Audit Service

Guides for Users and Partners

panda
a WatchGuard brand

AD360 als Audit Service und Türöffner

Dieses Konzept soll dazu dienen, Adaptive 360 nicht mehr als reines Verdrängungsprodukt gegenüber anderen an den Kunden/Partner zu bringen, sondern auf Grund der parallelen Funktionalität als Audit Service zu platzieren.

Es ist auch wichtig, dass hier von Adaptive Defense 360 und nicht dem reinen Adaptive Defense gesprochen wird. Vorteile bei diesem Szenario sind, dass das TrayIcon für mögliche Optionen/Interaktionen gegeben ist und ein schnelles Umschalten in den effektiven Modus vorbereitet ist.

Das Konzept:

In den AD360 Modulen bietet sich eine Vielzahl von Möglichkeiten Security as a Service anzubieten und dieses bereits ohne großen Aufwand. Der Schritt hin zu einem anderen Antivirus oder EDR-Lösung ist für viele sehr vorsichtig zu betrachten, da man ja alles neuinstallieren müsste, nicht weiß ob es problemlos funktioniert oder möglicherweise auch nicht zwingend besser ist.

Aus diesem Grund wird AD360 ergänzend zur bestehenden Infrastruktur installiert und lediglich Informationen gesammelt wie der Status der Endpoints und des Netzwerkes ist. Auf Basis dessen können nächste Entscheidungen getroffen werden und im schlechtesten Fall ein gutes und günstiges Audit durchgeführt worden sein.

Einsatzszenarios:

WatchGuard -> Potenzieller Partner -> Potenzieller Kunde
WatchGuard -> Potenzieller Kunde

Bestehender Partner -> Bestehender Kunde
Bestehender Partner -> Potenzieller Kunde

Platzierung:

Ein Audit Service bietet für Kunden/Partner einen wesentlichen Mehrwert, um einerseits seine Compliance zu prüfen, andererseits eine vertrauenswürdige Umgebung zu schaffen. Zudem ist es nicht annähernd so teuer wie ein Penetrationstest und zielt auch gar nicht ab diesen zu ersetzen. Wir möchten lediglich einen schnellen und unkomplizierten Überblick bieten, um mögliche Lücken aufzudecken und fragwürdige Verhalten innerhalb des Netzwerks zu klären.

Vorbereitung:

Zum Erstgespräch oder auch als Folgegespräche sollte das **Audit Service Modell** vorgestellt werden, da dieses für das Ziel einerseits **kostenfrei** durch die Trials erzeugt werden kann und andererseits für dieses einen geringen Verwaltungs- und Einführungsaufwand bedeutet.

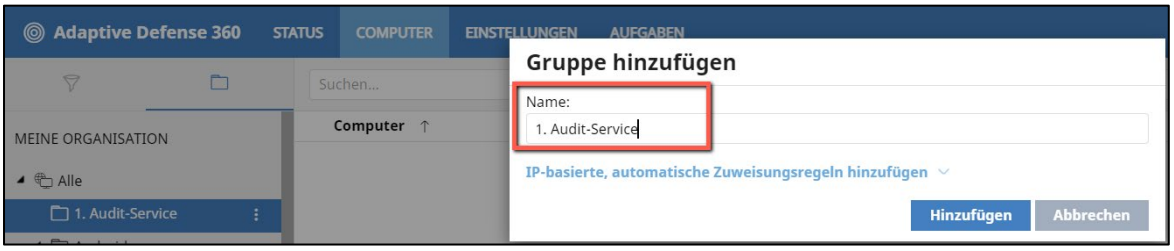
Anschließend wird eine Demo-Account erstellt, in dem die folgenden Produkte ergänzend zu **Adaptive Defense 360** freigeschaltet werden:

- Verschlüsselung
- Patch Management
- Data Control
- Advanced Reporting Tool

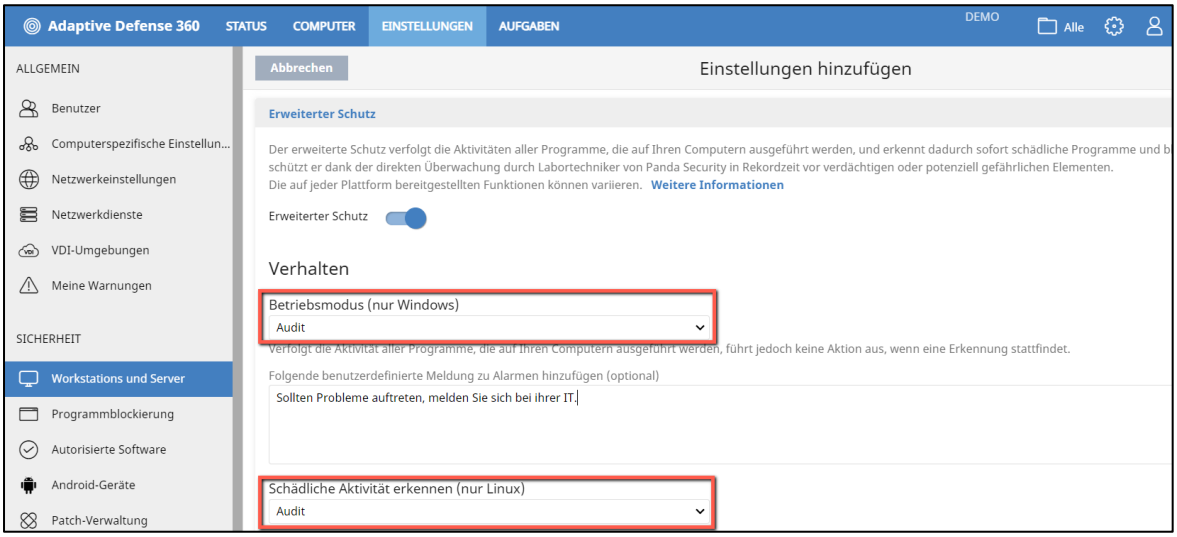
Bei bestehenden Kunden und Partnern mit Endpoint Protection oder Adaptive Defense 360 werden die entsprechenden Module als Trials aufgebucht.

Im Anschluss werden folgende Einstellungen in der Console getroffen:

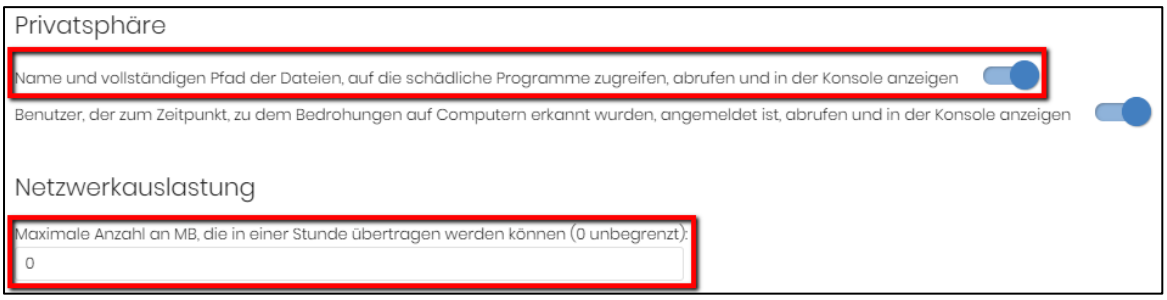
1. Anlegen einer Gruppe **Audit-Service.**



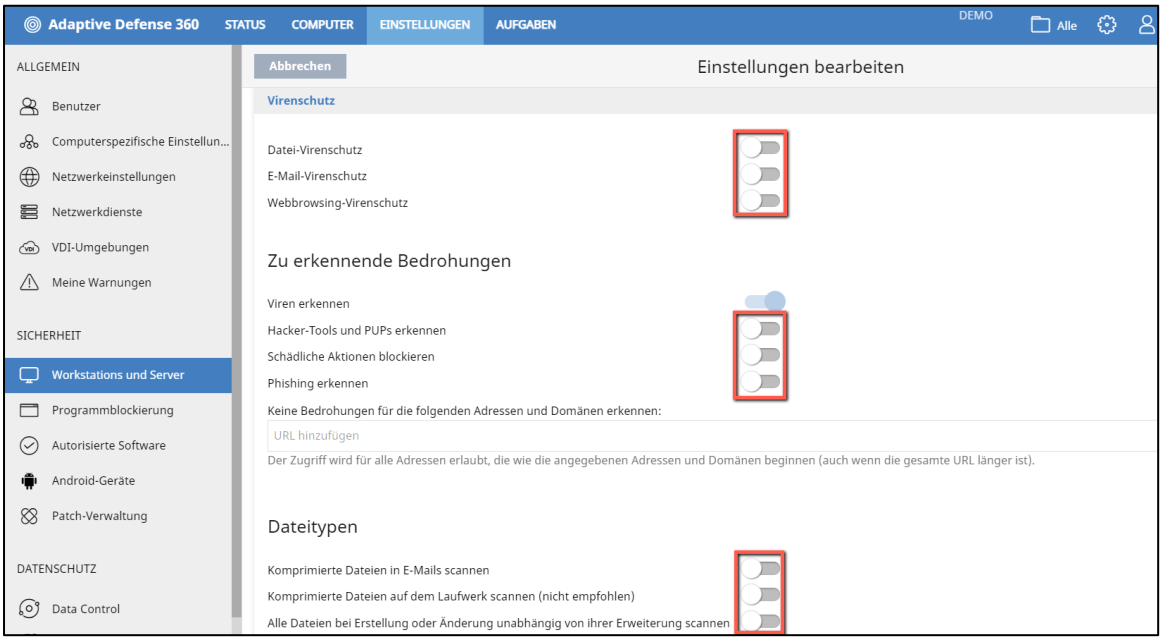
2. Erstellen eines Sicherheitsprofiles **Audit-Service,** in dem lediglich der erweiterte Schutz im *Audit-Modus* und aktiv ist und *Anti-Exploit* auf Prüfen steht.



