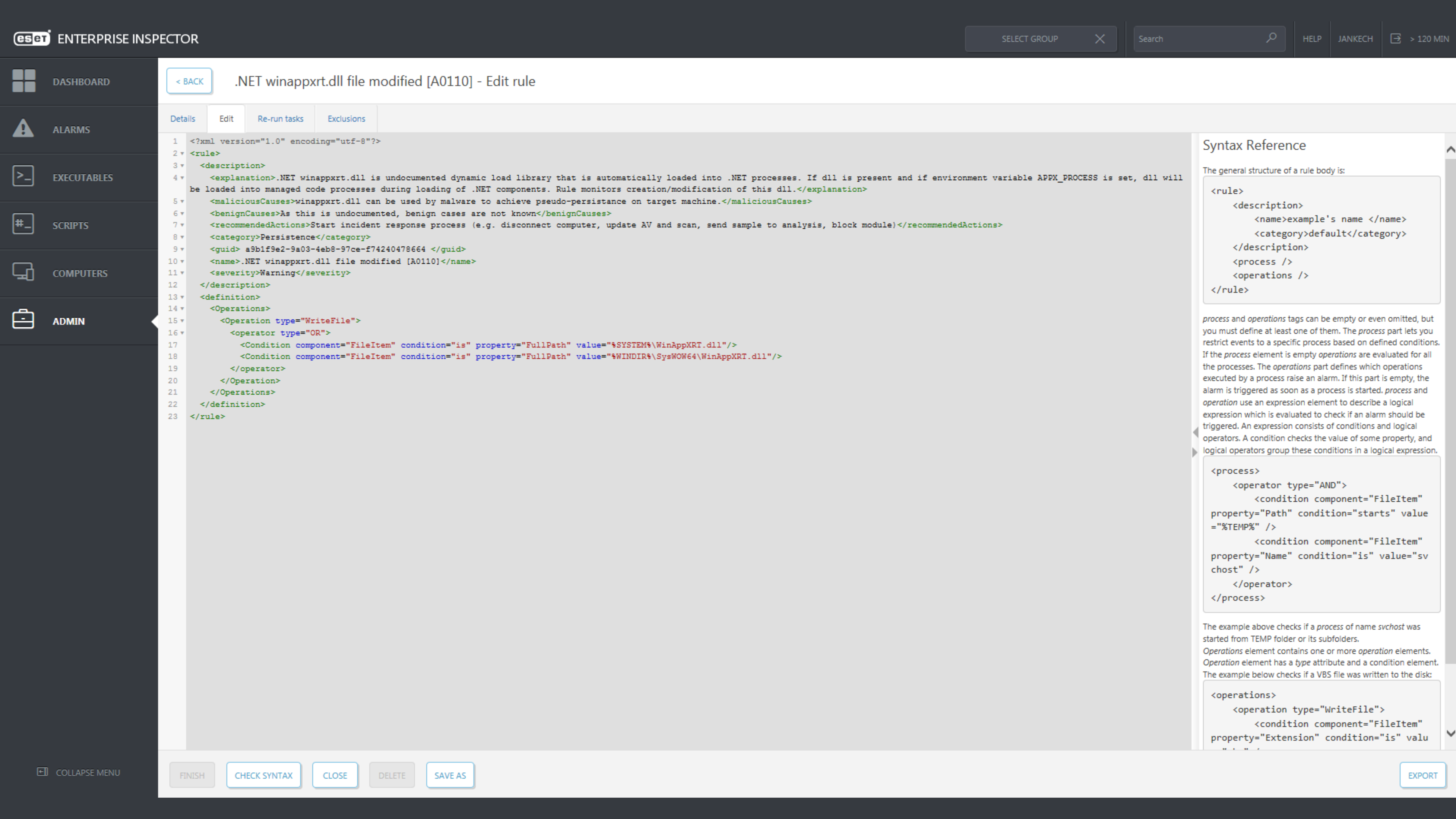
□ Computer is one of: Enter condition value

□ Group is one of: Desktops ×

□ User is one of: nt authority\system ×

Exclusion preview

```
Exclude processes whose value of
    <File name> is reg.exe
and
    <Signer> is Microsoft Windows
```



.NET winappxrt.dll file modified [A0110] - Edit rule

```
<?xml version="1.0" encoding="utf-8"?>
<rule>
  <description>
    <explanation>.NET winappxrt.dll is undocumented dynamic load library that is automatically loaded into .NET processes. If dll is present and if environment variable APPX_PROCESS is set, dll will be loaded into managed code processes during loading of .NET components. Rule monitors creation/modification of this dll.</explanation>
    <maliciousCauses>winappxrt.dll can be used by malware to achieve pseudo-persistance on target machine.</maliciousCauses>
    <benignCauses>As this is undocumented, benign cases are not known</benignCauses>
    <recommendedActions>Start incident response process (e.g. disconnect computer, update AV and scan, send sample to analysis, block module)</recommendedActions>
    <category>Persistence</category>
    <guid> a9b1f9e2-9a03-4eb8-97ce-f74240478664 </guid>
    <name>.NET winappxrt.dll file modified [A0110]</name>
    <severity>Warning</severity>
  </description>
  <definition>
    <Operations>
      <Operation type="WriteFile">
        <operator type="OR">
          <Condition component="FileItem" condition="is" property="FullPath" value="%SYSTEM%\WinAppXRT.dll"/>
          <Condition component="FileItem" condition="is" property="FullPath" value="%WINDIR%\SysWOW64\WinAppXRT.dll"/>
        </operator>
      </Operation>
    </Operations>
  </definition>
</rule>
```

