Cortex XDR

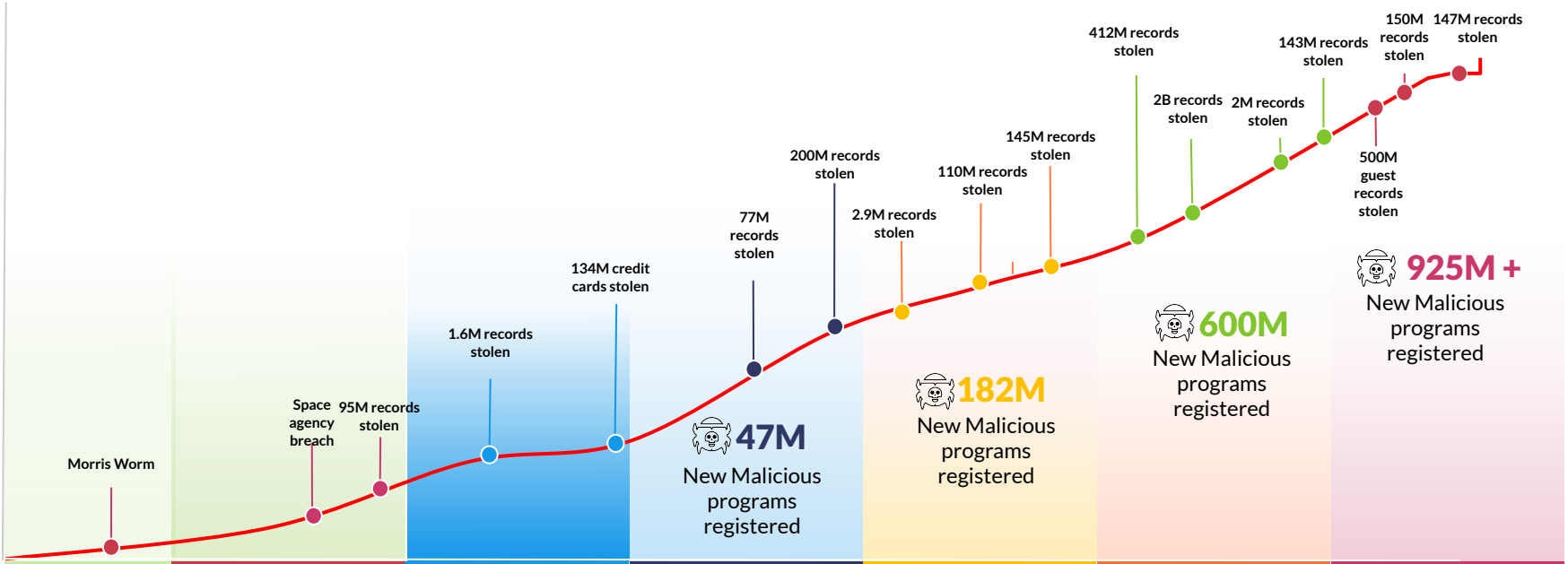
GET ALL THE ANSWERS

Before, During and After an Attack.

Mikkel Bossen

SE - Palo Alto Networks

Threats are Escalating



Get All the Answers

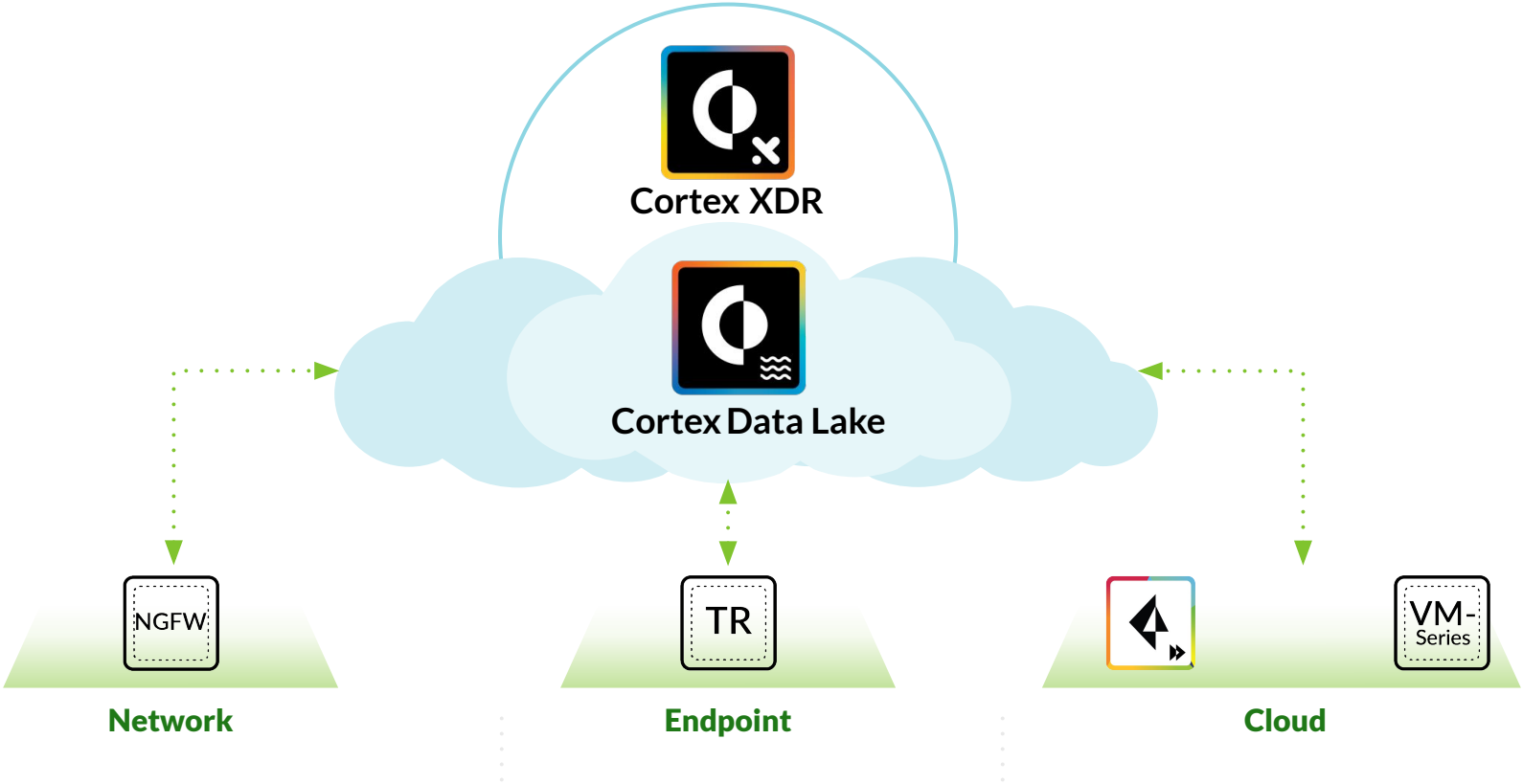
Cortex XDR breaks down silos to stop all attacks

