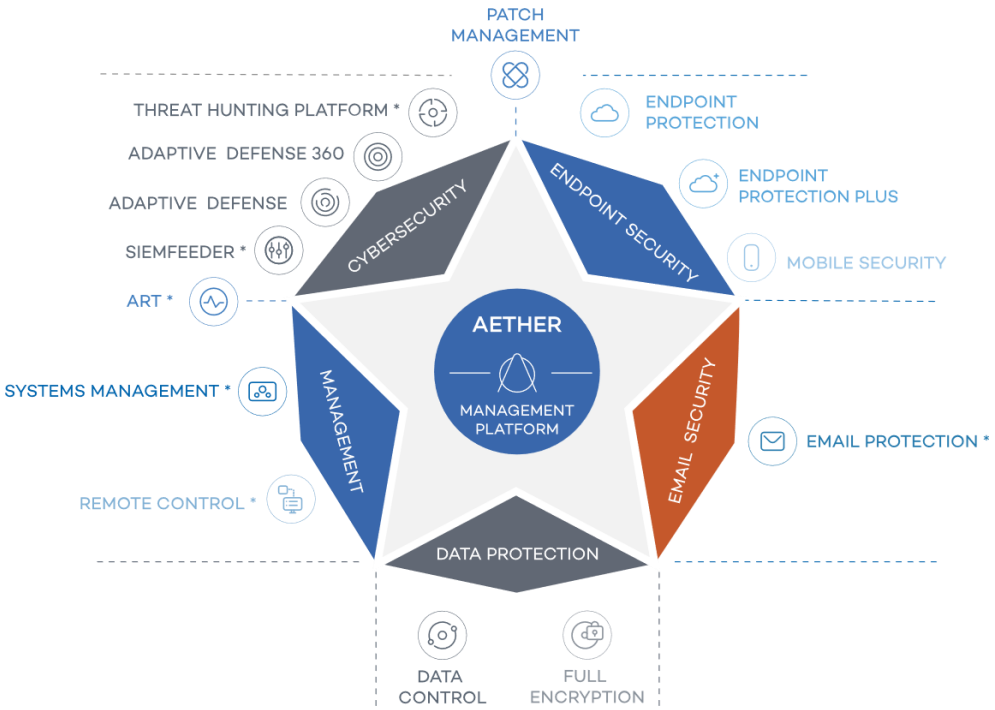
**Ziel**

Das Ziel dieses Service ist es, mittels Standard-Tools Indikationen zu liefern, wo in Ihrem Unternehmen Optimierungspotenzial hinsichtlich der Netzwerk-, IT- und Daten-Sicherheit liegen.

**Voraussetzungen**

Dazu ist es zunächst nötig, gemeinsam mit Ihrer IT-Administration auf denen für das Audit ausgewählten Systemen (Endgeräten) einen universellen Software (AETHER)-Agenten auszurollen, der dazu dient, die für das Audit notwendigen Daten zu erfassen. Darüber hinaus sind keine weiteren Installationen von Programmen bei Ihnen notwendig. Der reguläre Geschäftsablauf wird nicht beeinträchtigt.




**Ablauf**

Die Voraussetzungen dafür sind auf der Interessentenseite minimalst, was wir gemeinsam für Sie und Ihre IT in einer vorgeschalteten Web-Konferenz erläutern.

Sämtliche für die spätere Auswertung eingesetzten Tools werden cloudbasiert und zentral administriert durch IMMUNIT bereitgestellt. Zusammengefasst benötigen wir lediglich die administrative Autorisierung zur Installation und die Befähigung unsere Cloud-Dienste ansteuern zu können.