Syntax Reference

The general structure of a rule body is:

```
<rule>
    <description>
        <name>example's name </name>
        <category>default</category>
    </description>
    <process />
    <operations />
</rule>
```

process and *operations* tags can be empty or even omitted, but you must define at least one of them. The *process* part lets you restrict events to a specific process based on defined conditions. If the *process* element is empty *operations* are evaluated for all the processes. The *operations* part defines which operations executed by a process raise an alarm. If this part is empty, the alarm is triggered as soon as a process is started. *process* and *operation* use an expression element to describe a logical expression which is evaluated to check if an alarm should be triggered. An expression consists of conditions and logical operators. A condition checks the value of some property, and logical operators group these conditions in a logical expression.

```
<process>
    <operator type="AND">
        <condition component="FileItem"
property="Path" condition="starts" value
="%TEMP%" />
        <condition component="FileItem"
property="Name" condition="is" value="sv
chost" />
    </operator>
</process>
```

The example above checks if a *process* of name *svchost* was started from TEMP folder or its subfolders.
Operations element contains one or more *operation* elements.
Operation element has a *type* attribute and a condition element.
The example below checks if a VBS file was written to the disk:

```
<operations>
    <operation type="WriteFile">
        <condition component="FileItem"
property="Extension" condition="is" valu
```

ESET® SECURITY MANAGEMENT CENTER

ESET® REMOTE ADMINISTRATOR

Problem: Not enough visibility

- Too many solutions, too many consoles
- Time needed to manage security is increasing
- Solutions are often non-consistent

What is new in ESMC?

Enterprise Inspector & Dynamic Threat Defense

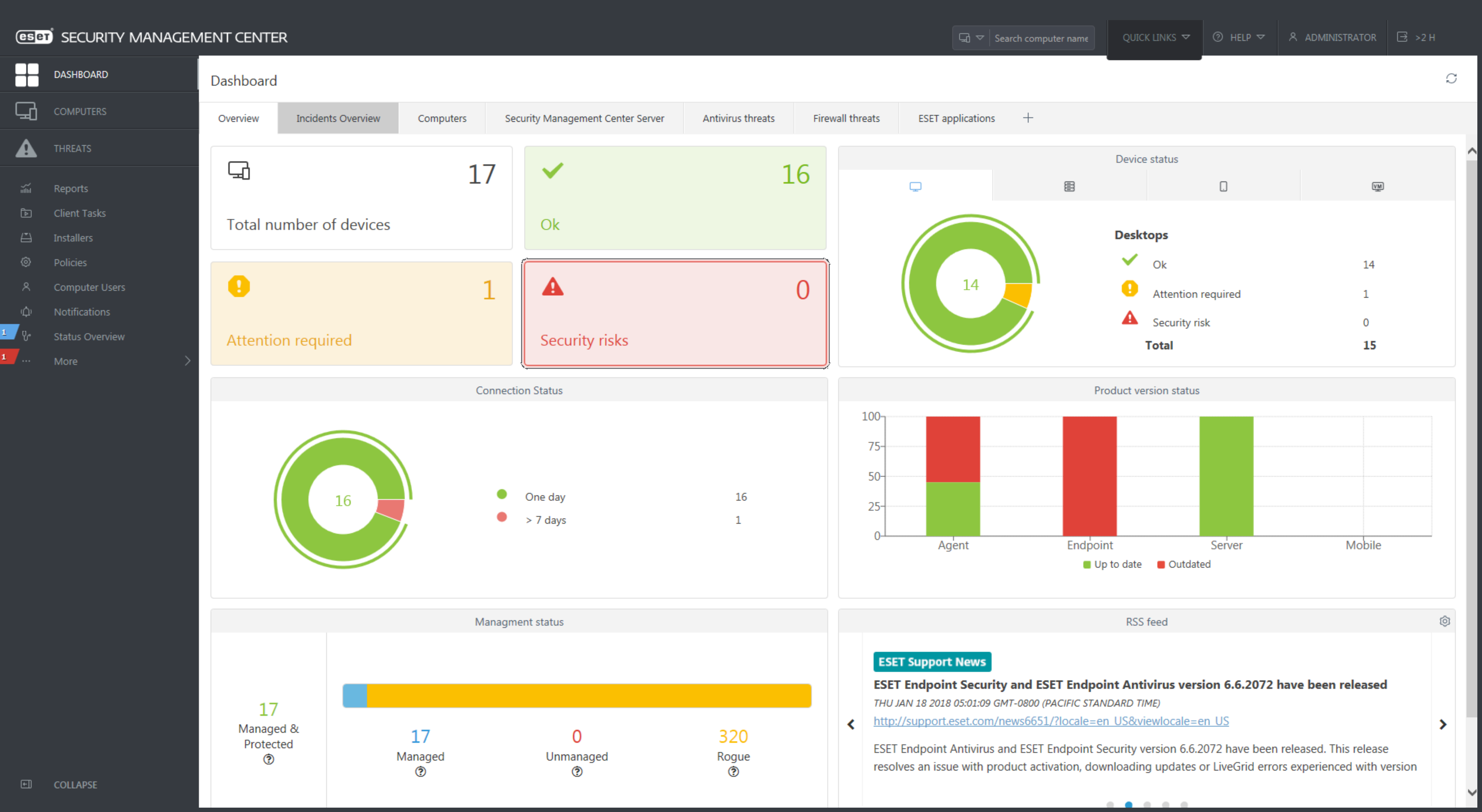
Full Network Troubleshooting & Visibility