CORTEX XDR™

The new category for detection & response

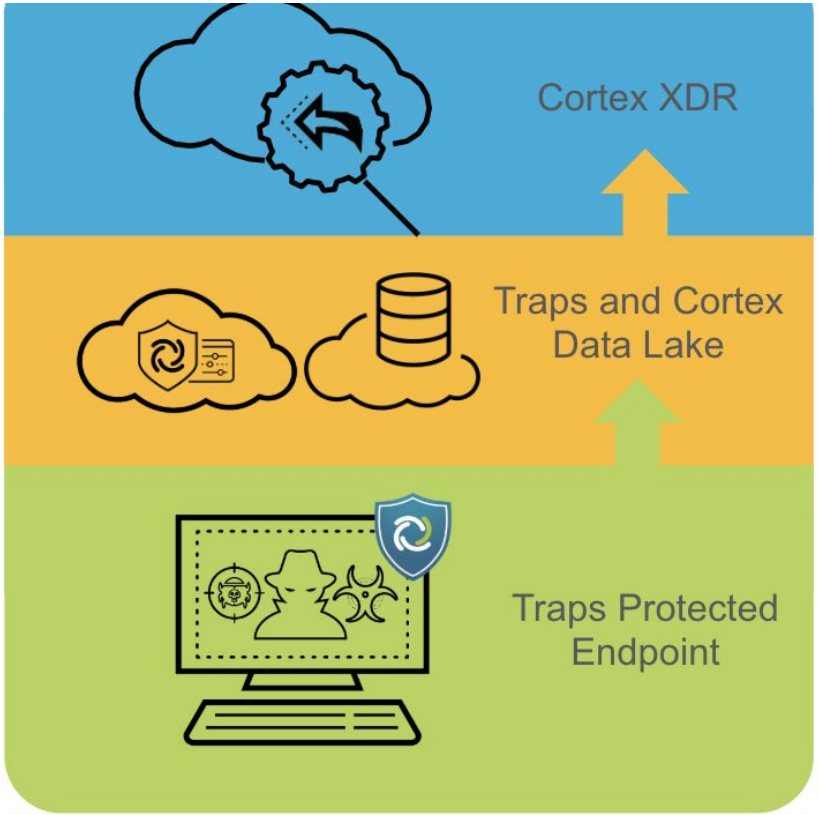
- Best-in-class prevention
- Most comprehensive security data asset
- Continuous ML-based detection
- Automated root-cause analysis
- Integrated response for network and endpoint

The industry's best security data asset

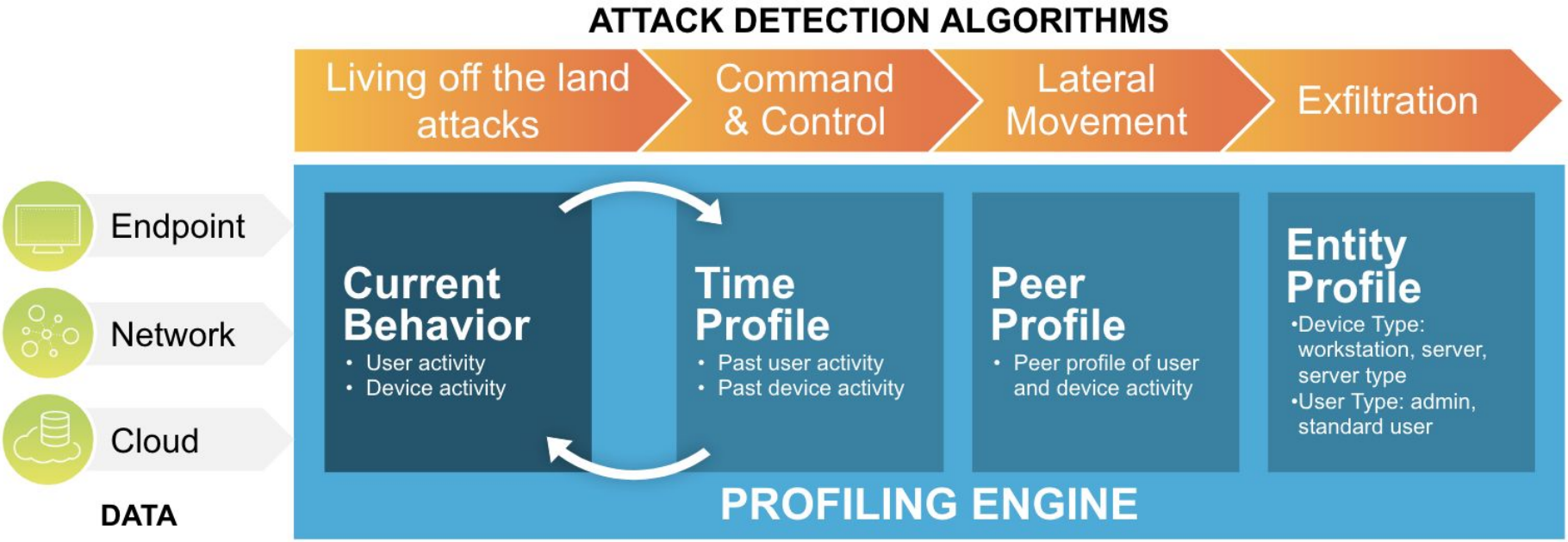


Rich Data Collection For Cortex XDR

- Data collected supports investigation, visualization and detection flows
- Controlled via content updates:
  - Process creation\termination events
  - Registry modification events
  - Image load events
  - Session log on\off & connect\disconnect information
  - File modification information
  - Network session information (5-tuple)
  - Endpoint events: time change and boot up



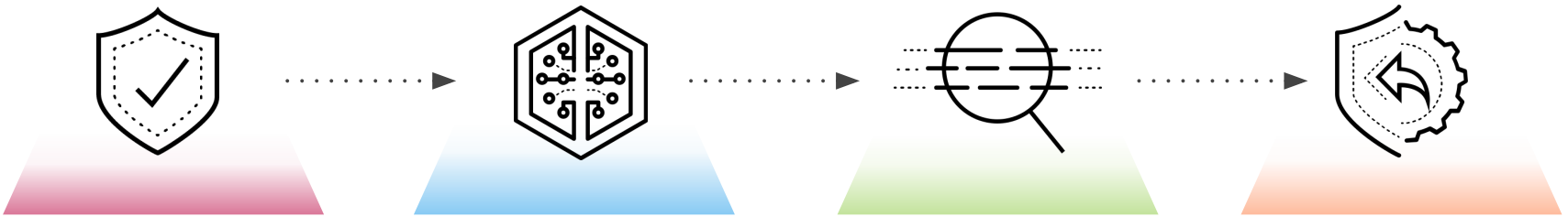
Automatically Detect Attacks with Machine Learning