Innerhalb der folgenden zwei bis drei Wochen, werden automatisiert sämtliche Daten erhoben, welche für die Auswertungen des Audits relevant sind. Gemeinsam mit dem Interessenten zeigen wir dann am Live-System, was wir gesehen haben und welche Interpretationen das zulässt. Hieraus ergeben sich die Optimierungspotenziale.


fon +49 2158 80 699 18

**Auswertungen**

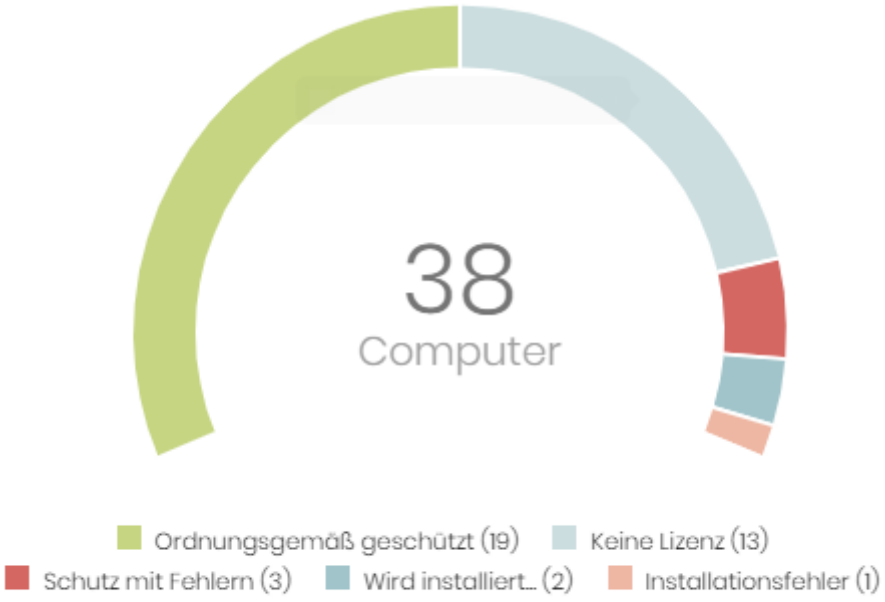
Neben individuellen Fragestellungen können wir z.B. betrachten:

- Wohin bzw. woher kommt der Datenverkehr in Ihrem Netzwerk?
- Welche Applikationen, Geräte oder Benutzer haben den größten Datenkonsum?
- Erfolgen die Benutzeranmeldungen am Netzwerk entsprechend der Richtlinien?
- Gibt es Anomalien bei den Remote-Verbindungen (RDP, SSH)?
- Gibt es Verdachtsmomente für Brute-Force-Attacken?
- Welche Applikationen und wie häufig werden diese im Netzwerk genutzt?
- Welche Applikationen mit bekannten Sicherheitslücken werden benutzt?
- Wie ist der Patch-Stand der einzelnen Systeme?
- Welche Systeme gibt es überhaupt im Netzwerk?
- Gibt es womöglich unentdeckte Malware innerhalb der Netze?
- Wo liegen Dateien mit personenbezogenen Daten außerhalb der datenführenden Systeme (DSGVO)?
- Was wird mit diesen personenbezogenen Daten gemacht?

Die im Rahmen der Betrachtung des Live-Systems gemachten Beobachtungen fassen wir in einer „Management Summary“ zusammen, welche als Handlungsempfehlung oder Entscheidungsvorlage für Folgeaktivitäten verwendet werden kann.