3. Des Weiteren werden der *vollständige Pfad* angezeigt und die *Netzwerkauflastung* auf *0* gesetzt. Lediglich bei sehr schwachen Internetanbindungen sollte diese limitiert werden!

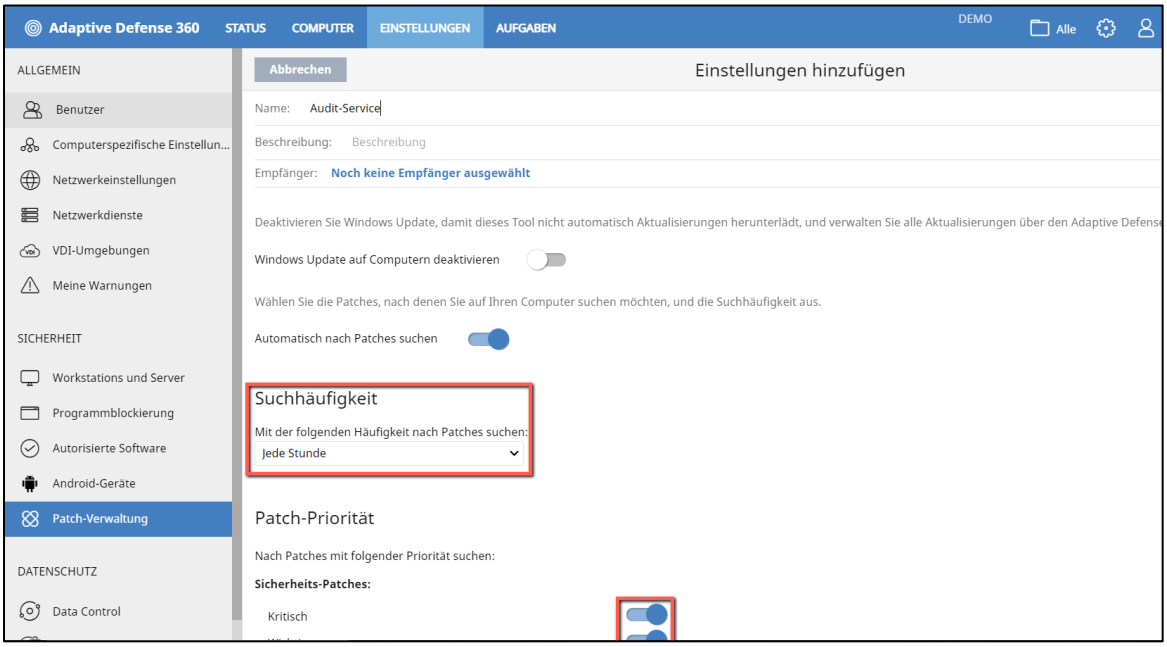


4. Im nächsten Schritt werden die Virenschutz-Komponenten ausgeschaltet, um ein mögliches Problem mit dem bestehenden Antivirus zu umgehen.

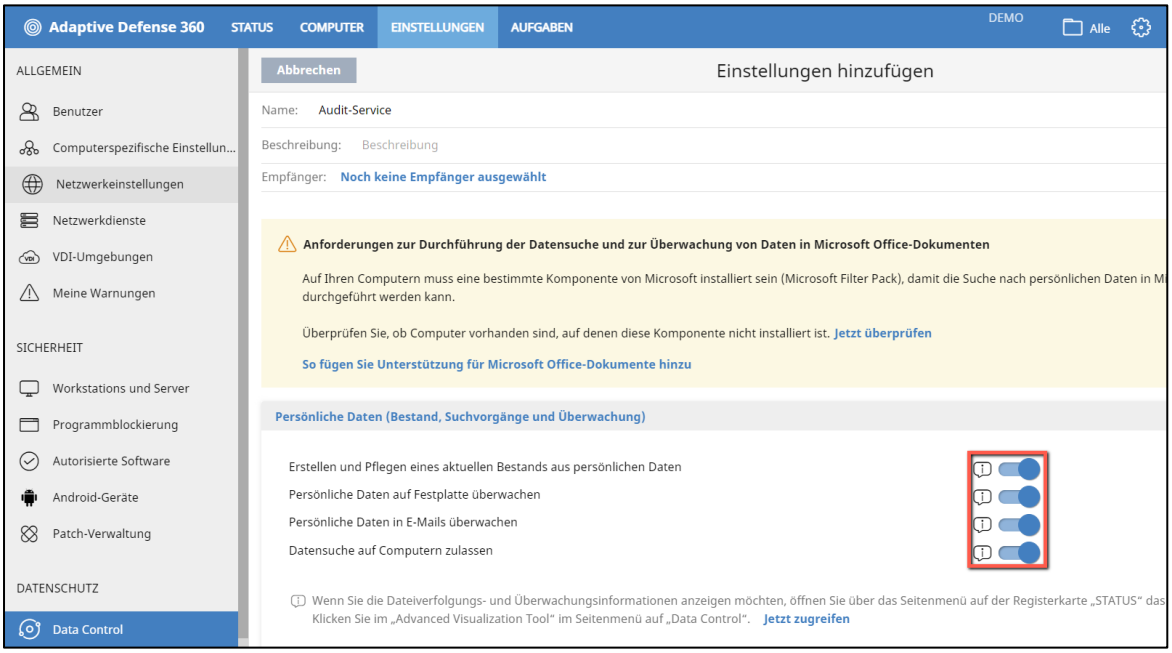


Wichtig: Die weiteren Einstellungen unter **Workstations und Server** können beibehalten werden, da diese bereits deaktiviert sind.

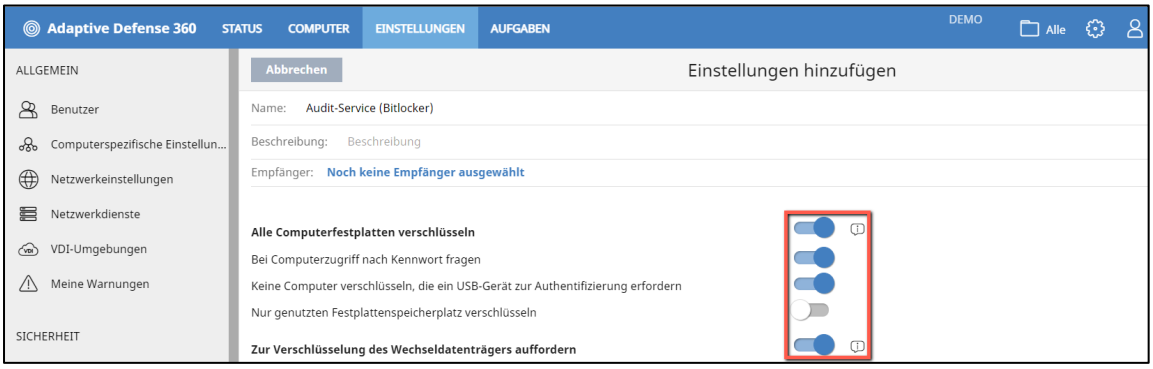
5. Erstellen Sie eine neues Einstellungsprofil für die Patch-Verwaltung mit dem Namen **Audit-Service** und setzen die *Suchhäufigkeit* auf jede Stunde.



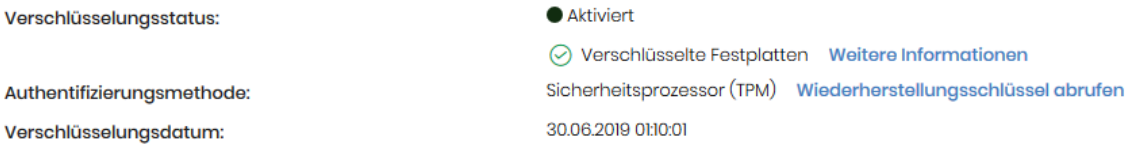
6. In den Einstellungen Sensible Daten erstellen Sie ebenfalls ein **Audit-Service** Profil und aktivieren alle 4 Optionen. Das Microsoft Filter Pack ist in der Regel ab Outlook 2013 über die Windows Updates bereits installiert worden. Andernfalls werden alle Geräte ohne dieses aufgelistet, aber nicht die entsprechenden Office-Dokumente analysiert.