Profile behavior & detect anomalies indicative of an attack

DEMO TIME

The Complete Solution for Security Operations



Stop threats with best-in-class prevention

Traps Endpoint & Next-Generation Firewall

Detect sophisticated threats with analytics

Cortex XDR

Accelerate investigations with rich context

Cortex XDR & AutoFocus

Automate response and get smarter with each incident

Demisto

SECURE THE ENTERPRISE

SECURE THE CLOUD

PRISMA™
BY PALO ALTO NETWORKS

SECURE THE FUTURE

CORTEX™
BY PALO ALTO NETWORKS

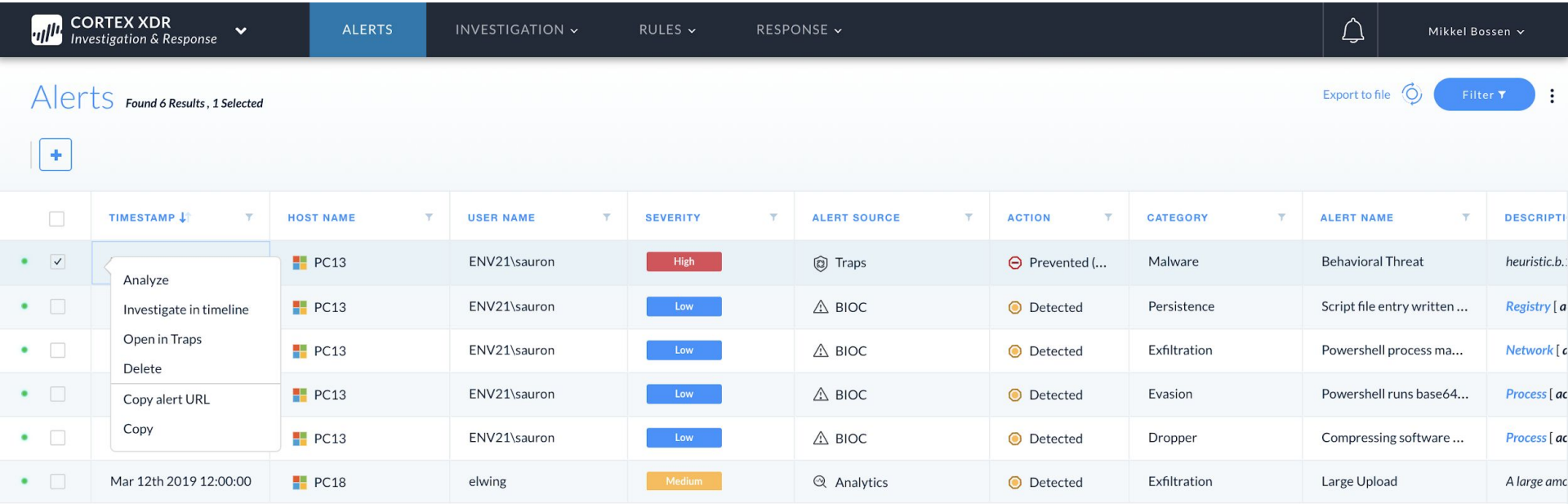
Thank You

See and Learn more @ Our Booth

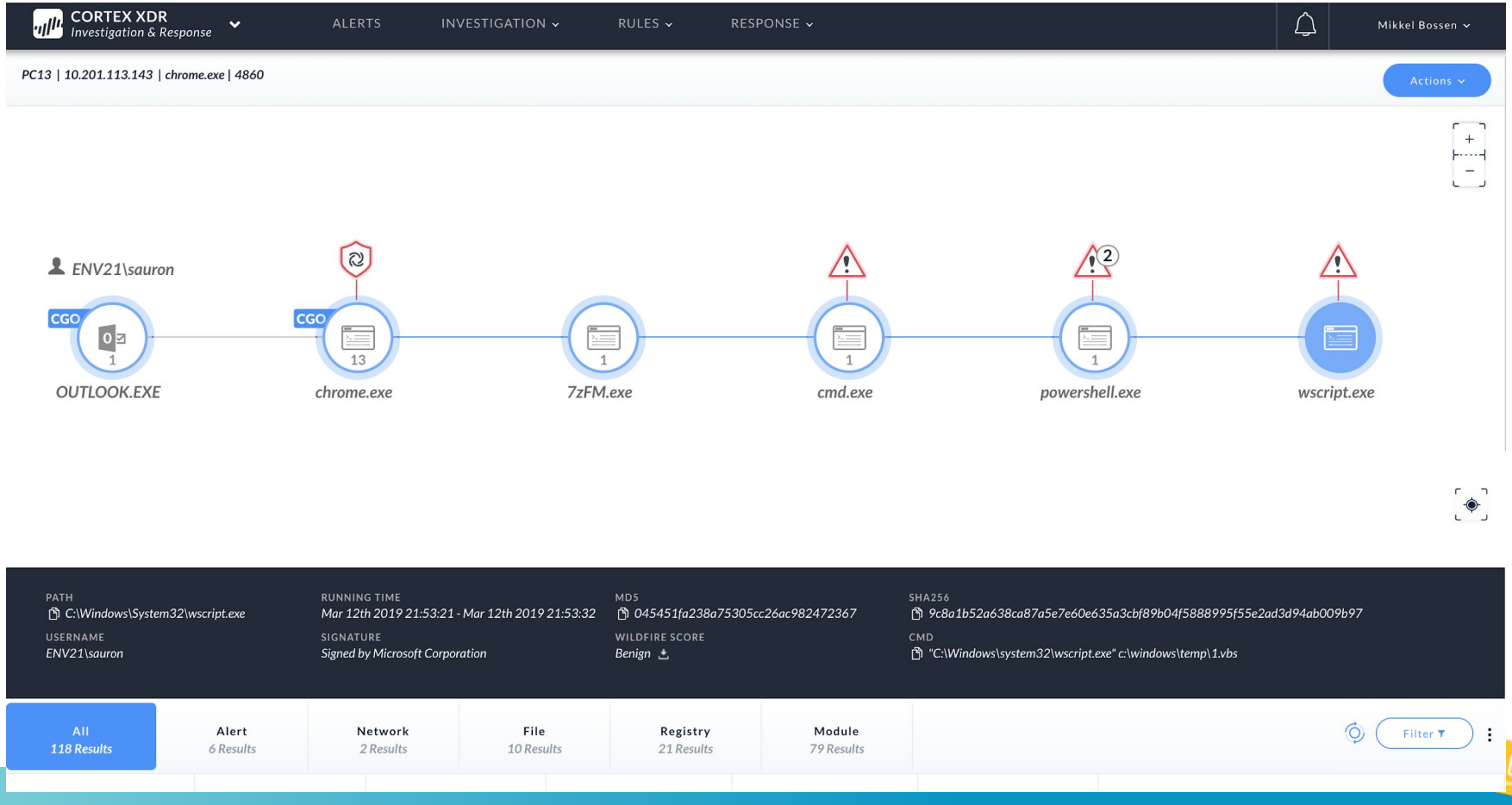
Email: mbossen@paloaltonetworks.com

Backup Slides

Alerts


CORTEX XDR
Investigation & Response
ALERTS
INVESTIGATION
RULES
RESPONSE
Mikkel Bossen
Alerts
Found 6 Results , 1 Selected
Export to file
Filter
TIMESTAMP
HOST NAME
USER NAME
SEVERITY
ALERT SOURCE
ACTION
CATEGORY
ALERT NAME
DESCRIPTI
Analyze
Investigate in timeline
Open in Traps
Delete
Copy alert URL
Copy
PC13
ENV21\sauron
High
Traps
Prevented (...
Malware
Behavioral Threat
heuristic.b.
PC13
ENV21\sauron
Low
BIOC
Detected
Persistence
Script file entry written ...
Registry [a
PC13
ENV21\sauron
Low
BIOC
Detected
Exfiltration
Powershell process ma...
Network [d
PC13
ENV21\sauron
Low
BIOC
Detected
Evasion
Powershell runs base64...
Process [ac
PC13
ENV21\sauron
Low
BIOC
Detected
Dropper
Compressing software ...
Process [ac
Mar 12th 2019 12:00:00
PC18
elwing
Medium
Analytics
Detected
Exfiltration
Large Upload
A large amo

Causality chain



Detailed information – Persistence Gained

PATH
C:\Windows\System32\wscript.exe

RUNNING TIME
Mar 12th 2019 21:53:21 - Mar 12th 2019 21:53:32

MD5
045451fa238a75305cc26ac982472367

SHA256
9c8a1b52a638ca87a5e7e60e635a3cbf89b04f5888995f55e2ad3d94ab009b97

USERNAME
ENV21\sauron

SIGNATURE
Signed by Microsoft Corporation

WILDFIRE SCORE
Benign

CMD
"C:\Windows\system32\wscript.exe" c:\windows\temp\1.vbs

All 118 Results | Alert 6 Results | Network 2 Results | File 10 Results | Registry 21 Results | Module 79 Results