**Einfaches Deployment**

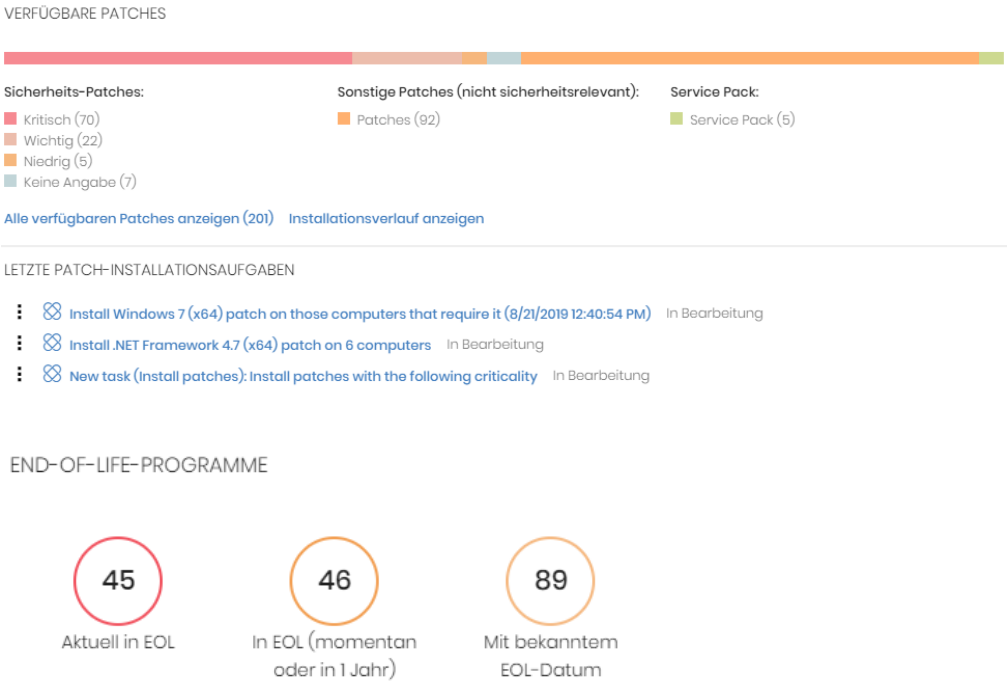
Mittels integrierter Werkzeuge erfolgt die Installation still und automatisiert, indem nicht mit dem Agent ausgestattete Systeme identifiziert werden und diese mit wenigen Klicks betankt werden können.





**Überprüfung des Patch-Standes**

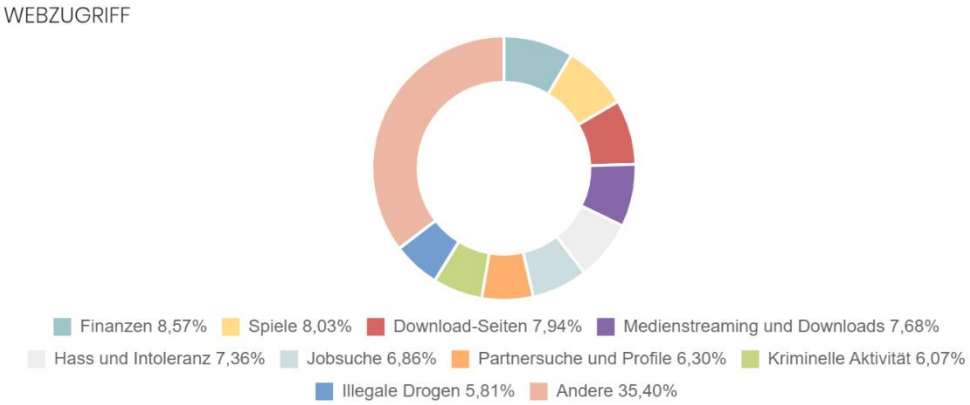
Die integrierte Inventarisierung liefert explizite Informationen über den Stand der fehlenden Patches und Sicherheits-Updates und gegebenenfalls den Einsatz von Software mit abgekündigtem Hersteller-Support (hohe Risiken).



**Überprüfung der Awareness bei der Internet-Nutzung der Mitarbeiter**

Auf Wunsch können Sie in das Surf-Verhalten der Mitarbeiter Einsicht nehmen und daraus Rückschlüsse auf die Awareness bezüglich etwaiger Risiken nehmen, hinischtlich der Gefahren die beim Surfen lauern.

Hält man sich an die etwaig vorgegebenen Richtlinien oder gibt es Ausbrüche? Was wären geeignete Maßnahmen, hier die Risiken für das Unternehmen und in den Arbeitsprozessen bearbeiteten Daten zu reduzieren oder einzudämmen.




Die Reports können nach verschiedenen Kriterien auch in der Tiefe erstellt werden.