Hardware Inventory

Automation

Friendly Interface

Enhanced Reporting / Notifications



17	Total number of devices
16	Ok
1	Attention required
0	Security risks

Desktops

✓ Ok	14
Attention required	1
Security risk	0
Total	**15**

● One day	16
● > 7 days	1

17 Managed & Protected	17 Managed	0 Unmanaged	320 Rogue

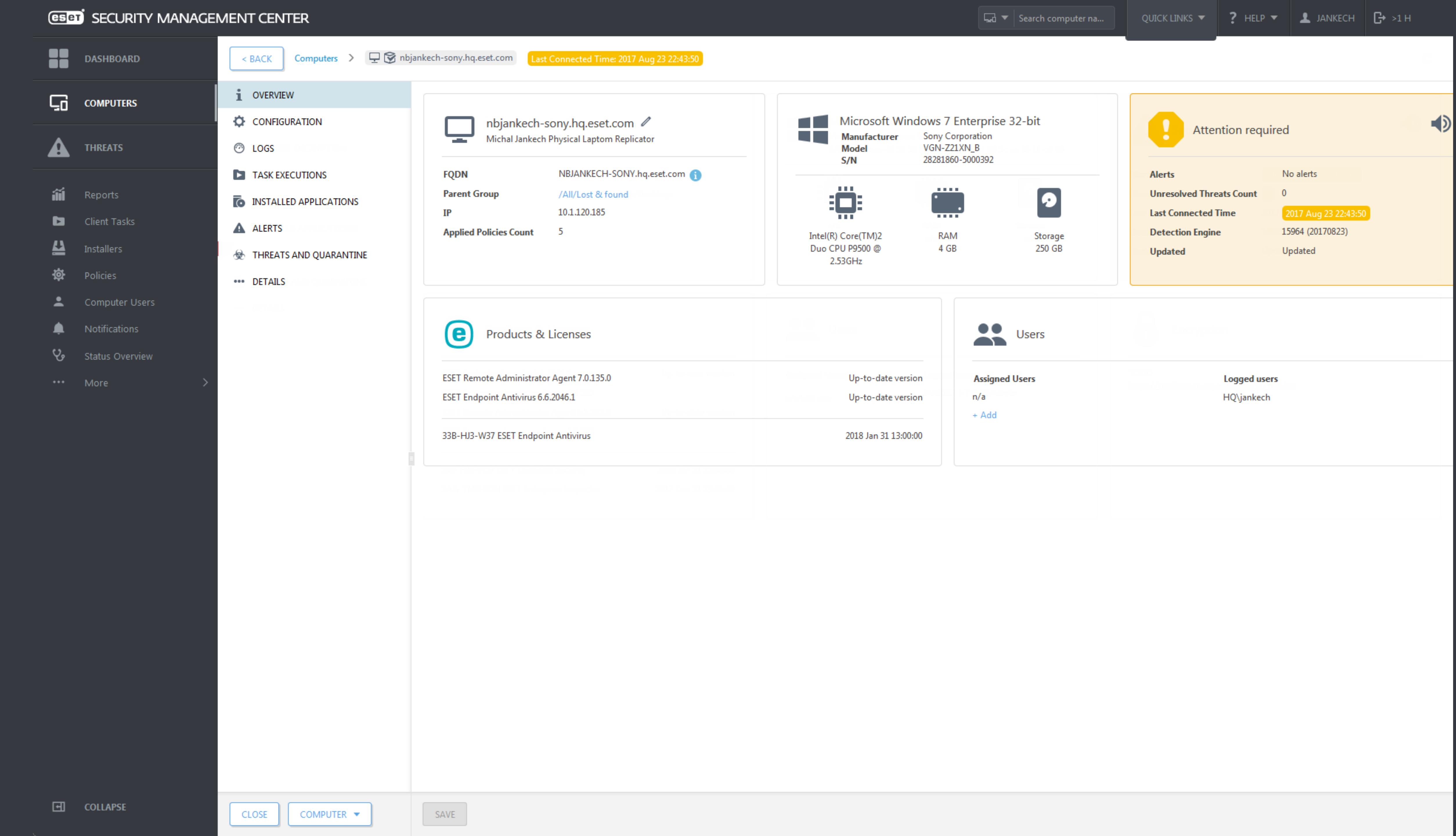
ESET Support News

ESET Endpoint Security and ESET Endpoint Antivirus version 6.6.2072 have been released

THU JAN 18 2018 05:01:09 GMT-0800 (PACIFIC STANDARD TIME)

http://support.eset.com/news6651/?locale=en_US&viewlocale=en_US

ESET Endpoint Antivirus and ESET Endpoint Security version 6.6.2072 have been released. This release resolves an issue with product activation, downloading updates or LiveGrid errors experienced with version



nbjankech-sony.hq.eset.com

Last Connected Time: 2017 Aug 23 22:43:50

nbjankech-sony.hq.eset.com
Michal Jankech Physical Laptom Replicator

FQDN	NBJANKECH-SONY.hq.eset.com
Parent Group	/All/Lost & found
IP	10.1.120.185
Applied Policies Count	5