Filter

TIMESTAMP	USER NAME	INITIATED BY	INITIATOR PID	INITIATOR TID	ACTION TYPE	DESCRIPTION
Mar 12th 2019 21:54:03	ENV21\sauron	wscript.exe	336	3876	Persistence	**Product** : IOC **Alert** : IOC (154.16.201.93) **Severity** : Informational **Process**
Mar 12th 2019 21:54:03	ENV21\sauron	wscript.exe	336	3876	Persistence	**Product** : IOC **Alert** : IOC (154.16.201.93) **Severity** : Informational **Process**
Mar 12th 2019 21:54:03	ENV21\sauron	wscript.exe	336	3876	Persistence	**Product** : IOC **Alert** : IOC (154.16.201.93) **Severity** : Informational **Process**
Mar 12th 2019 21:54:03	ENV21\sauron	wscript.exe	336	3876	Persistence	File [**action type** = file create **AND name** = *.exe , *.scr , *.dll , *.sys , *.com , *.
Mar 12th 2019 21:54:05	ENV21\sauron	wscript.exe	336	1296	Exfiltration	**Product** : IOC **Alert** : IOC (154.16.201.93) **Severity** : Informational **Process**
Mar 12th 2019 21:54:05	ENV21\sauron	wscript.exe	336	1296	IOC	**Product** : IOC **Alert** : IOC (154.16.201.93) **Severity** : Informational **Process**
Mar 12th 2019 21:54:03	ENV21\sauron	wscript.exe	336	3876	Module Load	**Type** : Load **Load Path** : C:\Windows\System32\wscript.exe
Mar 12th 2019 21:54:03	ENV21\sauron	wscript.exe	336	3876	Module Load	**Type** : Load **Load Path** : C:\Windows\System32\ntdll.dll
Mar 12th 2019 21:54:03	ENV21\sauron	wscript.exe	336	3876	File Read	**Type** : File Read **Path** : C:\Windows\Temp\1.vbs

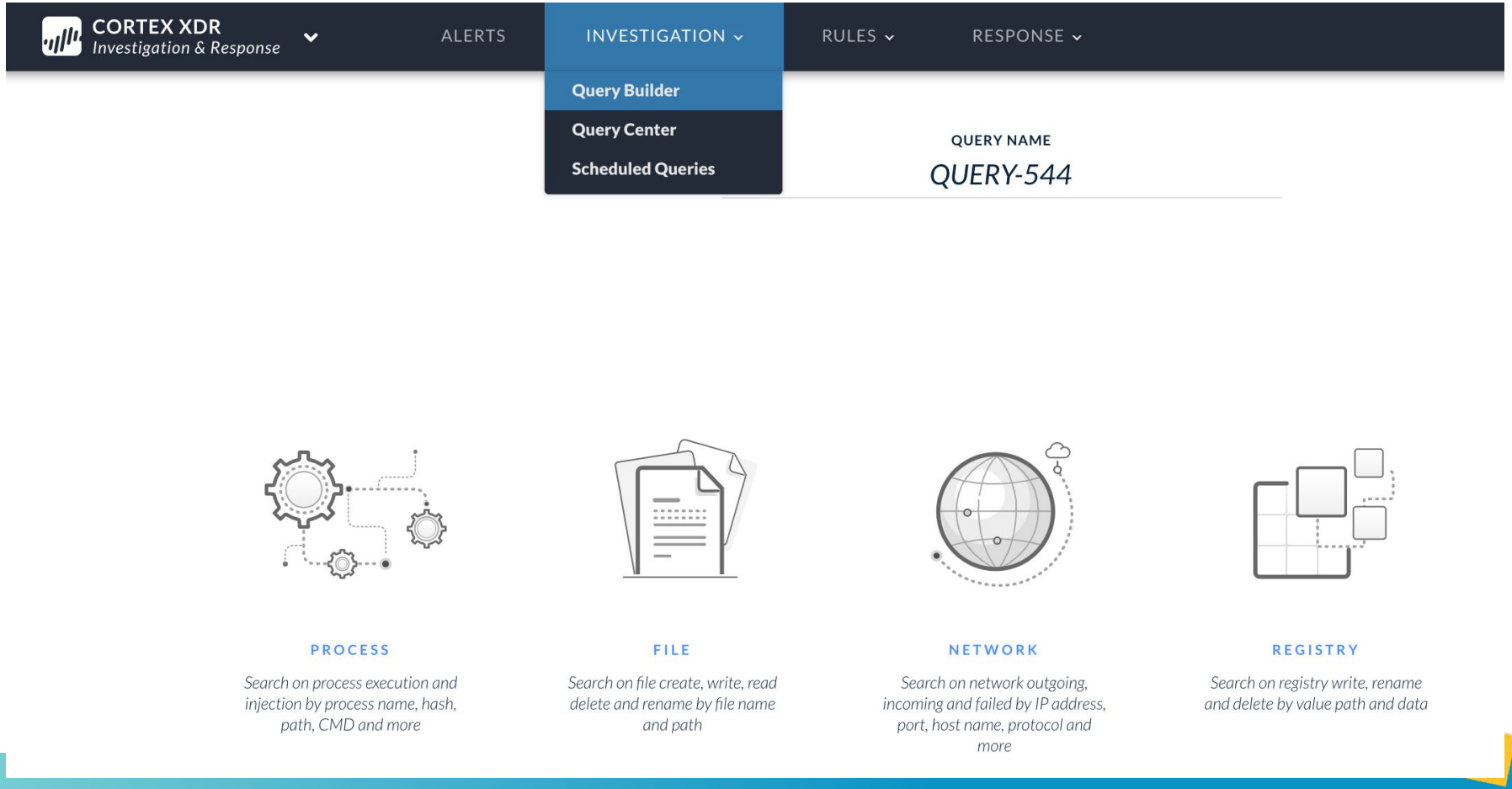
Detailed information – Files from 7zip

CORTEX XDR *Investigation & Response* | ALERTS | INVESTIGATION | RULES | RESPONSE | Mikkel Bossen

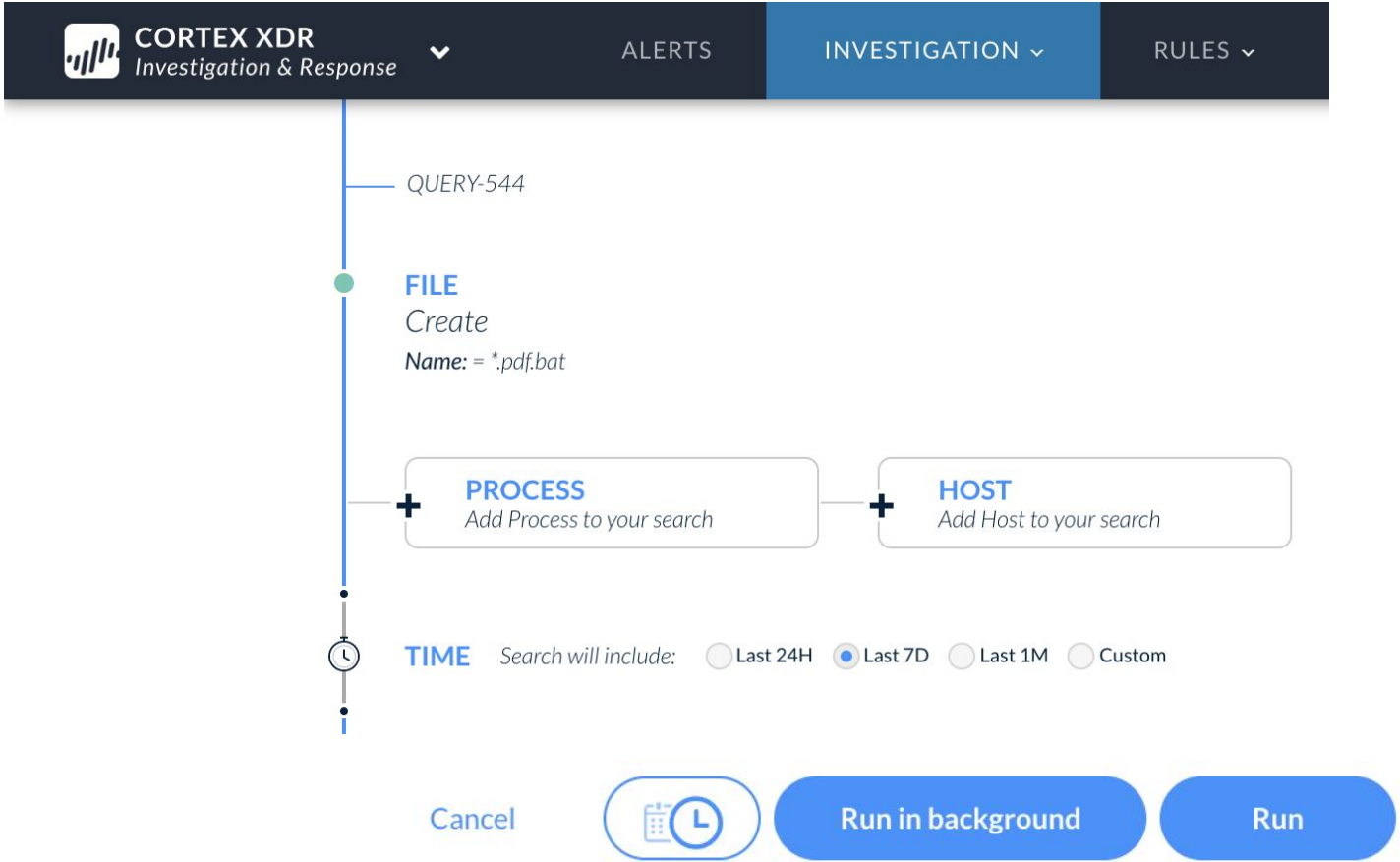
All 96 Results | Alert 1 Results | Process 1 Results | File 13 Results | Registry 5 Results | Module 76 Results | Filter