**Die 10 am häufigsten aufgerufenen Kategorien**

| Kategorie | Zugriffsversuche | Computer |
|---|---|---|
| Finanzen | 275 | 12 |
| Spiele | 261 | 10 |
| Download-Seiten | 248 | 11 |
| Hass und Intoleranz | 227 | 10 |
| Medienstreaming und Downloads | 215 | 11 |
| Jobsuche | 200 | 14 |
| Kriminelle Aktivität | 199 | 10 |
| Bildung | 191 | 10 |
| Illegale Drogen | 179 | 9 |
| Partnersuche und Profile | 173 | 10 |

Vollständigen Bericht anzeigen

**Die 10 am häufigsten aufgerufenen Kategorien nach Computer**

| Computer | Kategorie | Zugriffsversuche |
|---|---|---|
| WIN_LAPTOP_2 | Spiele | 59 |
| WIN_SERVER_1 | Spiele | 55 |
| WIN_DESKTOP_12 | Finanzen | 52 |
| WIN_DESKTOP_9 | Finanzen | 51 |
| WIN_DESKTOP_9 | Partnersuche und Profile | 48 |
| WIN_DESKTOP_8 | Hass und Intoleranz | 44 |
| WIN_DESKTOP_2 | Download-Seiten | 42 |
| WIN_SERVER_6 | Kriminelle Aktivität | 40 |
| WIN_DESKTOP_9 | Spiele | 40 |
| WIN_DESKTOP_9 | Illegale Drogen | 40 |

Vollständigen Bericht anzeigen

**Die 10 am häufigsten blockierten Kategorien**

| Kategorie | Verweigerte Zugriffsversuche | Computer |
|---|---|---|
| Medienstreaming und Downloads | 225 | 11 |
| Finanzen | 216 | 12 |
| Download-Seiten | 207 | 11 |
| Spiele | 199 | 11 |
| Hass und Intoleranz | 195 | 10 |
| Jobsuche | 193 | 14 |
| Partnersuche und Profile | 188 | 11 |
| Computer und Technologie | 168 | 12 |
| Glücksspiele | 163 | 11 |
| Regierung | 159 | 9 |

Vollständigen Bericht anzeigen

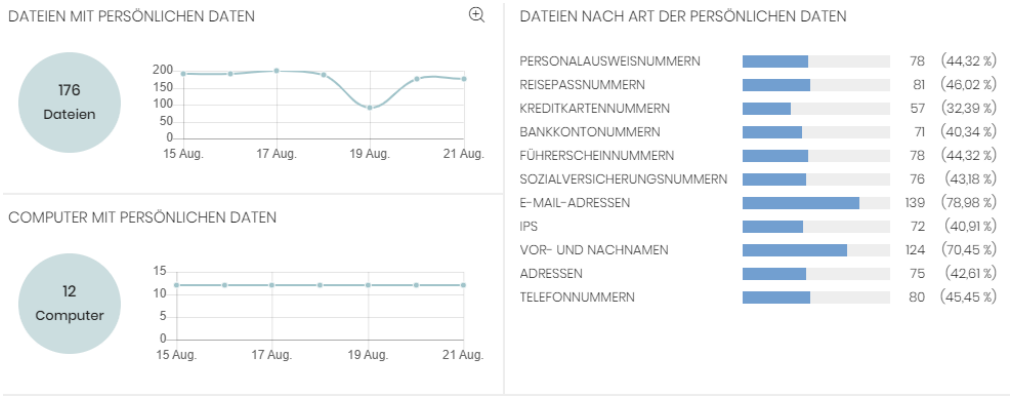
**Die 10 am häufigsten blockierten Kategorien nach Computer**

| Computer | Kategorie | Verweigerte Zugriffsversuche |
|---|---|---|
| WIN_DESKTOP_2 | Regierung | 48 |
| WIN_DESKTOP_2 | Unterhaltung | 46 |
| WIN_LAPTOP_2 | Spiele | 45 |
| WIN_LAPTOP_2 | Computer und Technologie | 44 |
| WIN_SERVER_1 | Medienstreaming und Downloads | 44 |
| WIN_DESKTOP_2 | Partnersuche und Profile | 36 |
| WIN_DESKTOP_8 | Download-Seiten | 36 |
| WIN_DESKTOP_8 | Hass und Intoleranz | 36 |
| WIN_DESKTOP_12 | Regierung | 35 |
| WIN_LAPTOP_2 | Download-Seiten | 33 |