Microsoft Windows 7 Enterprise 32-bit

Manufacturer	Sony Corporation
Model	VGN-Z21XN_B
S/N	28281860-5000392

Intel(R) Core(TM)2 Duo CPU P9500 @ 2.53GHz

RAM
4 GB

Storage
250 GB

Attention required

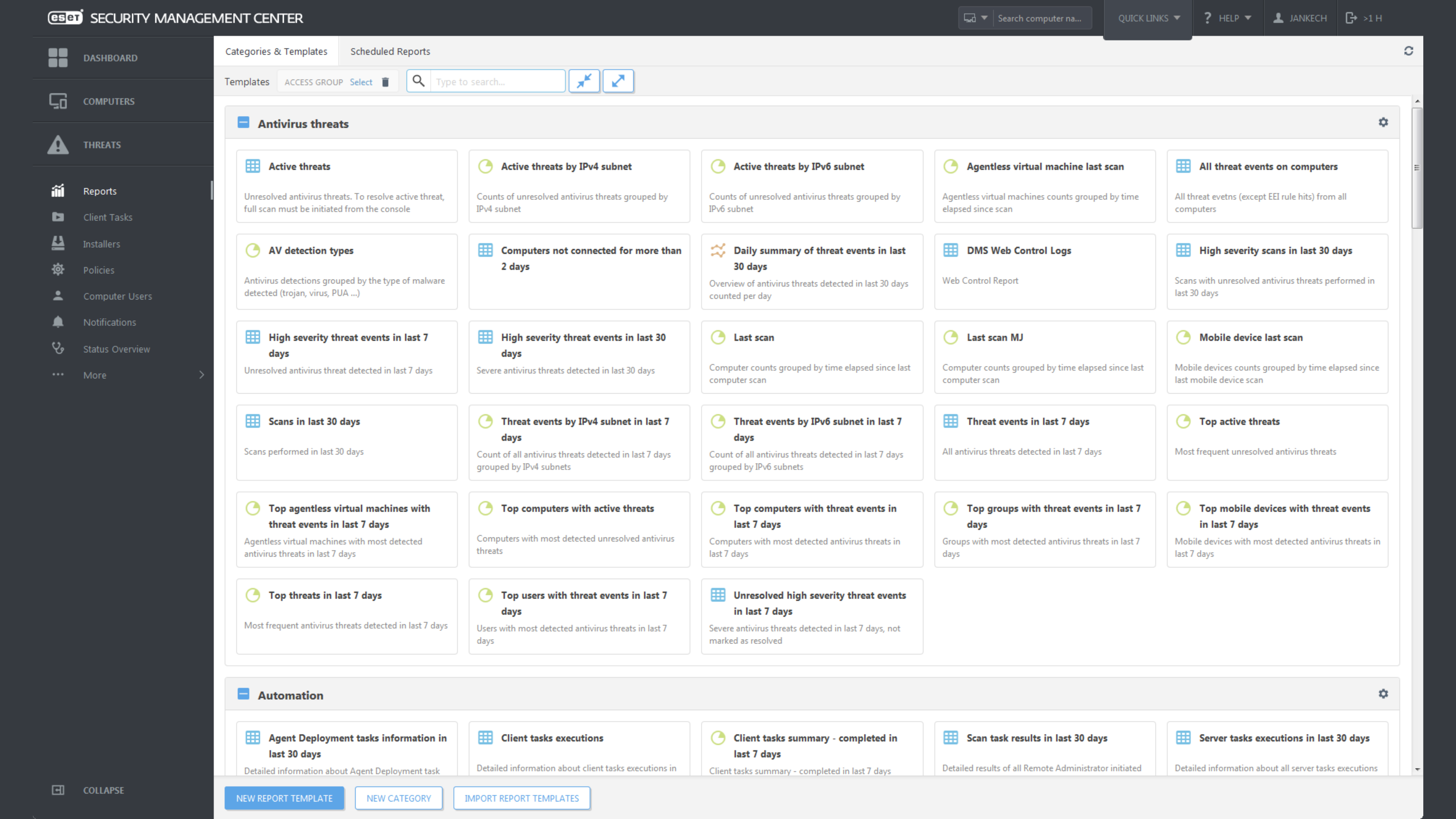
Alerts	No alerts
Unresolved Threats Count	0
Last Connected Time	2017 Aug 23 22:43:50
Detection Engine	15964 (20170823)
Updated	Updated

Products & Licenses

ESET Remote Administrator Agent 7.0.135.0	Up-to-date version
ESET Endpoint Antivirus 6.6.2046.1	Up-to-date version
33B-HJ3-W37 ESET Endpoint Antivirus	2018 Jan 31 13:00:00

Users

Assigned Users	Logged users
n/a	HQ\jankech
+ Add	



Antivirus threats

Active threats
Unresolved antivirus threats. To resolve active threat, full scan must be initiated from the console

Active threats by IPv4 subnet
Counts of unresolved antivirus threats grouped by IPv4 subnet

Active threats by IPv6 subnet
Counts of unresolved antivirus threats grouped by IPv6 subnet

Agentless virtual machine last scan
Agentless virtual machines counts grouped by time elapsed since scan

All threat events on computers
All threat evetns (except EEI rule hits) from all computers

AV detection types
Antivirus detections grouped by the type of malware detected (trojan, virus, PUA ...)

Computers not connected for more than 2 days

Daily summary of threat events in last 30 days
Overview of antivirus threats detected in last 30 days counted per day

DMS Web Control Logs
Web Control Report

High severity scans in last 30 days
Scans with unresolved antivirus threats performed in last 30 days

High severity threat events in last 7 days
Unresolved antivirus threat detected in last 7 days

High severity threat events in last 30 days
Severe antivirus threats detected in last 30 days

Last scan
Computer counts grouped by time elapsed since last computer scan

Last scan MJ
Computer counts grouped by time elapsed since last computer scan

Mobile device last scan
Mobile devices counts grouped by time elapsed since last mobile device scan

Scans in last 30 days
Scans performed in last 30 days

Threat events by IPv4 subnet in last 7 days
Count of all antivirus threats detected in last 7 days grouped by IPv4 subnets

Threat events by IPv6 subnet in last 7 days
Count of all antivirus threats detected in last 7 days grouped by IPv6 subnets

Threat events in last 7 days
All antivirus threats detected in last 7 days

Top active threats
Most frequent unresolved antivirus threats

Top agentless virtual machines with threat events in last 7 days
Agentless virtual machines with most detected antivirus threats in last 7 days

Top computers with active threats
Computers with most detected unresolved antivirus threats

Top computers with threat events in last 7 days
Computers with most detected antivirus threats in last 7 days

Top groups with threat events in last 7 days
Groups with most detected antivirus threats in last 7 days

Top mobile devices with threat events in last 7 days
Mobile devices with most detected antivirus threats in last 7 days

Top threats in last 7 days
Most frequent antivirus threats detected in last 7 days