HOST NAME	HOST IP	USER NAME	HOST OS	ACTION TYPE	DESCRIPTION
PC13	10.201.113.143	ENV21\sauron	Windows	File Write	***Type** : File Write **Path** : C:\Windows\System32\en-US\msctf.dll.mui*
PC13	10.201.113.143	ENV21\sauron	Windows	File Read	***Type** : File Read **Path** : C:\Users\sauron\Downloads\RSU Grant Update.zip*
PC13	10.201.113.143	ENV21\sauron	Windows	File Write	***Type** : File Write **Path** : C:\Windows\System32\en-US\d2d1.dll.mui*
PC13	10.201.113.143	ENV21\sauron	Windows	File Read	***Type** : File Read **Path** : C:\Users\sauron\Downloads\RSU Grant Update.zip:Zone.Identifier*
PC13	10.201.113.143	ENV21\sauron	Windows	File Create	***Type** : File Create **Path** : C:\Users\sauron\AppData\Local\Temp\7zO06D338C4\RSU Grant Update.pdf.bat*
PC13	10.201.113.143	ENV21\sauron	Windows	File Write	***Type** : File Write **Path** : C:\Users\sauron\AppData\Local\Temp\7zO06D338C4\RSU Grant Update.pdf.bat*
PC13	10.201.113.143	ENV21\sauron	Windows	File Write	***Type** : File Write **Path** : C:\Users\sauron\AppData\Local\Temp\7zO06D338C4\RSU Grant Update.pdf.bat:Zone.Identifier*
PC13	10.201.113.143	ENV21\sauron	Windows	File Create	***Type** : File Create **Path** : C:\Users\sauron\AppData\Local\Temp\7zO06D338C4\RSU Grant Update.pdf.bat:Zone.Identifier*
PC13	10.201.113.143	ENV21\sauron	Windows	File Read	***Type** : File Read **Path** : C:\Users\sauron\AppData\Local\Temp\7zO06D338C4\RSU Grant Update.pdf.bat:Zone.Identifier*
PC13	10.201.113.143	ENV21\sauron	Windows	File Read	***Type** : File Read **Path** : C:\Users\sauron\AppData\Local\Temp\7zO06D338C4\RSU Grant Update.pdf.bat*
PC13	10.201.113.143	ENV21\sauron	Windows	File Read	***Type** : File Read **Path** : C:\Users\sauron\AppData\Local\Temp\7zO06D338C4\RSU Grant Update.pdf.bat*
PC13	10.201.113.143	ENV21\sauron	Windows	File Write	***Type** : File Write **Path** : C:\Windows\System32\en-US\shdocvw.dll.mui*
PC13	10.201.113.143	ENV21\sauron	Windows	File Write	***Type** : File Write **Path** : C:\Windows\winsxs\amd64_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.1*

Query Builder – looking for double extensions



Query Builder – looking for double extensions



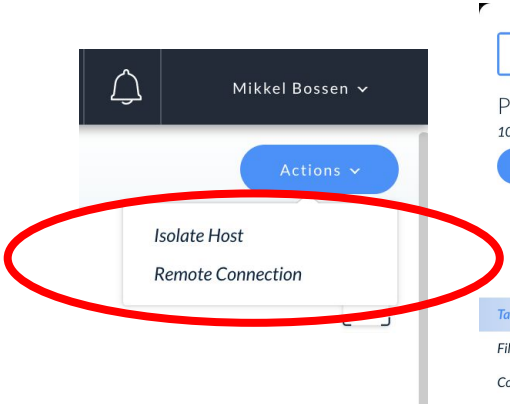
Query Builder – looking for double extensions

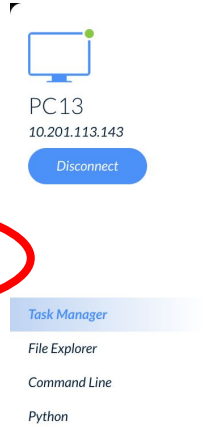
Results *Found 5 Results*

Export to file

TIMESTAMP	HOST NAME	HOST IP	USER NAME	HOST OS	ACTION TYPE	FILE NAME
Mar 12th 2019 21:53:50	PC13	10.201.113.143	ENV21\sauron	Windows	File Create	RSU Grant Update.pdf.bat
Mar 12th 2019 21:09:34	PC13	10.201.113.143	ENV21\sauron	Windows	File Create	RSU Grant Update.pdf.bat
Mar 12th 2019 14:39:48	PC13	10.201.113.143	ENV21\sauron	Windows	File Create	RSU Grant Update.pdf.bat
Mar 12th 2019 14:37:56	PC12	10.201.113.142	ENV21\galadriel	Windows	File Create	Some Band - Upcoming shows.pdf.bat
Mar 12th 2019 14:37:56	PC12	10.201.113.142	ENV21\galadriel	Windows	File Create	Some Band - Links to more songs.pdf.bat