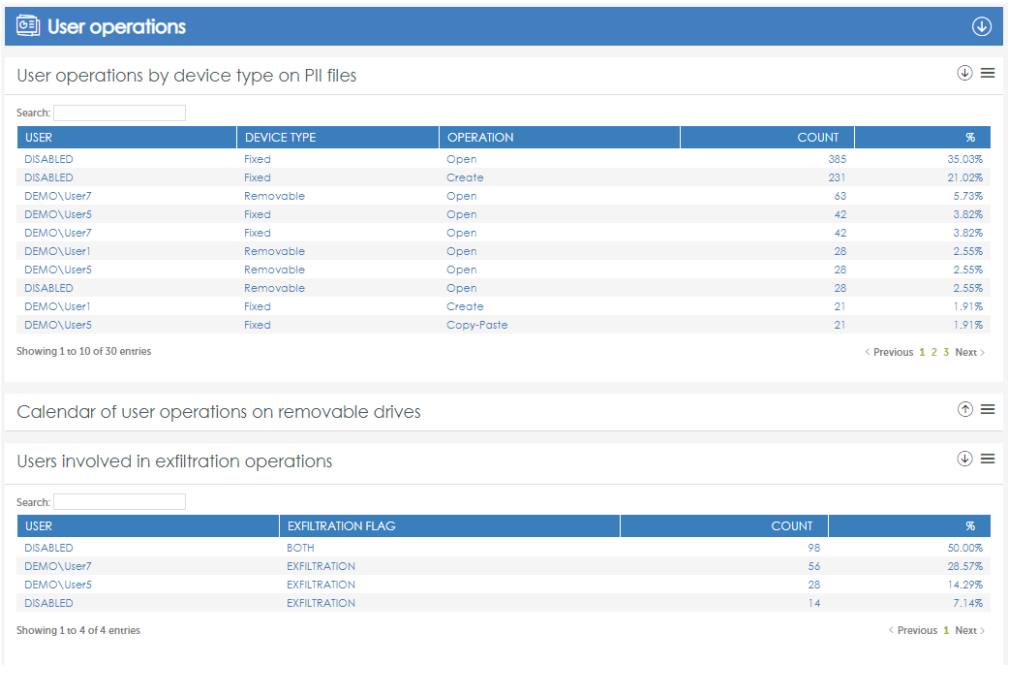
Vollständigen Bericht anzeigen

**Aufspüren von relevanten Risiken hinsichtlich DSGVO**

Über den Agent werden die an die Massenspeicher der einbezogenen Endgeräte dahingehend überprüft, ob dort außerhalb der datenführenden Systeme Dateien liegen, welche personenbezogene Daten beinhalten und damit ein hohes Risiko darstellen, ungewollt exfiltriert zu werden, also das Unternehmen verlassen könnten.