Top users with threat events in last 7 days
Users with most detected antivirus threats in last 7 days

Unresolved high severity threat events in last 7 days
Severe antivirus threats detected in last 7 days, not marked as resolved

Automation

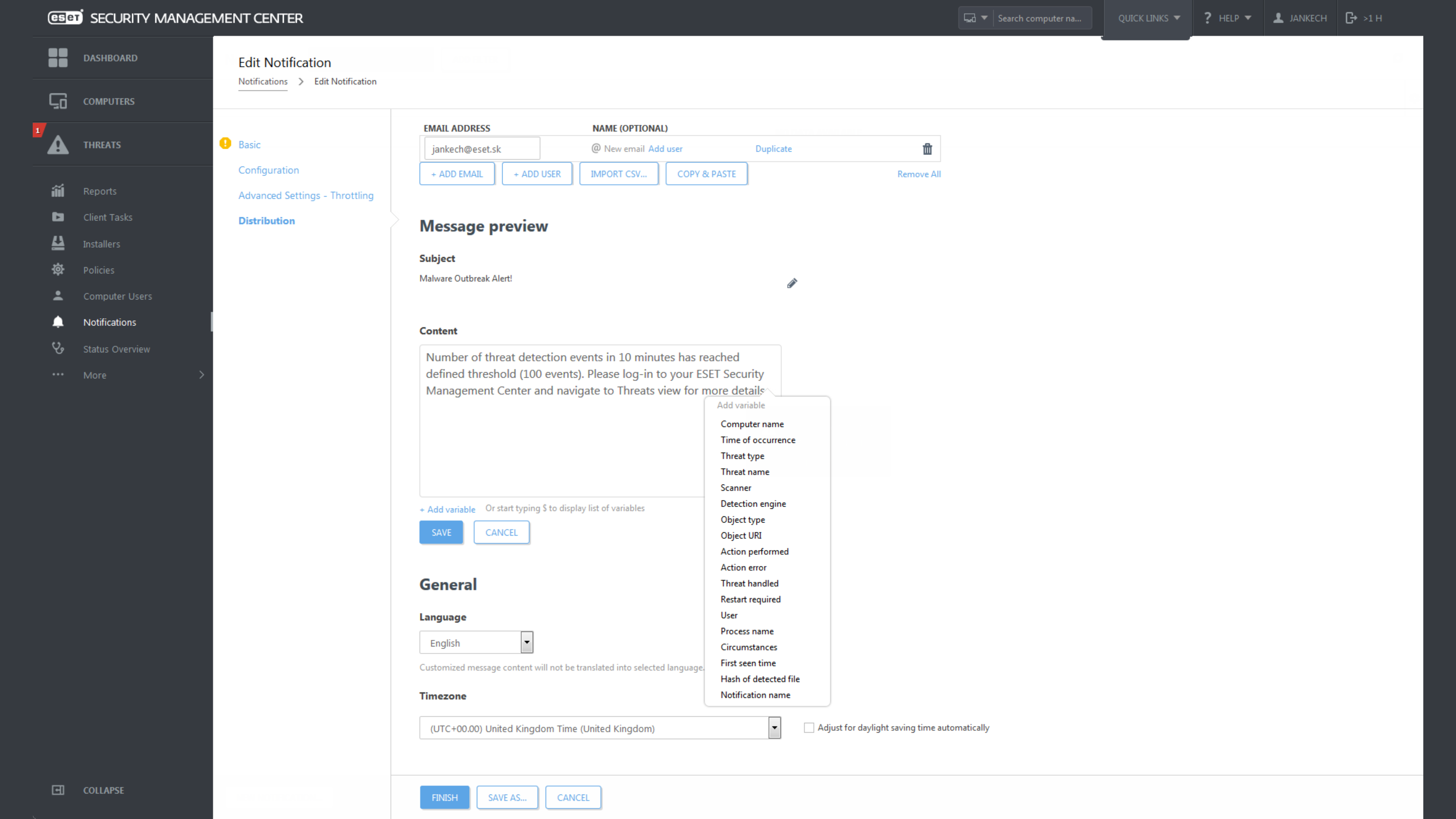
Agent Deployment tasks information in last 30 days
Detailed information about Agent Deployment task

Client tasks executions
Detailed information about client tasks executions in

Client tasks summary - completed in last 7 days
Client tasks summary - completed in last 7 days

Scan task results in last 30 days
Detailed results of all Remote Administrator initiated

Server tasks executions in last 30 days
Detailed information about all server tasks executions



Edit Notification

Notifications > Edit Notification

EMAIL ADDRESS: jankech@eset.sk

NAME (OPTIONAL): New email

Message preview

Subject

Malware Outbreak Alert!

Content

Number of threat detection events in 10 minutes has reached defined threshold (100 events). Please log-in to your ESET Security Management Center and navigate to Threats view for more details

Or start typing $ to display list of variables

Add variable

- Computer name
- Time of occurrence
- Threat type
- Threat name
- Scanner
- Detection engine
- Object type
- Object URI
- Action performed
- Action error
- Threat handled
- Restart required
- User
- Process name
- Circumstances
- First seen time
- Hash of detected file
- Notification name