Actions





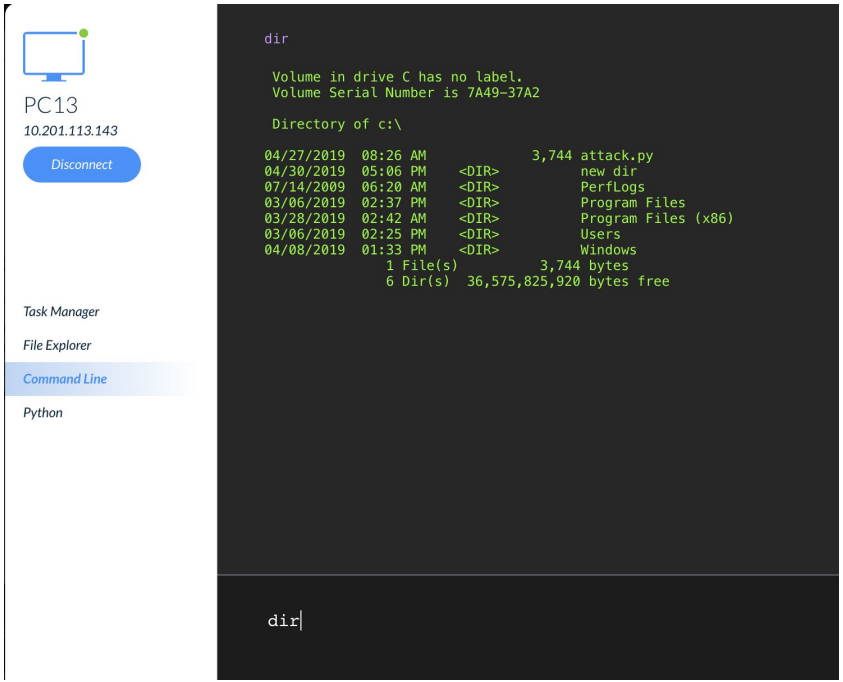
Filter results

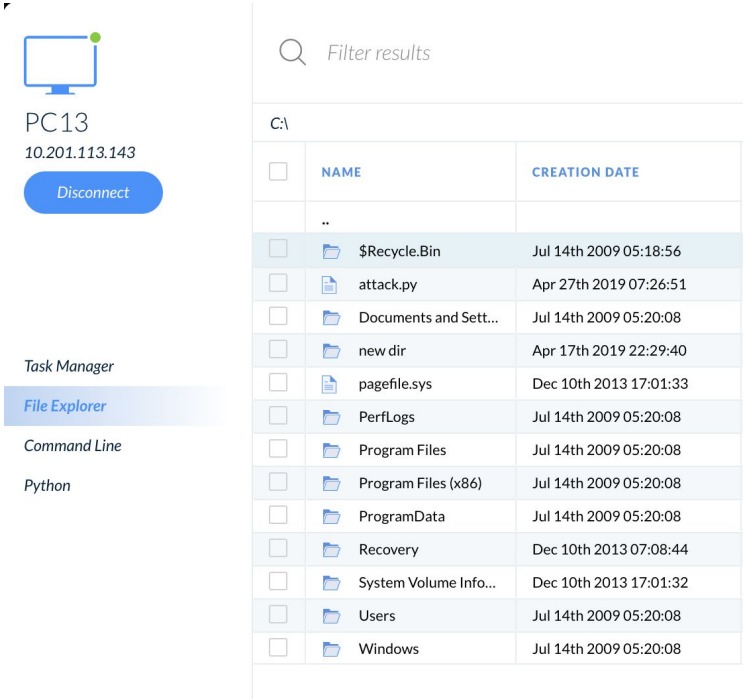
Export CSV

PROCESS HIERARCHY	PROCESS ID	PARENT ID	USER NAME	COMMAND LINE
System Idle Process	0		NT AUTHORITY\SYSTEM	
System	4	0	NT AUTHORITY\SYSTEM	
smss.exe	280	4	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
csrss.exe	372	364	NT AUTHORITY\SYSTEM	%SystemRoot%\system32\csrss.exe,ObjectDirectory=\Wind.
conhost.exe	444	372	ENV21\Administrator	\??\C:\Windows\system32\conhost.exe,-102351180432050..
wininit.exe	424	364	NT AUTHORITY\SYSTEM	wininit.exe
services.exe	528	424	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
svchost.exe	320	528	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe,-k,GPSvcGroup
svchost.exe	656	528	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe,-k,DcomLaunch
slui.exe	1632	656	ENV21\Sauron	C:\Windows\System32\slui.exe,-Embedding
WmiPrvSE.exe	2648	656	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\wbem\wmiprvse.exe
powershell.exe	872	2648	ENV21\Administrator	Powershell,-NoLogo,-NoProfile,-NonInteractive,-WindowStyl.
cortex-xdr.exe	1740	872	ENV21\Administrator	C:\Windows\Magnifier\lrc-414ebc490a\cortex-xdr.exe,-serv..
cortex-xdr.exe	2316	1740	ENV21\Administrator	C:\Windows\Magnifier\lrc-414ebc490a\cortex-xdr.exe,-serv..
svchost.exe	736	528	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe,-k,RPCSS
svchost.exe	824	528	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe,-k,LocalServiceNetwork...
svchost.exe	920	528	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe,-k,LocalSystemNetwork...
dwm.exe	2684	920	ENV21\Sauron	C:\Windows\system32\Dwm.exe
svchost.exe	956	528	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe,-k,LocalService
svchost.exe	992	528	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe,-k,netsvcs
svchost.exe	1080	528	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe,-k,NetworkService
spoolsv.exe	1204	528	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe