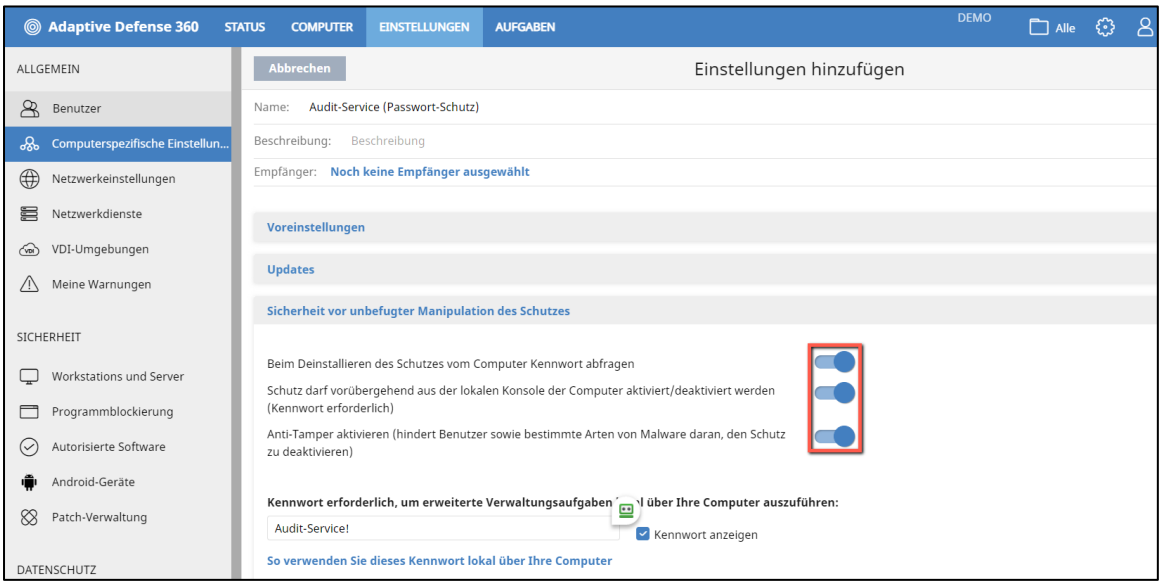
7. **Optional**: Haben Sie Laptops oder andere PCs mit personenbezogenen Daten, die sehr schützenswert sind, können Sie diese mit der Bitlocker-Version von Microsoft direkt aus der Konsole verschlüsseln.



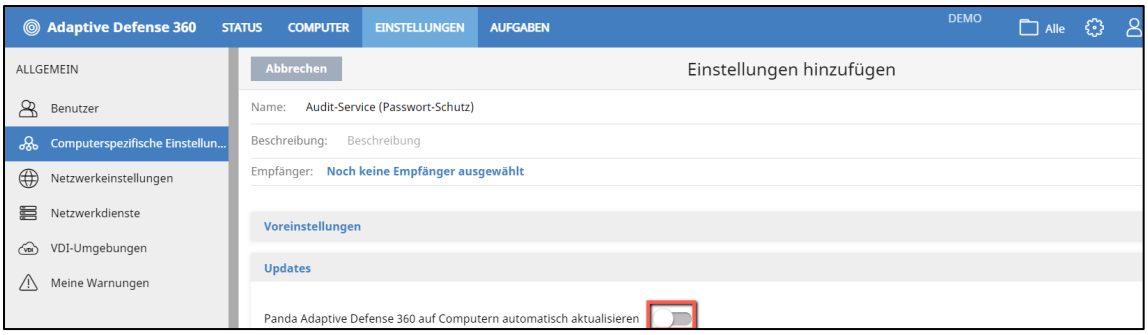
Wichtig: Bewahren Sie den Schlüssel gut auf oder entschlüsseln Sie die Maschinen vorm Ablauf der Testlaufzeit wieder, damit Ihnen der Schlüssel nicht fehlt und die Maschinen verwaltbar bleiben.
Die Informationen finden Sie direkt in den Details des Computers.



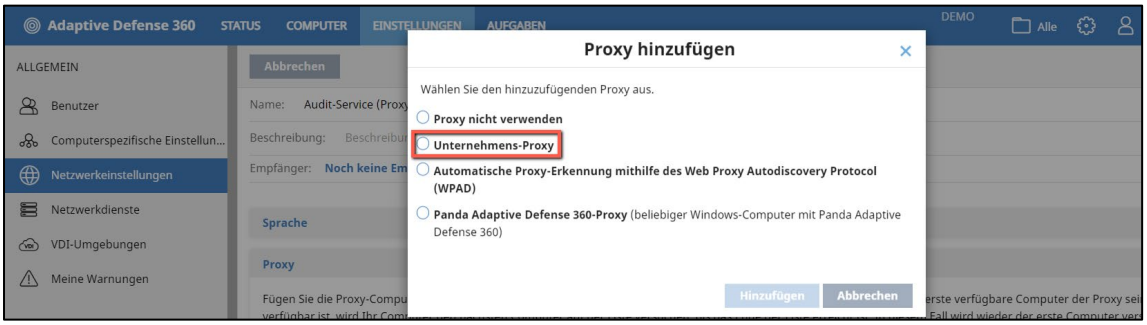
8. Als nächstes sollte zwingend ein Passwort-Schutz etabliert werden, damit unser Audit-Service gegenüber dritten und Malware unverändert bleiben kann.



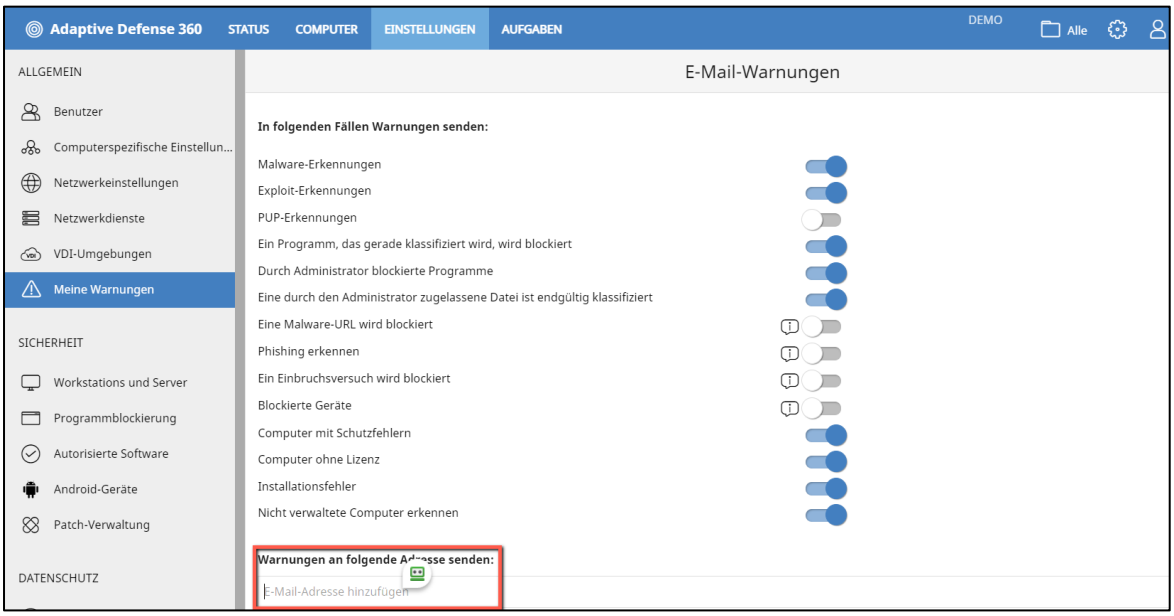
9. **Optional:** In manchen Server-/Client-Landschaften möchte man im Produktivbetrieb nicht existent auffallen. Hier sollte die automatische Schutzaktualisierung zunächst deaktiviert bleiben.



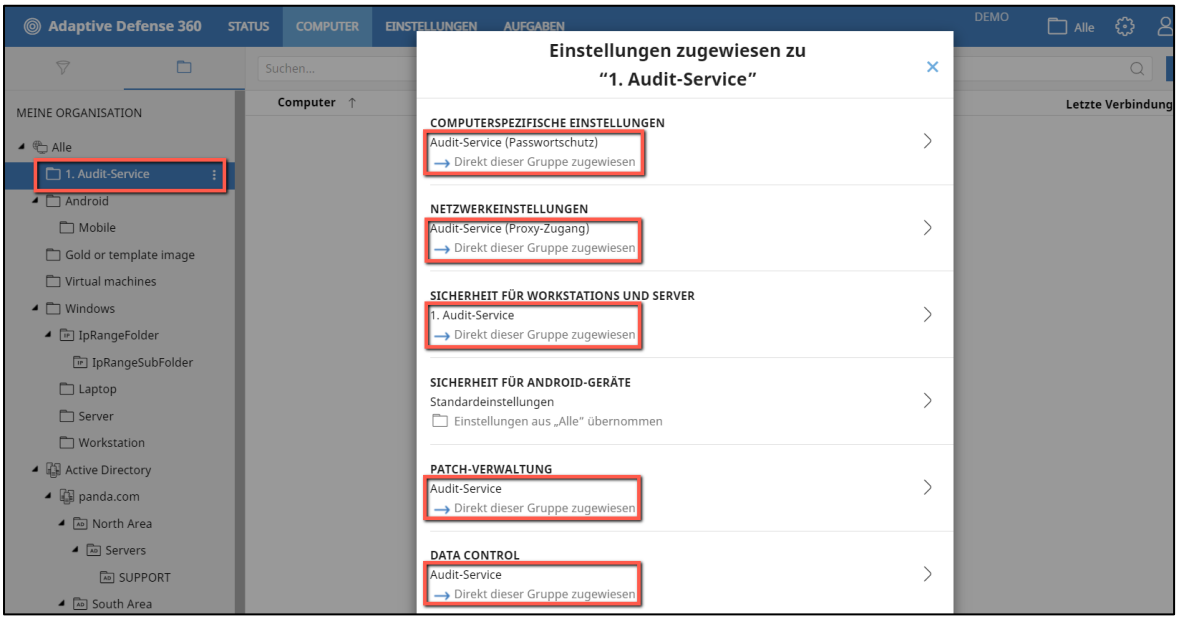
10. **Optional:** Ist ein Proxy im Unternehmen vorhanden, sollte auch dieser für eine einwandfreie Kommunikation bei uns hinterlegt werden:



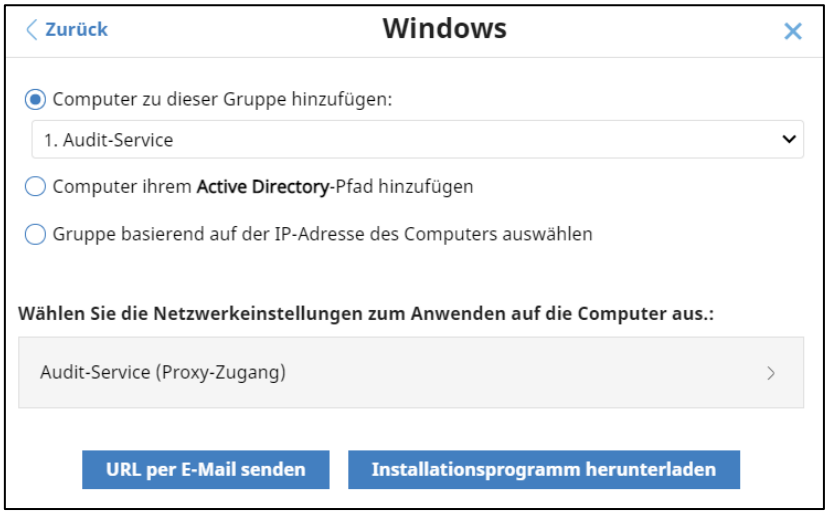
11. **Optional:** Bei Bedarf können die Warnungen per Mail auch deaktiviert werden, sofern nur ein endgültiger Report durchgeführt wird.



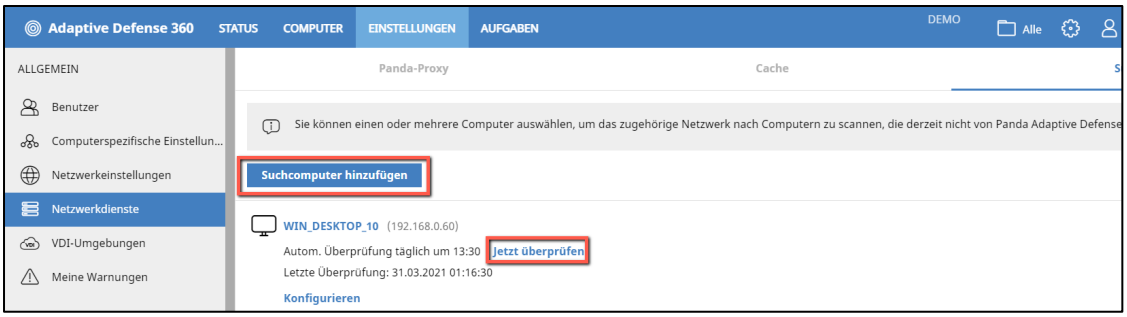
12. Im Anschluss werden nun der **Gruppe Audit-Service** über die 3 Punkte die entsprechenden Module zugewiesen:

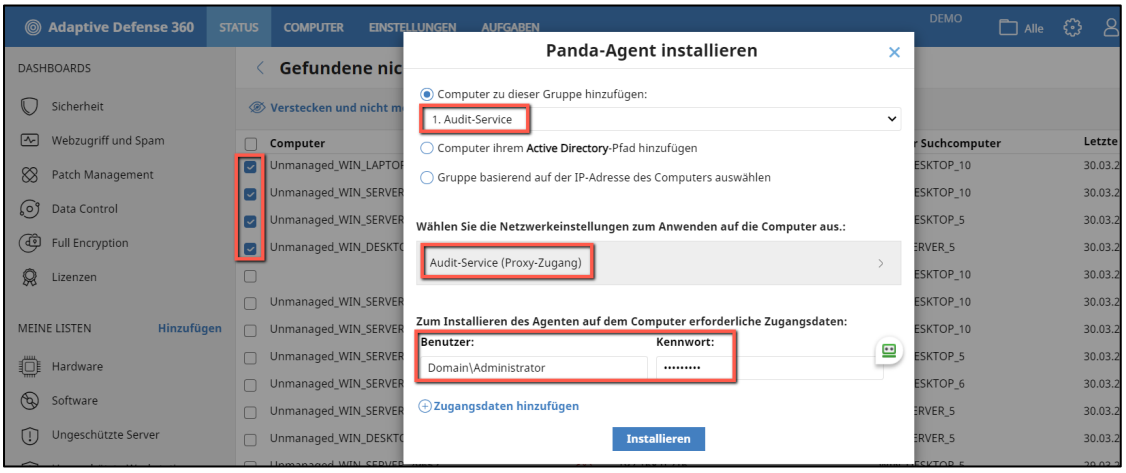


13. Im letzten Schritt wird der fertige Agent über **Computer hinzufügen** erstellt und kann dem Ziel bereitgestellt werden:



14. **Optional:** Zum vereinfachten Verteilen kann auch ein Suchcomputer definiert werden, der anschließend den Agenten mit Domänen-Administratoren an die anderen PCs versucht zu pushen. Hierzu muss lediglich ein Agent beim Ziel manuell installiert werden und diese Suche durchführen.





Audit-Zeitraum:

Wir empfehlen den Audit-Zeitraum nach den Installationen auf den Endpoints zunächst auf eine Länge von 2 Wochen zu definieren. In einer Regel-Umgebung sollte dieses ausreichen, um die Prozesse und deren Verhalten kennen zu lernen und zu bewerten. Sollten mehrere Standorte existieren oder ein Deployment nicht zu schnell realisierbar sein, kann der Zeitraum auch auf 3-4 Wochen erhöht werden.

Beachten: Nach der Erst-Installation kann der Agent etwas mehr Leistung des CPUs für einen Zeitraum von 30-90 Minuten in Anspruch nehmen. In dieser Zeit erstellt dieser den lokalen Index über alle von uns klassifizierten Dokumente mit personenbezogenem Inhalt.
Auf Clients der heutigen Generationen fällt dieses jedoch kaum auf.

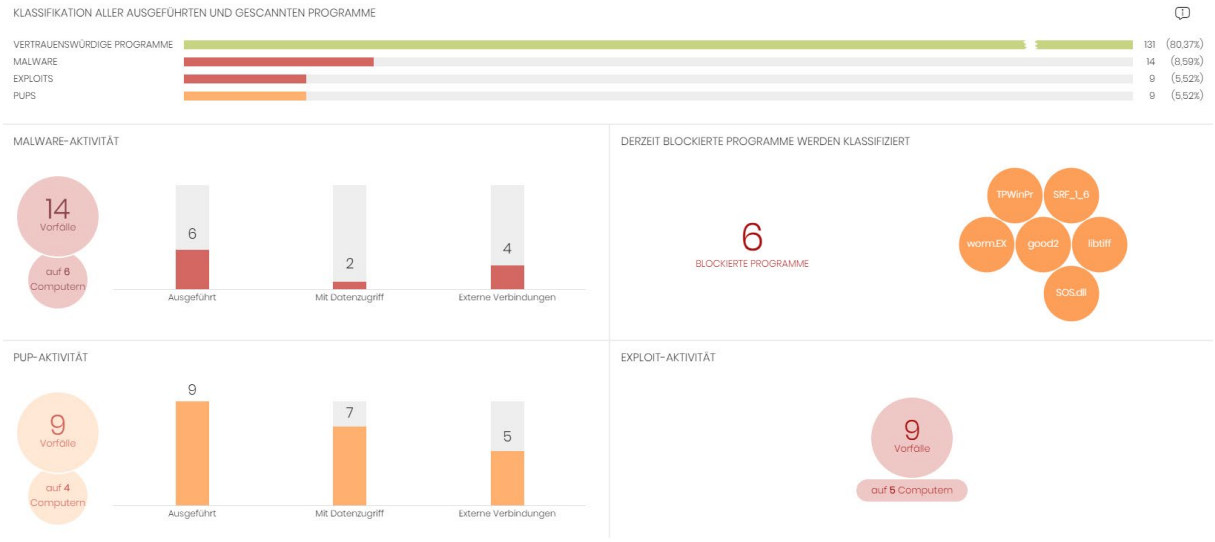
Auswertungen nach dem Audit-Zeitraum:

Nach dem Audit-Zeitraum geht an den Schritt die gesammelten Informationen auszuwerten. Hierbei ist es wichtig zunächst nicht jedes kleine Detail auseinander zu nehmen, sondern die schnell zu erkennenden Erkenntnisse zu deuten.
Aus diesem Grund unterteilen wir die Auswertung in 3 verschiedene Grade:

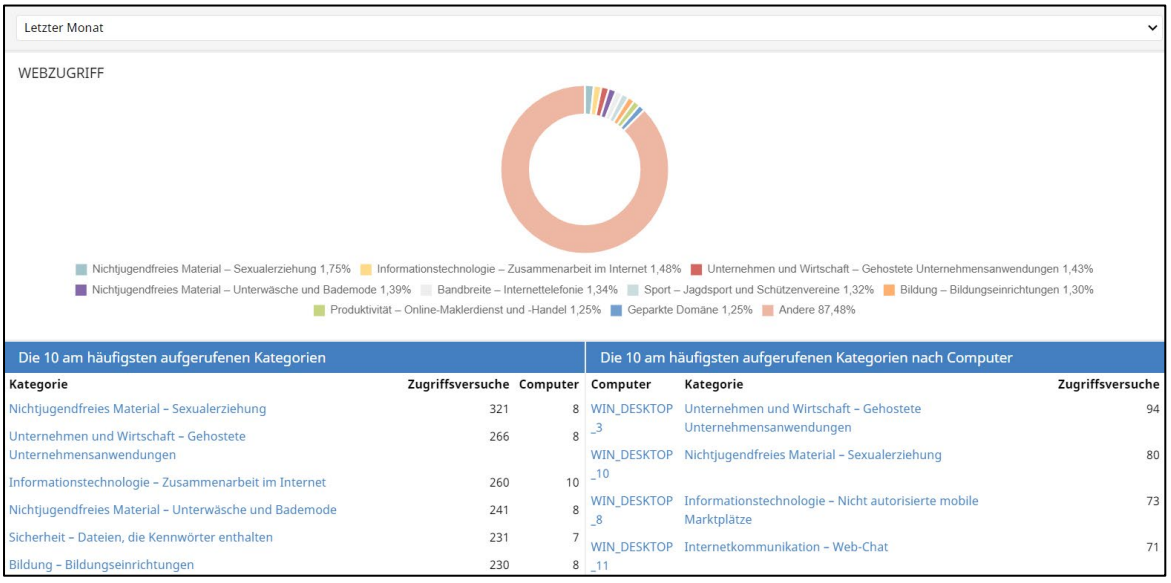
- Basic
- Advanced
- Expert

Basic Auswertung:

- Überprüfen der Exploits, PUPs und Malware (auch im Verlauf)



- Surfverhalten der User prüfen und einstufen (Privates Surfen, Compliance-Verletzungen)



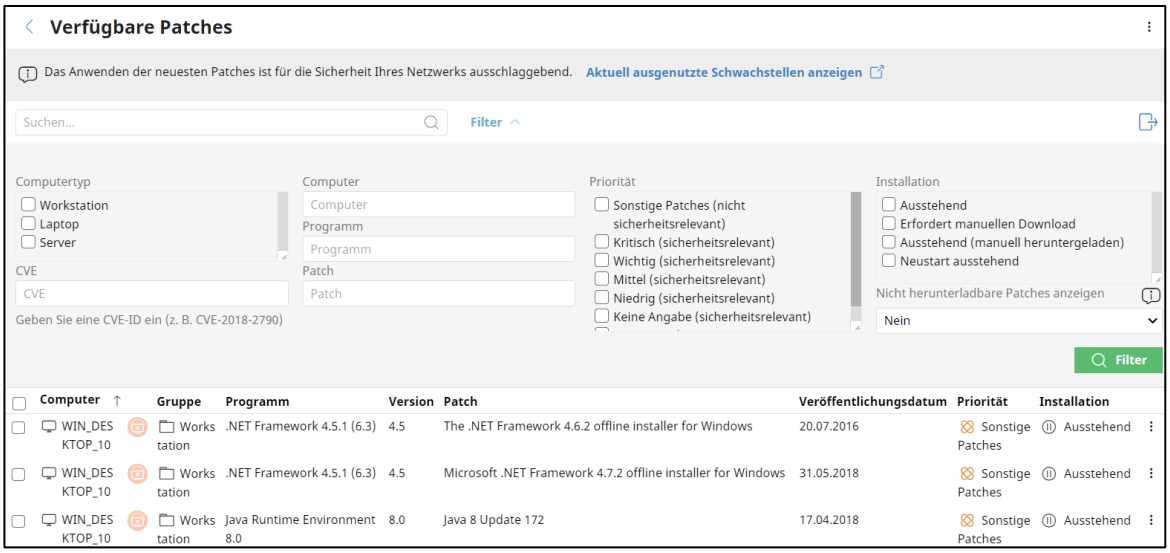
Die 10 am häufigsten aufgerufenen Kategorien

Kategorie	Zugriffsversuche	Computer
Nichtjugendfreies Material – Sexualerziehung	321	8
Unternehmen und Wirtschaft – Gehostete Unternehmensanwendungen	266	8
Informationstechnologie – Zusammenarbeit im Internet	260	10
Nichtjugendfreies Material – Unterwäsche und Bademode	241	8
Sicherheit – Dateien, die Kennwörter enthalten	231	7
Bildung – Bildungseinrichtungen	230	8

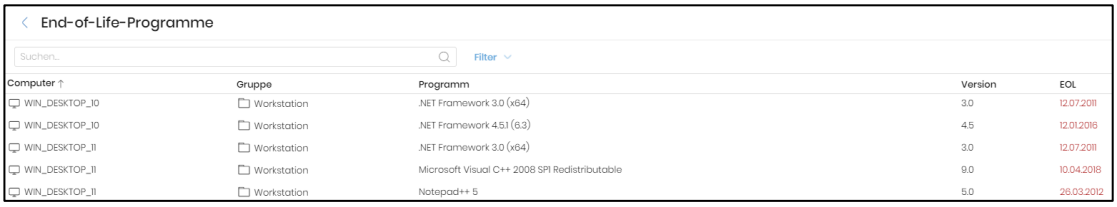
Die 10 am häufigsten aufgerufenen Kategorien nach Computer

Computer	Kategorie	Zugriffsversuche
WIN_DESKTOP_3	Unternehmen und Wirtschaft – Gehostete Unternehmensanwendungen	94
WIN_DESKTOP_10	Nichtjugendfreies Material – Sexualerziehung	80
WIN_DESKTOP_8	Informationstechnologie – Nicht autorisierte mobile Marktplätze	73
WIN_DESKTOP_11	Internetkommunikation – Web-Chat	71

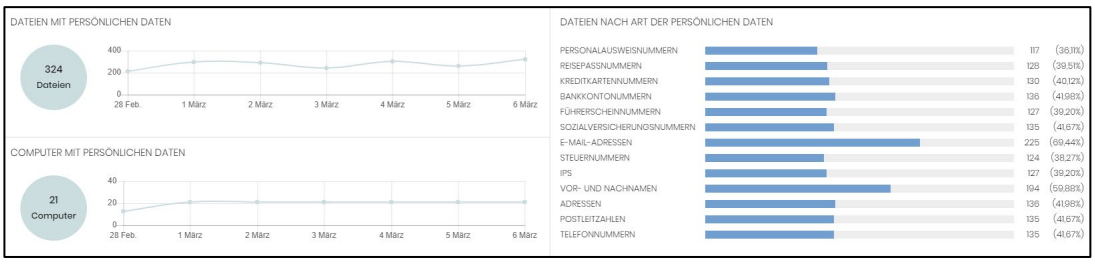
- Patch-Stand des Unternehmens bewerten
  - Allgemeine Anzahl an fehlenden Patches Workstations/Server
  - Kritische Programme, wie Adobe, Java, Office, Internet Browser
  - Wie viele Sicherheitsrelevante Patches fehlen



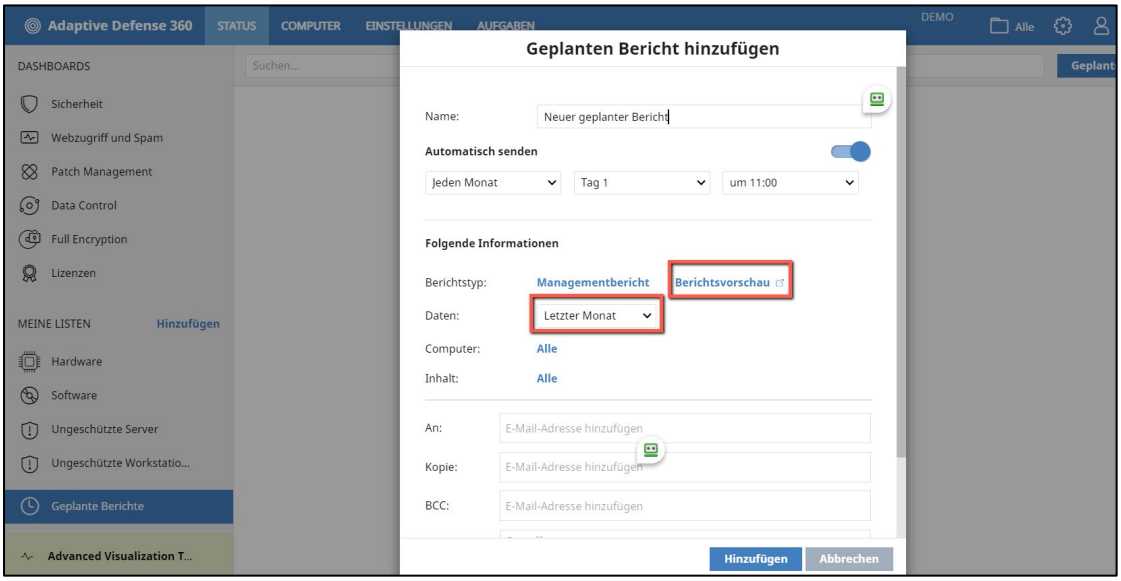
- End-Of-Life Programme, die nach und nach abgelöst werden sollte