General

Language

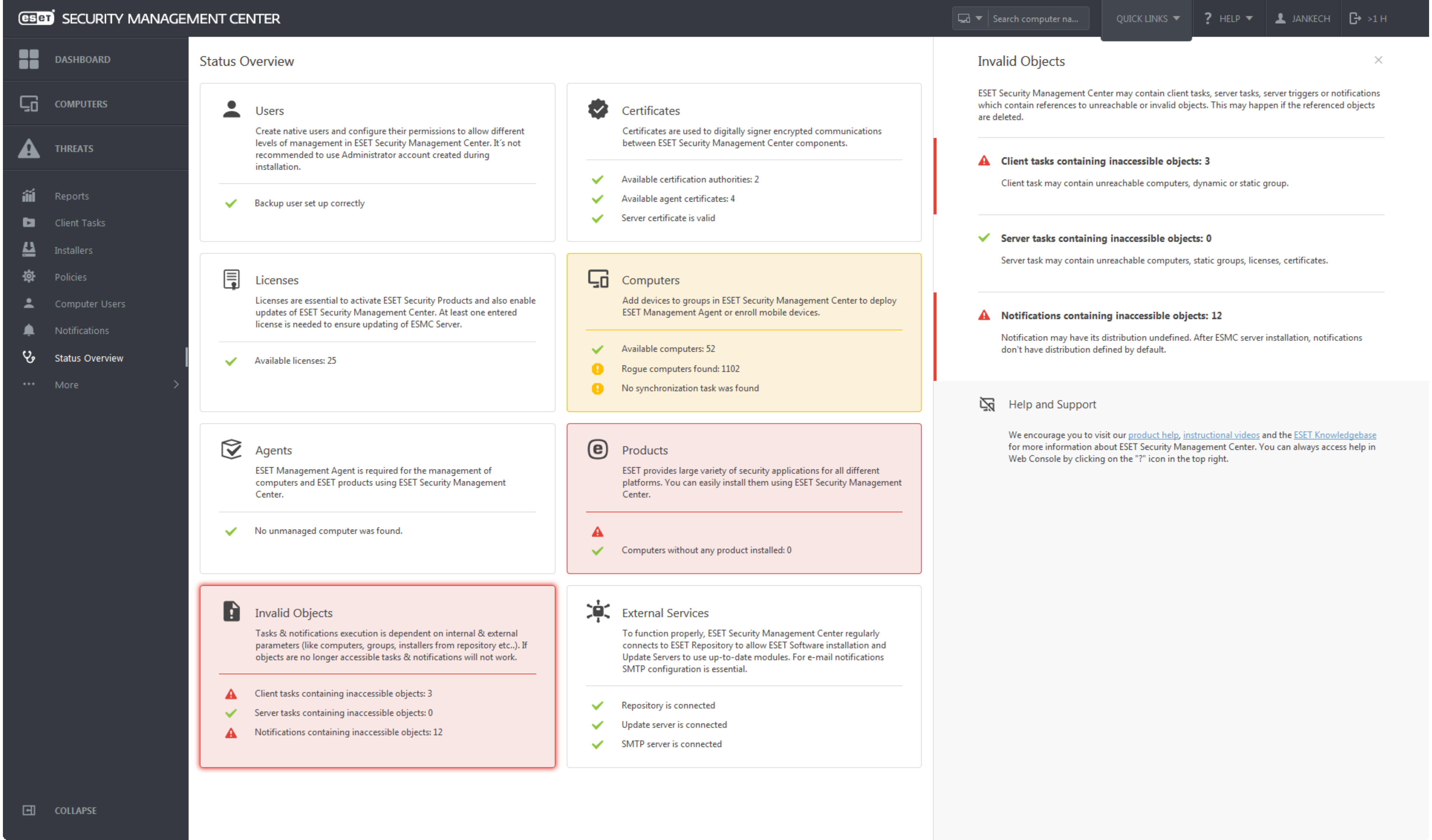
English

Customized message content will not be translated into selected language.

Timezone

(UTC+00.00) United Kingdom Time (United Kingdom)

□ Adjust for daylight saving time automatically



Status Overview

Users

Create native users and configure their permissions to allow different levels of management in ESET Security Management Center. It's not recommended to use Administrator account created during installation.

✓ Backup user set up correctly

Certificates

Certificates are used to digitally signer encrypted communications between ESET Security Management Center components.

✓ Available certification authorities: 2
✓ Available agent certificates: 4
✓ Server certificate is valid

Licenses

Licenses are essential to activate ESET Security Products and also enable updates of ESET Security Management Center. At least one entered license is needed to ensure updating of ESMC Server.

✓ Available licenses: 25

Computers

Add devices to groups in ESET Security Management Center to deploy ESET Management Agent or enroll mobile devices.

✓ Available computers: 52
! Rogue computers found: 1102
! No synchronization task was found

Agents

ESET Management Agent is required for the management of computers and ESET products using ESET Security Management Center.

✓ No unmanaged computer was found.

Products

ESET provides large variety of security applications for all different platforms. You can easily install them using ESET Security Management Center.

⚠
✓ Computers without any product installed: 0

Invalid Objects

Tasks & notifications execution is dependent on internal & external parameters (like computers, groups, installers from repository etc..). If objects are no longer accessible tasks & notifications will not work.

⚠ Client tasks containing inaccessible objects: 3
✓ Server tasks containing inaccessible objects: 0
⚠ Notifications containing inaccessible objects: 12

External Services

To function properly, ESET Security Management Center regularly connects to ESET Repository to allow ESET Software installation and Update Servers to use up-to-date modules. For e-mail notifications SMTP configuration is essential.

✓ Repository is connected
✓ Update server is connected
✓ SMTP server is connected

Invalid Objects

ESET Security Management Center may contain client tasks, server tasks, server triggers or notifications which contain references to unreachable or invalid objects. This may happen if the referenced objects are deleted.

⚠ **Client tasks containing inaccessible objects: 3**

Client task may contain unreachable computers, dynamic or static group.