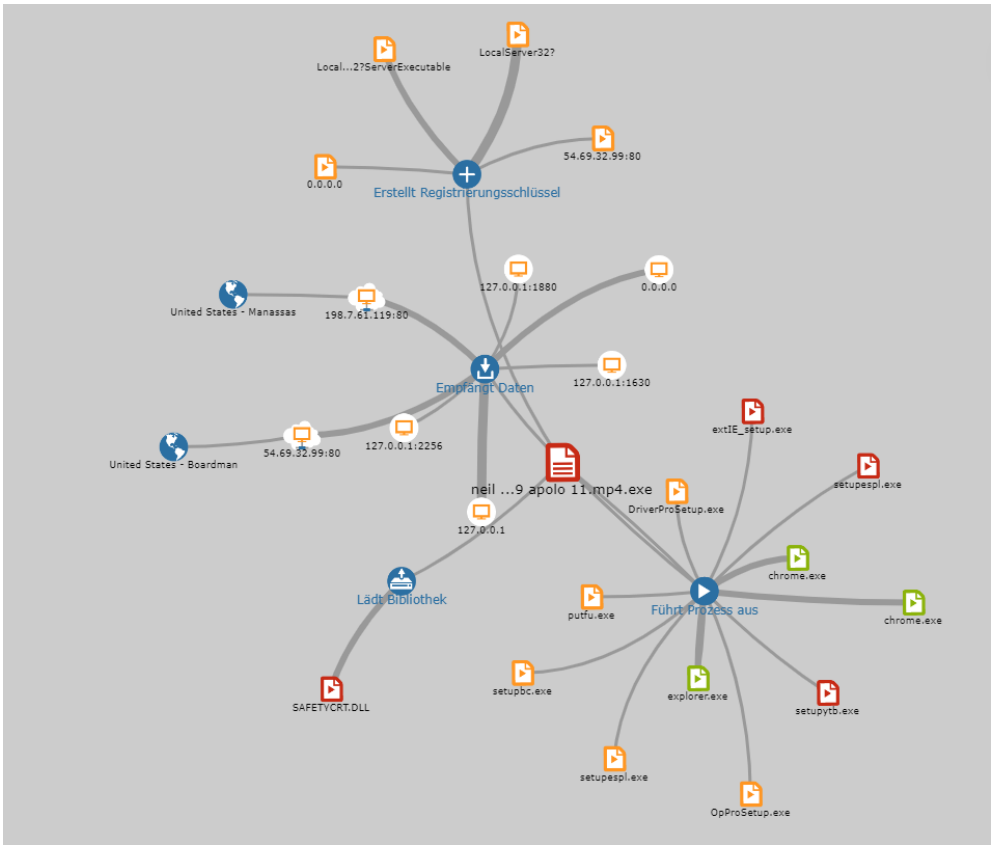



Über das verbundene SIEM-Framework lassen sich etwaige Benutzer-Aktivitäten tiefer analysieren.



**Forensische Analyse**

Werden anormale oder verdächtige Prozesse auf irgendeinem Endgerät erkannt, können diese forensisch im Detail analysiert werden.



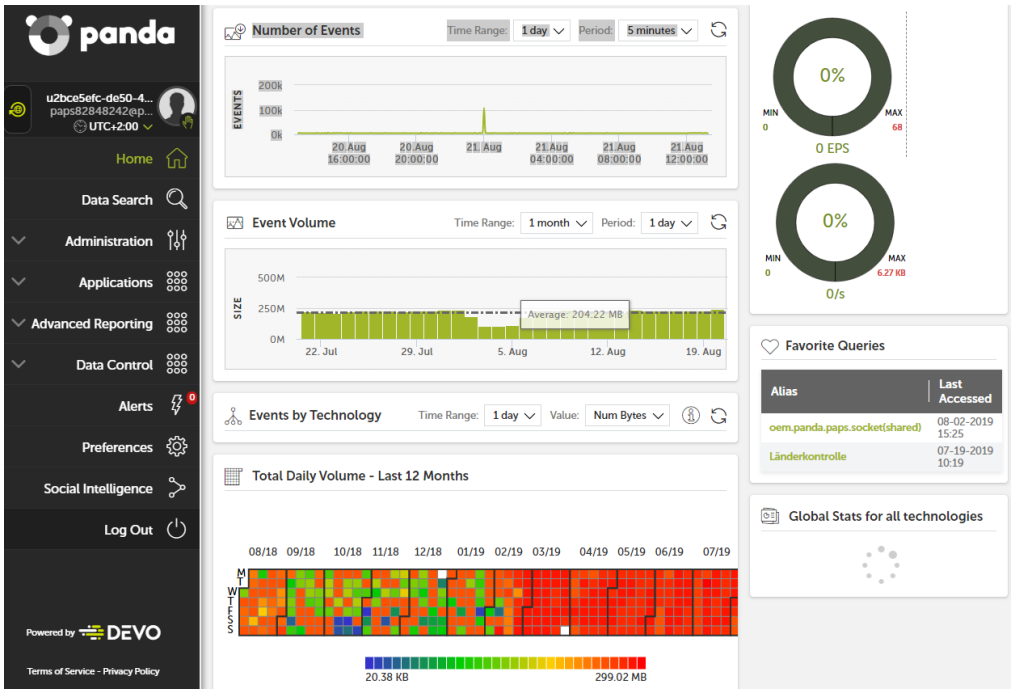

**Vollständiges Aufzeichnen aller Events auf jedem Endgerät**

Über den Agenten werden sämtliche Aktivitäten (Events) aller Prozesse auf allen Endgeräten inklusive deren Interaktionen intern und extern aufgezeichnet.