- Übersicht der Personenbezogene Dateien verifizieren
  - Wie viele Dateien sind gesamt gefunden worden?
  - Gibt es PCs, die exorbitant viele Dateien mit PII beherbergen
  - Werden diese aktuell in irgendeiner Methode kontrolliert und gegen Diebstahl geschützt?
  - Mit der Computersuche explizite Dateien suchen und prüfen



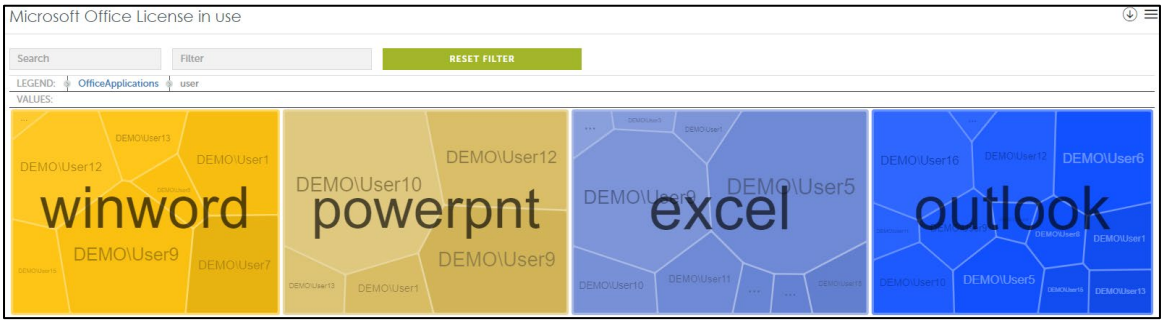
- Bericht erstellen inklusive Erkennungen, Webzugriff und Spam



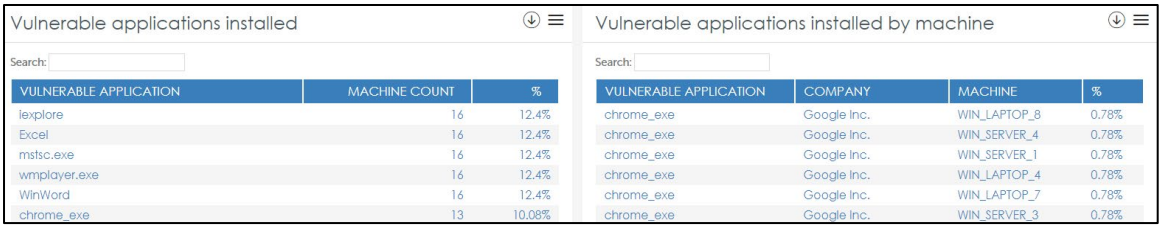
Advanced Auswertung:

- Übersicht aller benutzten Anwendungen zeigen und Suchfähigkeit

- Nachvollziehbarkeit der wirklich genutzten Microsoft Office-Produkte (Lizenz)



- Vorhandene Software mit bekannten Exploits sollten upgedatet werden



Vulnerable applications installed

Search:

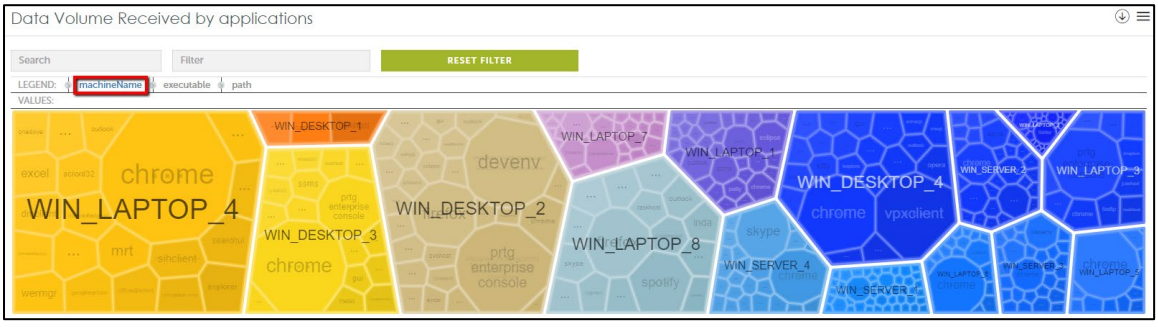
VULNERABLE APPLICATION	MACHINE COUNT	%
Iexplore	16	12.4%
Excel	16	12.4%
mstsc.exe	16	12.4%
wmplayer.exe	16	12.4%
WinWord	16	12.4%
chrome_exe	13	10.08%

Vulnerable applications installed by machine

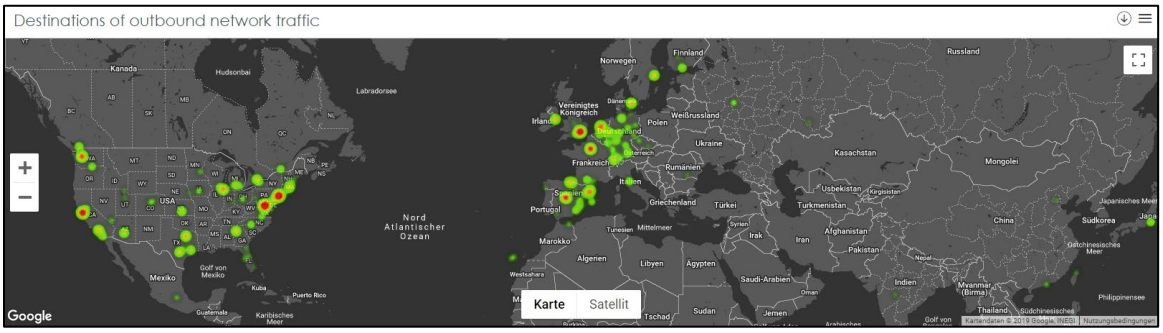
Search:

VULNERABLE APPLICATION	COMPANY	MACHINE	%
chrome_exe	Google Inc.	WIN_LAPTOP_8	0.78%
chrome_exe	Google Inc.	WIN_SERVER_4	0.78%
chrome_exe	Google Inc.	WIN_SERVER_1	0.78%
chrome_exe	Google Inc.	WIN_LAPTOP_4	0.78%
chrome_exe	Google Inc.	WIN_LAPTOP_7	0.78%
chrome_exe	Google Inc.	WIN_SERVER_3	0.78%

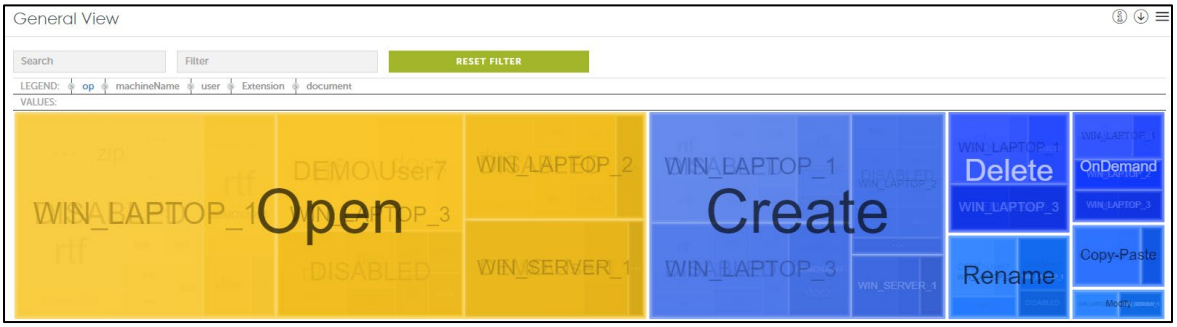
- Bandbreitennutzung der Applikationen und PCs eingehend und ausgehend



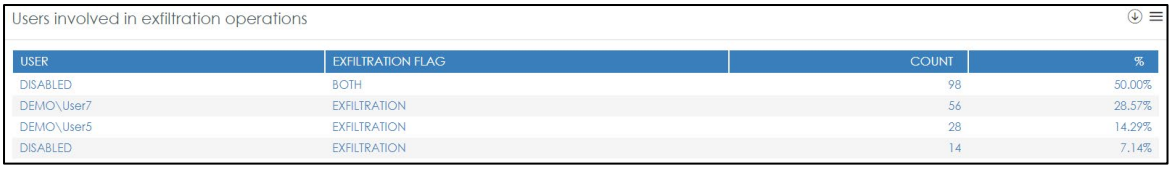
- Kommunikationskontrolle der Applikationen nach Ländern sortiert (Liegen hier Compliance-Verletzungen vor? Suspekte Kommunikation?)