✓ **Server tasks containing inaccessible objects: 0**

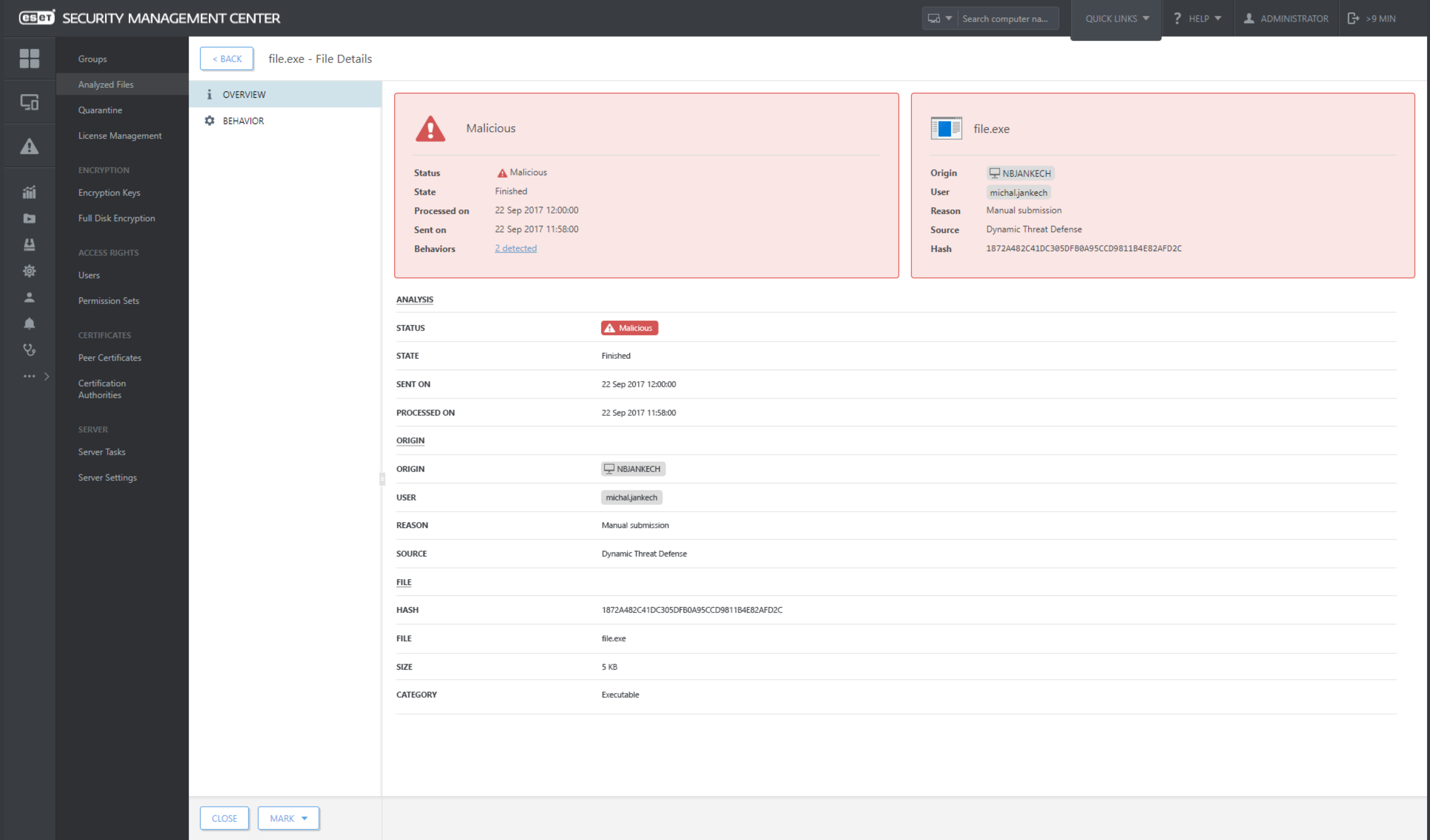
Server task may contain unreachable computers, static groups, licenses, certificates.

⚠ **Notifications containing inaccessible objects: 12**

Notification may have its distribution undefined. After ESMC server installation, notifications don't have distribution defined by default.

Help and Support

We encourage you to visit our product help, instructional videos and the ESET Knowledgebase for more information about ESET Security Management Center. You can always access help in Web Console by clicking on the "?" icon in the top right.



file.exe - File Details

Malicious

Status	Malicious
State	Finished
Processed on	22 Sep 2017 12:00:00
Sent on	22 Sep 2017 11:58:00
Behaviors	2 detected

file.exe

Origin	NBJANKECH
User	michal.jankech
Reason	Manual submission
Source	Dynamic Threat Defense
Hash	1872A482C41DC305DFB0A95CCD9811B4E82AFD2C

ANALYSIS

STATUS	Malicious
STATE	Finished
SENT ON	22 Sep 2017 12:00:00
PROCESSED ON	22 Sep 2017 11:58:00