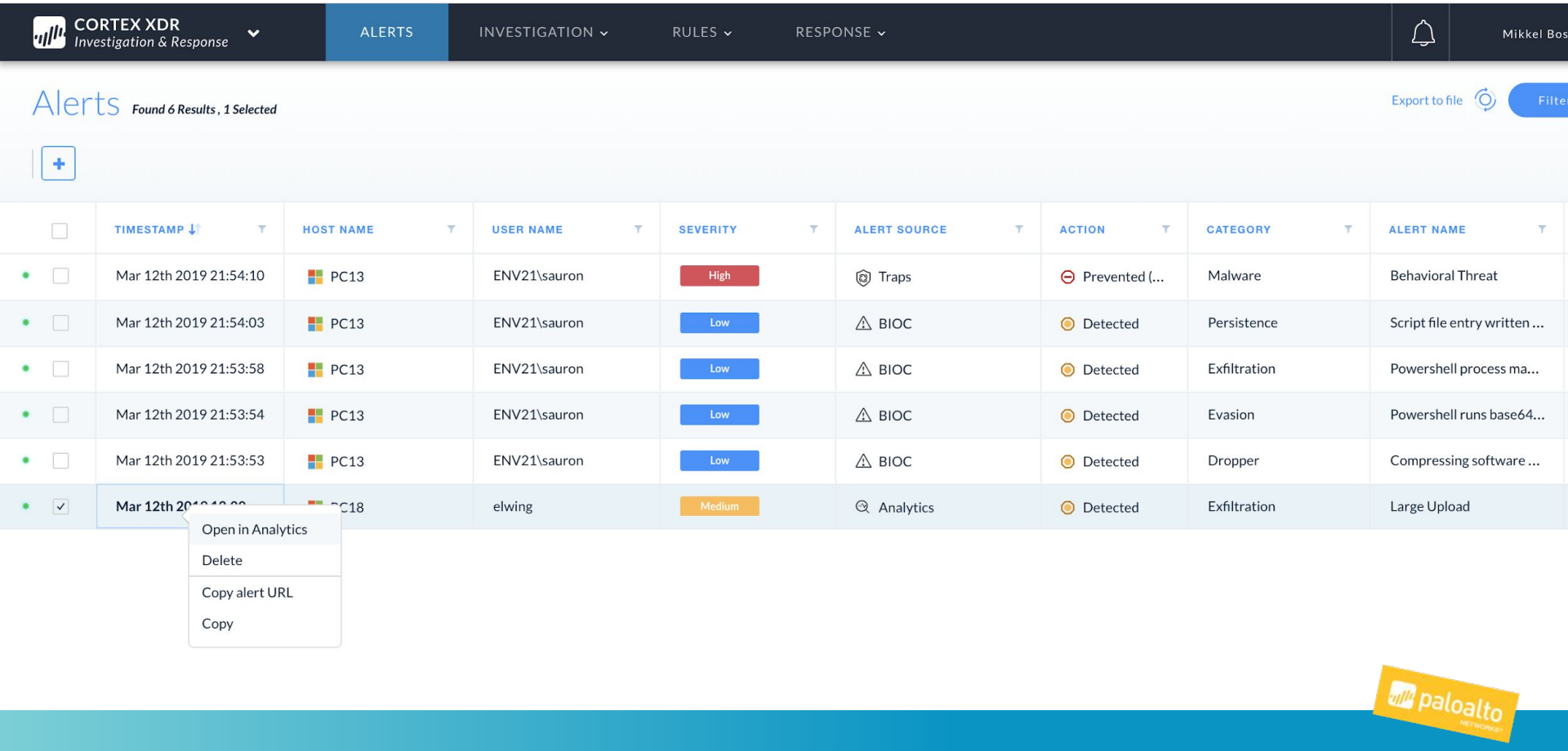
Showing 46 processes

Command Line

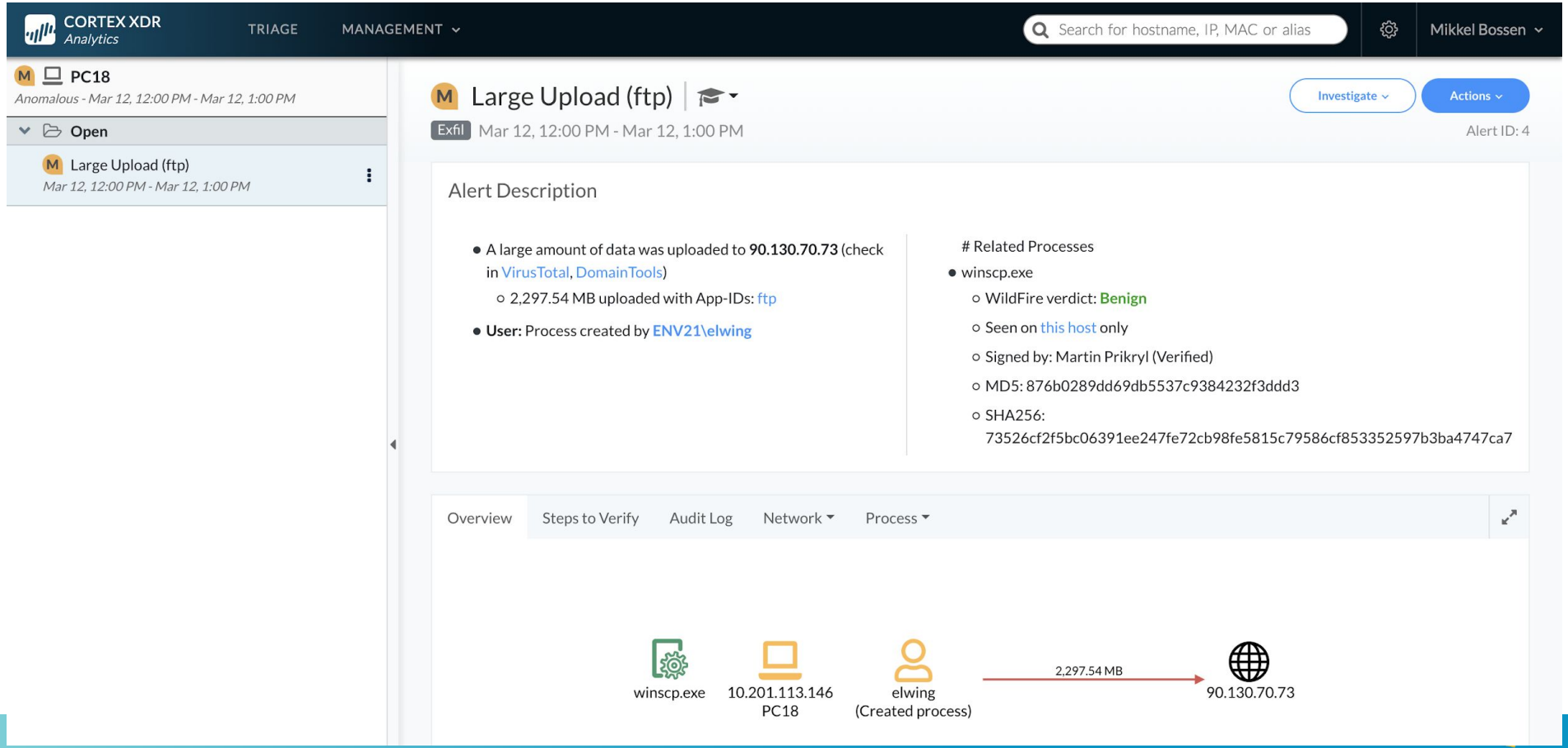




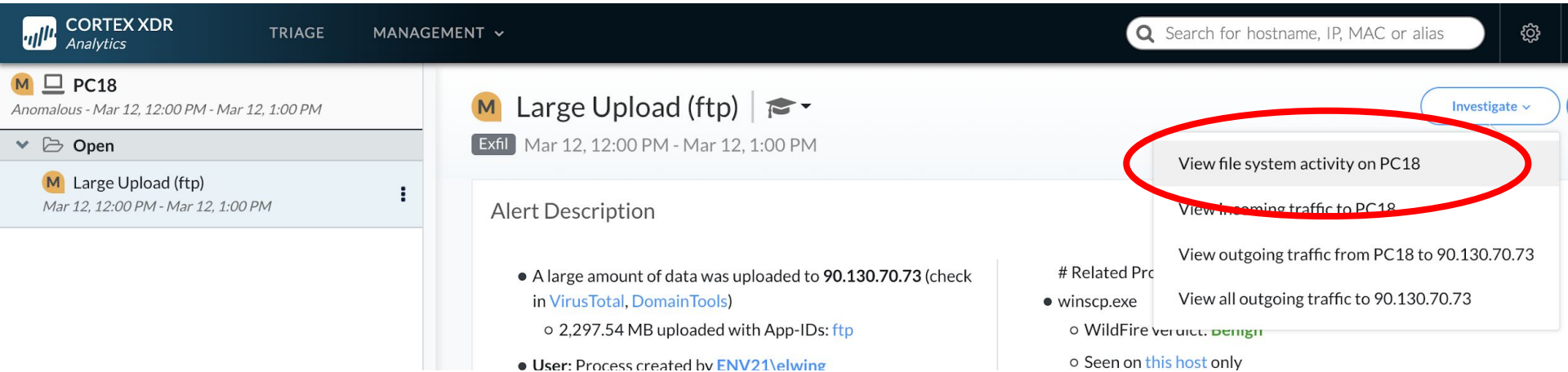
Network Behavior Alert – Large Upload



Large Upload – FTP



View File System Activity



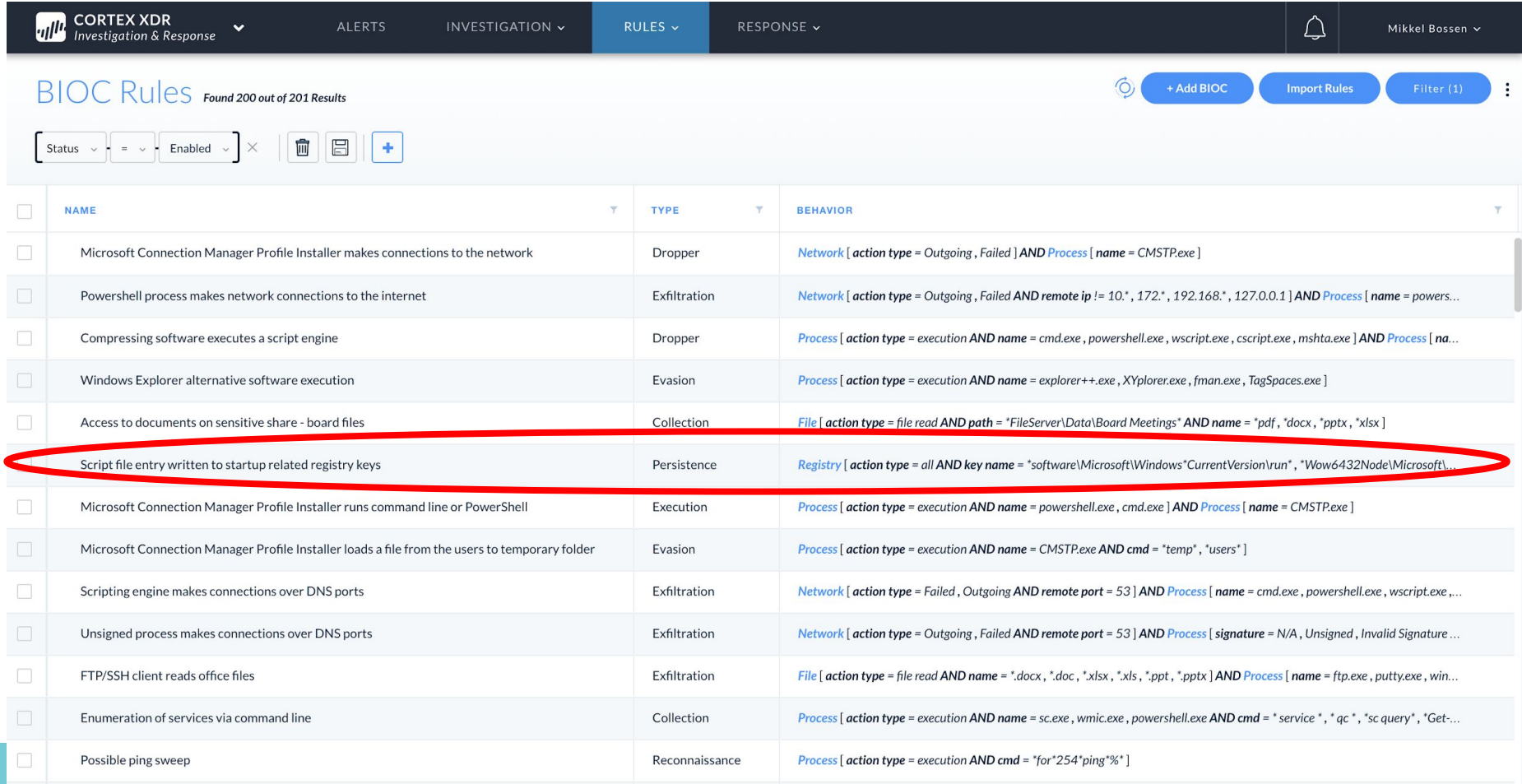
Location the ZIP file and Identifying Content

Results *Found 507 Results*

Export to file | Filter

ACTION TYPE	FILE NAME	FILE PREVIOUS NAME	FILE PATH
File Rename	Data.zip	Data.zip.tmp	C:\Users\elwing\Desktop\Data.zip
File Read	XDR Beta Feedback Review.pptx		\\10.201.112.10\FileServer\Data\Product\XDR\XDR Beta Feedback Review.pptx
File Read	Upcoming XDR Screens Design.xlsx		\\10.201.112.10\FileServer\Data\Product\XDR\Upcoming XDR Screens Design.xlsx
File Read	Upcoming XDR Features.xlsx		\\10.201.112.10\FileServer\Data\Product\XDR\Upcoming XDR Features.xlsx
File Read	Or's Plan to Take Over the World (better than Hadar's plan).docx		\\10.201.112.10\FileServer\Data\Product\XDR\Or's Plan to Take Over the World (better than Hadar's pl
File Read	Hadar's Plan to Take Over the World.pptx		\\10.201.112.10\FileServer\Data\Product\XDR\Hadar's Plan to Take Over the World.pptx
File Read	New Prevention Patent #2.docx		\\10.201.112.10\FileServer\Data\Product\Traps\New Prevention Patent #2.docx
File Read	Transactions.mdf		\\10.201.112.10\FileServer\Data\Databases\MSSQL\BizTech\Transactions.mdf
File Read	Nov5th 2018.pdf		\\10.201.112.10\FileServer\Data\Board Meetings\PANW Board Meeting Minutes\Nov5th 2018.pdf
File Read	Mar4th 2018.pdf		\\10.201.112.10\FileServer\Data\Board Meetings\PANW Board Meeting Minutes\Mar4th 2018.pdf
File Write	UsrClass.dat		C:\Users\elwing\AppData\Local\Microsoft\Windows\UsrClass.dat
File Write	UsrClass.dat.LOG1		C:\Users\elwing\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
File Read	Jan7th 2019.pdf		\\10.201.112.10\FileServer\Data\Board Meetings\PANW Board Meeting Minutes\Jan7th 2019.pdf
File Read	Dec3rd 2018.pdf		\\10.201.112.10\FileServer\Data\Board Meetings\PANW Board Meeting Minutes\Dec3rd 2018.pdf
File Write	Data.zip.tmp		C:\Users\elwing\Desktop\Data.zip.tmp

BIOCs


CORTEX XDR
Investigation & Response
ALERTS
INVESTIGATION
RULES
RESPONSE
Mikkel Bossen
BIOC Rules
Found 200 out of 201 Results
+ Add BIOC
Import Rules
Filter (1)
Status
=
Enabled
NAME
TYPE
BEHAVIOR