- Handhabung der Dokumente mit PII und deren Operationen (Vor allem Delete und Copy-Paste könnten gravierende Auswirkungen haben)

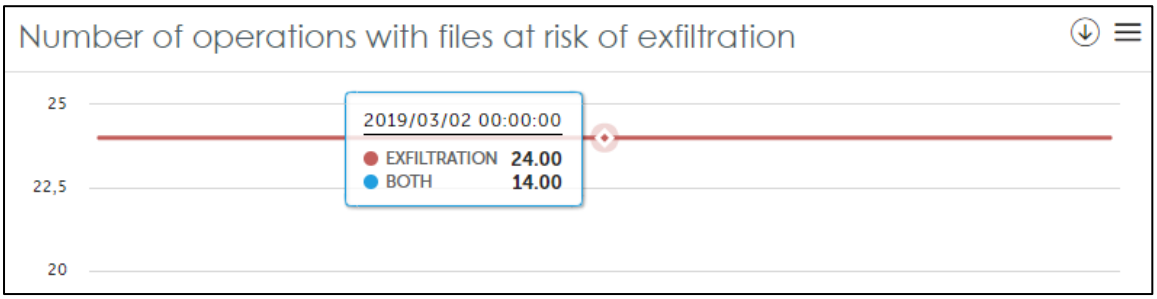


- Von welchen Benutzern werden viele Dateien ins Internet hochgeladen oder auf externe Laufwerke transferiert



USER	EXFILTRATION FLAG	COUNT	%
DISABLED	BOTH	98	50.00%
DEMO\User7	EXFILTRATION	56	28.57%
DEMO\User5	EXFILTRATION	28	14.29%
DISABLED	EXFILTRATION	14	7.14%

- Gibt es Tage an denen eine erhöhte Menge an Dateien exfiltriert wurden?



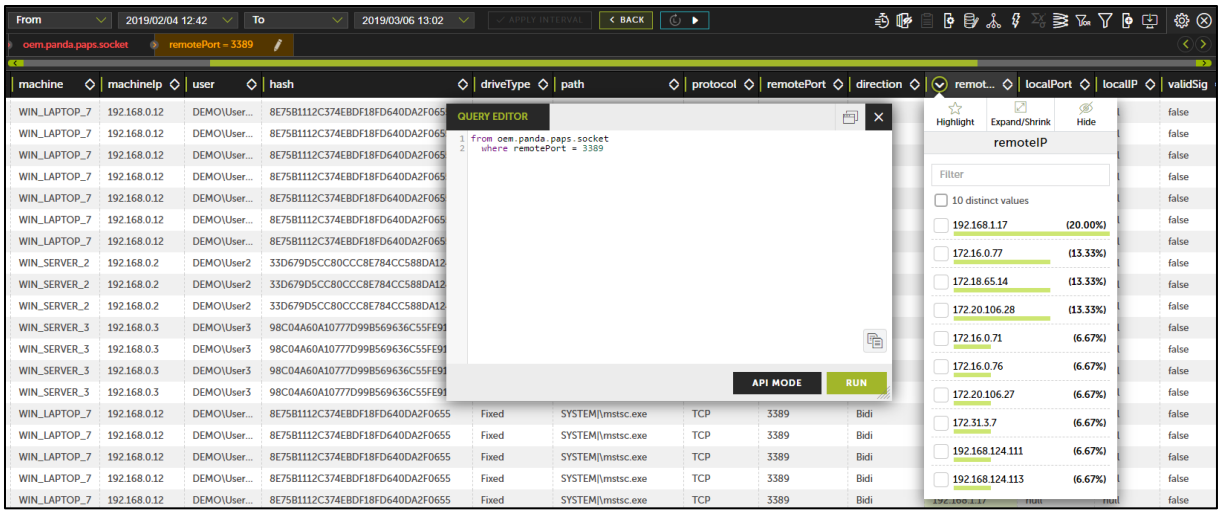
Expert Auswertung:

In der höchsten Ebene der Auswertung werden mit Queries und Analysen innerhalb der Tabellen selbst Verfahren. Die Abfragen selbst können im Nachhinein auch als Alarm definiert werden, sodass von einem Auditing in einen aktives Alerting gewechselt wird. Welche Sachen hierbei in Erfahrung gebracht werden sollen, hängt jedoch sehr stark vom Unternehmen und deren (Compliance-)Richtlinien ab.

Nachfolgend werden ein paar Queries und Filterungen vorgestellt, die Ihnen mögliche Probleme im Netzwerk darbieten und im Audit-Service standarisiert werden können.

RDP-Verbindungen kontrollieren:

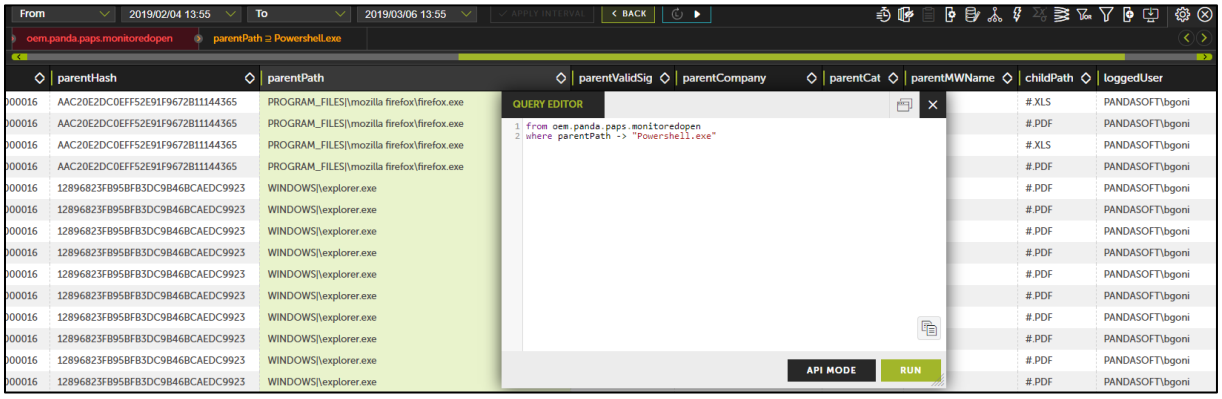
In vielen Szenarien wird RDP noch immer alles eines der ersten Eingangstüren genutzt, um Angriffe auf Unternehmen zu fahren. In der Tabelle **socket** überwachen wir alle ausgeführten Prozesse und ihre Verbindungen hinsichtlich eigener IP und der Ziel IP. Treten hier beispielsweise IPs auf, die nicht aus ihrem lokalen Netzwerk stammen oder aus einem validen Ziel im Internet, besteht hier ein mögliches Fehlverhalten, das in ihrem Hause auftaucht.



Solche Abfragen können mit einem **Query Editor** erstellt werden oder auch über die Drop-Down und Filter-Methodik ohne SQL-Statements. Hier sollte suspekte Erkenntnisse in Frage gestellt und anschließend gemeinsam verifiziert werden.

Prüfung ausgeführt Programme:

Prüfen Sie ihr Netzwerk nach Programmen, die oftmals für schädliche Interaktionen genutzt werden und ob diese ggfs. auf Dateien zugegriffen haben. Sie können dieses in der **socket** und **monitoredopen** Tabelle gegenprüfen, sowie die dazugehörigen eingeloggten User erkennen.



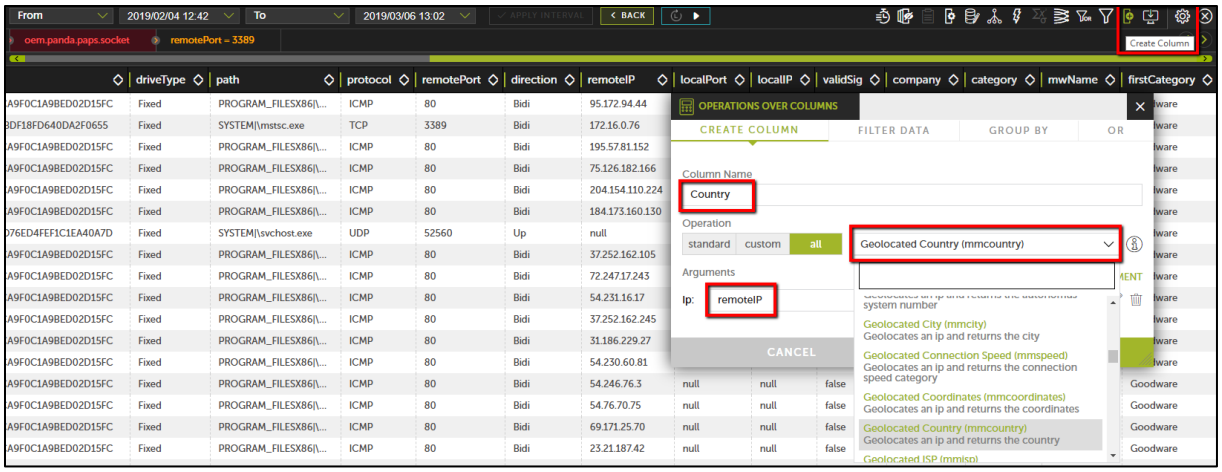
Beispiele für dies könnten sein:

- Tor.exe -> Prozess für das Tor-Netzwerk
- Bittorrent.exe -> Wird in vielen Fällen für Datei-Transfers genutzt
- Powershell.exe -> 26% aller Angriffe werden mit dieser durchgeführt
- Winlogon.exe -> Erhöhte Anmeldeversuche erkennen (Penetration)

Kommunikation in andere Länder:

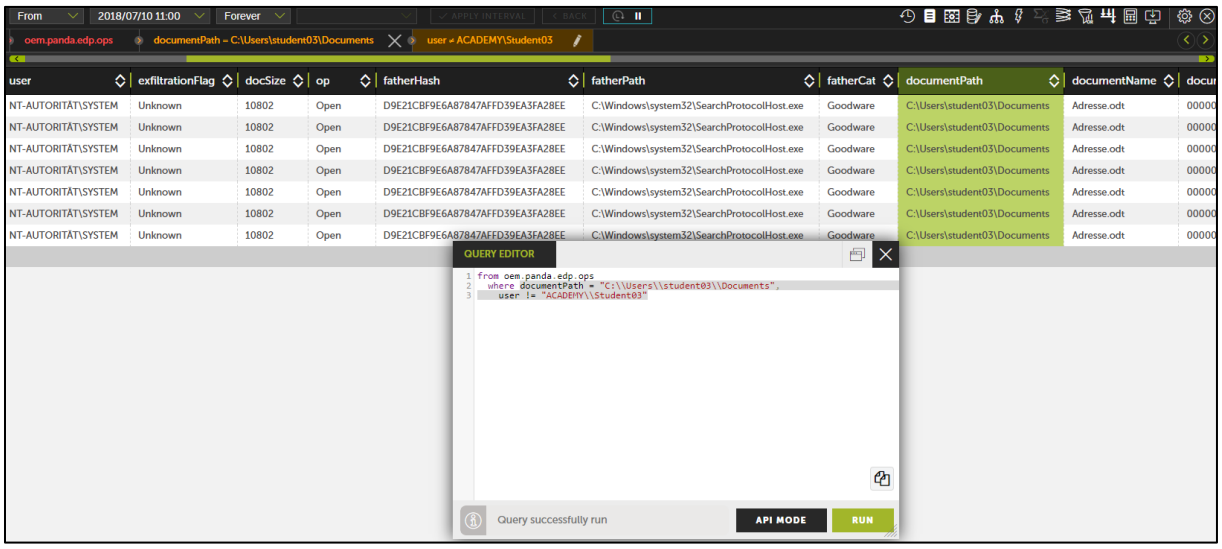
Prüfen Sie, welche Applikationen in welche Länder kommunizieren, in dem Sie eine Tabelle Stadt und Land der Tabelle **socket** anhand der Geolokation der RemoteIP hinzufügen. Dieses kann stark zum Verständnis der Netzstruktur helfen und über welche Server Sie bzw. ihre Software kommuniziert.

Möglicherweise werden so Kommunikationen aufgedeckt, die mit ihrer Compliance im Zuge der DSGVO oder auch dem CLOUD Act nicht zu Stande kommen sollten oder Fragen zur einer Kommunikation *made in Europe* aufwerfen.



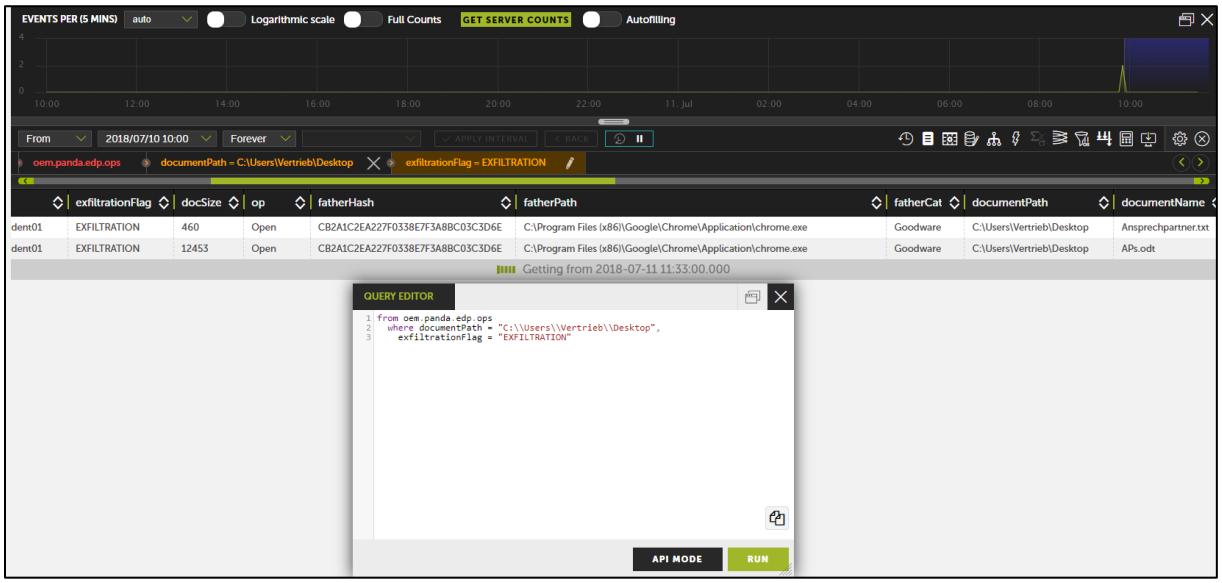
Nicht gestattete Zugriffe auf Dokumente:

In vielen Unternehmen gibt es bestimmte Verzeichnisse, die nur mit bestimmten Berechtigungen zugreifbar sein sollten. Kritisch wird es hier immer, wenn personenbezogene Informationen enthalten sind. Zur Einhaltung dieser Richtlinien können Sie in der Tabelle **edp.ops** überprüfen, ob ein nicht gestatteter Benutzer auf dieses Laufwerk zugegriffen hat:



Exfiltrierte Dateien aus lokalem Verzeichnis:

Aufbauend auf das vorherige Szenario gibt es auch Laufwerke und Ordner, von denen keine Dokumente nach außen weichen dürfen. Sie können relativ einfach über die Filterung oder auch dem Query Editor eine Abfrage eines Verzeichnisses erstellen, sobald Dateien mit PII exfiltriert wurden.



Nachfolgend noch ein paar Queries und deren Funktion, die ebenfalls angewendet werden können:

//Traffic-Verbot nach Russland außer Microsoft-Applicationen

```
from oem.panda.paps.socket
  select mmcountry(remoteIP) as Country
  where Country = "RU",
    company != "Microsoft Corporation"
```

//Download von ausführbaren PE-Files

```
from oem.panda.paps.urldownload
  select lower(url) as url_lower
  where has(url_lower, "http://", "https://"),
    has(url_lower, ".exe", ".dll", ".sct", ".hta", ".vbs", ".ps1", ".txt", ".ps2")
```

//Remote Connection Tools gefunden

```
from oem.panda.paps.ops
  select lower(params) as params_low,
    lower(childPath) as child_low,
    lower(parentPath) as parent_low
  select peek(parent_low, re("\\\\(\\w+.\\w+)$"), 1) as Exec_low
  where has(Exec_low, "aa_v3.exe", "g2comm.exe", "g2fileh.exe", "g2host.exe",
"g2mainh.exe", "g2printh.exe", "g2svc.exe", "g2tray.exe", "gopcsrv.exe", "logmein.exe",
"teamviewer.exe", "winvnc.exe", "mstsc.exe", "radmin3.exe", "lmiignition.exe",
"lmiguardiansvc.exe", "termsrv.exe", "famitrfc.exe", "awrem32.exe", "awhost32.exe",
"smpcsetup.exe", "showmypc.exe", "teamviewer_desktop.exe",
"teamviewer_service.exe", "teamviewerhost.exe", "dwrcs.exe", "vncviewer.exe",
"winvncsc.exe", "strwinchat.exe", "clientoobe.exe", "strwinclt.exe", "vnc.exe")
  group every 30m by Exec_low, parentCompany
  every –

from oem.panda.paps.ops
  select lower(params) as params_low,
    lower(childPath) as child_low,
    lower(parentPath) as parent_low
  select peek(parent_low, re("\\\\(\\w+.\\w+)$"), 1) as Exec_low
  where has(child_low, "aa_v3.exe", "g2comm.exe", "g2fileh.exe", "g2host.exe",
"g2mainh.exe", "g2printh.exe", "g2svc.exe", "g2tray.exe", "gopcsrv.exe", "logmein.exe",
"teamviewer.exe", "winvnc.exe", "mstsc.exe", "radmin3.exe", "lmiignition.exe",
"lmiguardiansvc.exe", "termsrv.exe", "famitrfc.exe", "awrem32.exe", "awhost32.exe",
"smpcsetup.exe", "showmypc.exe", "teamviewer_desktop.exe",
"teamviewer_service.exe", "teamviewerhost.exe", "dwrcs.exe", "vncviewer.exe",
"winvncsc.exe", "strwinchat.exe", "clientoobe.exe", "strwinclt.exe", "vnc.exe")
  group every 30m by parentCompany, child_low
  every -
```

Angriffsszenarien nach MITRE

Cscript.exe

Binary wird benutzt um Scripte in Windows auszuführen.

Mitre:T1096

```
from oem.panda.paps.ops
select lower(parentPath) as parent_low,
  lower(childPath) as child_low,
  lower(params) as param_low
select parent_low -> "cscript" as parent_found,
  child_low -> "cscript" as child_found,
  parent_found or child_found as parent_or_child_found
where parent_or_child_found = true
where param_low -> ".vbs"
```

Certutil.exe

Windows binary wird zum Handeln von Zertifikaten benutzt.

Mitre:T1105

Mitre:T1027

Mitre:T1140

```
from oem.panda.paps.ops
  select lower(parentPath) as parent_low,
    lower(childPath) as child_low,
    lower(params) as param_low
  select parent_low -> "certutil" as parent_found,
    child_low -> "certutil" as child_found,
    parent_found or child_found as parent_or_child_found
  where parent_or_child_found = true,
    has(param_low, "-urlcache", "-split", "http", "ftp", "-encode", "-decode")
```