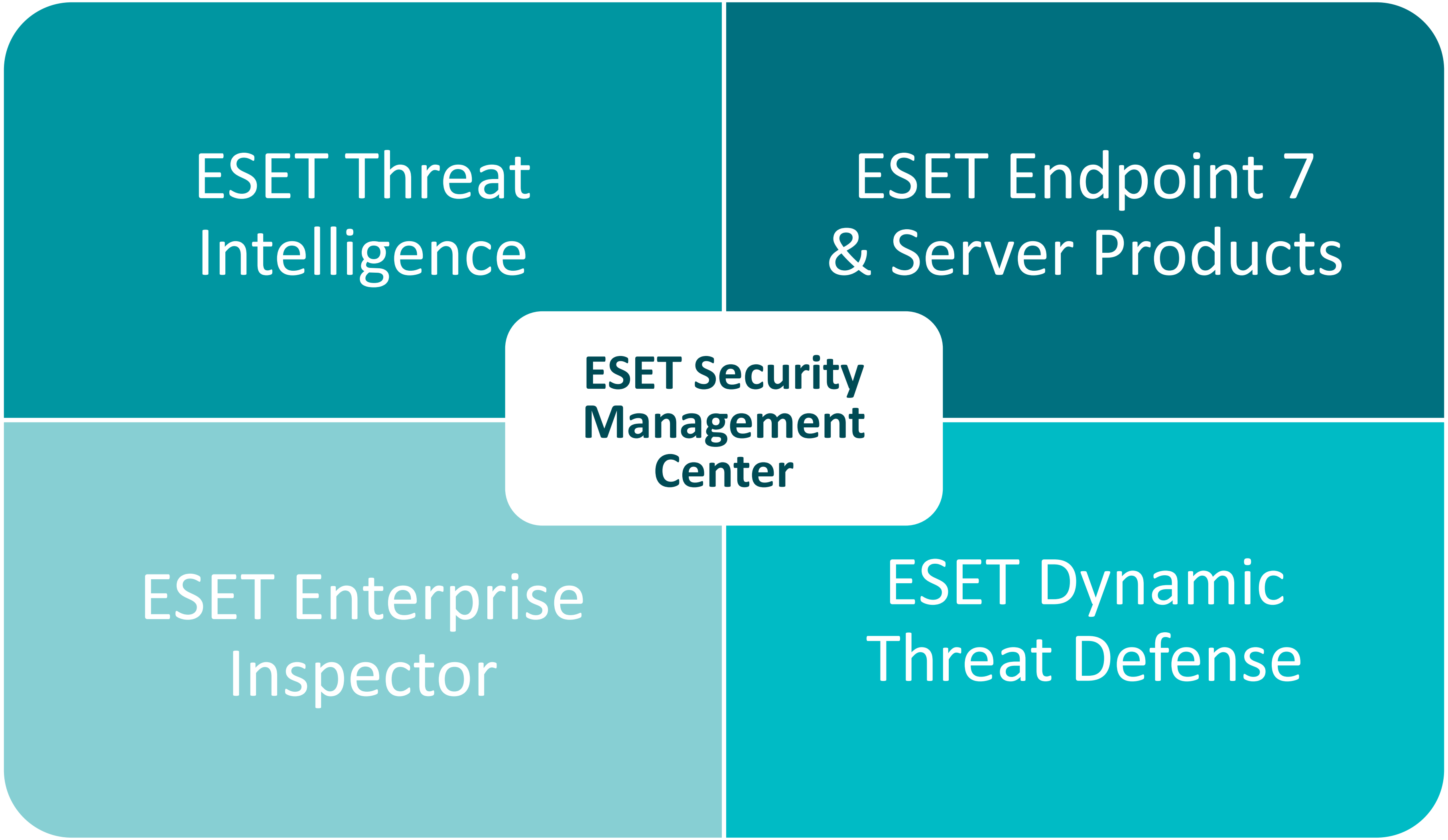
ORIGIN

ORIGIN	NBJANKECH
USER	michal.jankech
REASON	Manual submission
SOURCE	Dynamic Threat Defense

FILE

HASH	1872A482C41DC305DFB0A95CCD9811B4E82AFD2C
FILE	file.exe
SIZE	5 KB
CATEGORY	Executable

Solution tailored for Enterprises



ESET Threat Intelligence

ESET Endpoint 7 & Server Products

ESET Security Management Center

ESET Enterprise Inspector

ESET Dynamic Threat Defense

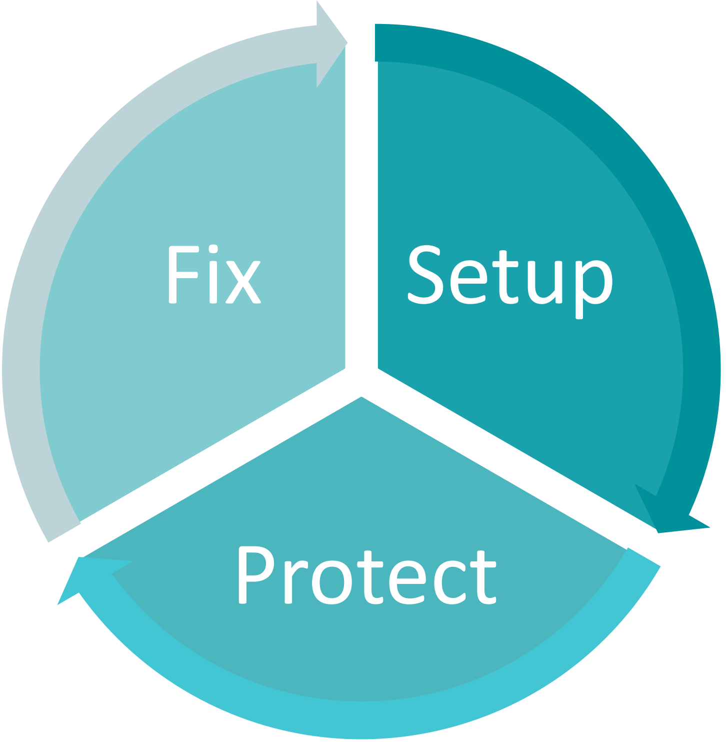
Professional & Security Services

Problem: Not enough workforce

- Not enough budget
- Enough budget, but not enough people
- It takes time to known your solution well

ESET Enterprise Service Portfolio

Malware Analysis
Forensic Analysis
Incident Response



Deployment Service
Premium Support

Threat Monitoring & Threat Hunting
ETI Data Feeds & Early Warning

Summary

- **Continuous growth in enterprise segment**
- **Top 4 enterprise endpoint security vendor**
- **Expanding enterprise sales teams globally** to support customers
- The most **complete endpoint, advanced cloud sandboxing & EDR facility** managed via a **single management console for the widest range of platforms**

30 YEARS OF
CONTINUOUS
IT SECURITY
INNOVATION

ESET®

ENJOY SAFER TECHNOLOGY™