Microsoft Connection Manager Profile Installer makes connections to the network
Dropper
Network [action type = Outgoing , Failed] AND Process [name = CMSTP.exe]
Powershell process makes network connections to the internet
Exfiltration
Network [action type = Outgoing , Failed AND remote ip != 10.* , 172.* , 192.168.* , 127.0.0.1] AND Process [name = powers...
Compressing software executes a script engine
Dropper
Process [action type = execution AND name = cmd.exe , powershell.exe , wscript.exe , cscript.exe , mshta.exe] AND Process [na...
Windows Explorer alternative software execution
Evasion
Process [action type = execution AND name = explorer++.exe , XYplorer.exe , fman.exe , TagSpaces.exe]
Access to documents on sensitive share - board files
Collection
File [action type = file read AND path = *FileServer\Data\Board Meetings* AND name = *pdf , *docx , *pptx , *xlsx]
Script file entry written to startup related registry keys
Persistence
Registry [action type = all AND key name = *software\Microsoft\Windows*CurrentVersion\run* , *Wow6432Node\Microsoft\...
Microsoft Connection Manager Profile Installer runs command line or PowerShell
Execution
Process [action type = execution AND name = powershell.exe , cmd.exe] AND Process [name = CMSTP.exe]
Microsoft Connection Manager Profile Installer loads a file from the users to temporary folder
Evasion
Process [action type = execution AND name = CMSTP.exe AND cmd = *temp* , *users*]
Scripting engine makes connections over DNS ports
Exfiltration
Network [action type = Failed , Outgoing AND remote port = 53] AND Process [name = cmd.exe , powershell.exe , wscript.exe ,...
Unsigned process makes connections over DNS ports
Exfiltration
Network [action type = Outgoing , Failed AND remote port = 53] AND Process [signature = N/A , Unsigned , Invalid Signature ...
FTP/SSH client reads office files
Exfiltration
File [action type = file read AND name = *.docx , *.doc , *.xlsx , *.xls , *.ppt , *.pptx] AND Process [name = ftp.exe , putty.exe , win...
Enumeration of services via command line
Collection
Process [action type = execution AND name = sc.exe , wmic.exe , powershell.exe AND cmd = * service * , * qc * , *sc query* , *Get-...
Possible ping sweep
Reconnaissance
Process [action type = execution AND cmd = *for*254*ping*%*]

Thank You

See and Learn more @ Our Booth

Email: mbossen@paloaltonetworks.com