| Datum | Male | Aktion | Pfad/URL/Registrierungsschlüssel/IP:Port | Datei-Hash/Registrierungswert/Protokollrichtung/Beschreibung | Vertrauenswürdig |
|---|---|---|---|---|---|
| | | Wählen Sie eine Ak | | Wählen Sie einen Hash aus | Wählen Sie ei |
| 19.08.2019 16:38:03 | 1 | Erstellt Registrierungsschlüssel für die Ausführung | \REGISTRY\USER\S-1-5-21-3286655578-1091891218-2006878755-1004_CLASSES\CLSID\{F28C2F70-47DE-4EA5-8F6D-7D1476CD1EF5}\LocalServer32? | C:\Documents and Settings\Adminri\Mis documentos\Downloads\Neil Armstrong transmisin original del alunizaje 1969 Apolo 11.mp4.exe | Unbekannt |
| 19.08.2019 16:38:03 | 1 | Erstellt Registrierungsschlüssel für die Ausführung | \REGISTRY\USER\S-1-5-21-3286655578-1091891218-2006878755-1004_CLASSES\CLSID\{F28C2F70-47DE-4EA5-8F6D-7D1476CD1EF5}\LocalServer32? ServerExecutable | C:\Documents and Settings\Adminri\Mis documentos\Downloads\Neil Armstrong transmisin original del alunizaje 1969 A | Unbekannt |
| 19.08.2019 16:38:04 | 1 | Erstellt Registrierungsschlüssel für die Ausführung | \REGISTRY\USER\S-1-5-21-3286655578-1091891218-2006878755-1004_CLASSES\TypeLib\{F57B1AA6-3E5C-404A-9118-C1D91F537040}\1.0\0\win32? | C:\Documents and Settings\Adminri\Mis documentos\Downloads\Neil Armstrong transmisin original del alunizaje 1969 Apolo 11.mp4.exe | Unbekannt |
| 19.08.2019 16:38:40 | 1 | Verwendet Netzwerkadapter | 127.0.0.1 | CUDP-UnKnown | Unbekannt |
| 19.08.2019 16:38:40 | 1 | Verwendet Netzwerkadapter | 127.0.0.1:1630 | UDP-Bidirectional | Unbekannt |
| 19.08.2019 16:38:48 | 1 | Verwendet Netzwerkadapter | 0.0.0.0 | TCP-UnKnown | Unbekannt |
| 19.08.2019 16:38:48 | 1 | Verwendet Netzwerkadapter | 54.69.32.99:80 | TCP-Bidirectional | Unbekannt |
| 19.08.2019 16:38:49 | 1 | Verwendet Netzwerkadapter | 198.7.61.119:80 | TCP-Bidirectional | Unbekannt |
| 19.08.2019 16:39:52 | 1 | Lädt | PROGRAM_FILES\MOVIES TOOLBAR\SAFETYNUT\SAFETYCRT.DLL | 9994BF035813FE8EB6BC98ECCBD5B0E1 | Nein |
| 19.08.2019 16:39:55 | 1 | Führt aus | TEMP\087B213b8b8\temp\setupespl.exe | F69E31FAA4B9159ABD590D0CD2CC94A5 | Nein |
| 19.08.2019 16:40:33 | 1 | Führt aus | TEMP\087B213b8b8\temp\extIE_setup.exe | 66D0E599FC9EDDCA4A591D4C54BA6187 | Nein |
| 19.08.2019 16:40:56 | 1 | Führt aus | TEMP\087B213b8b8\temp\setupytb.exe | 8C212F89ED8AAF04D7665B24473FCB36 | Nein |

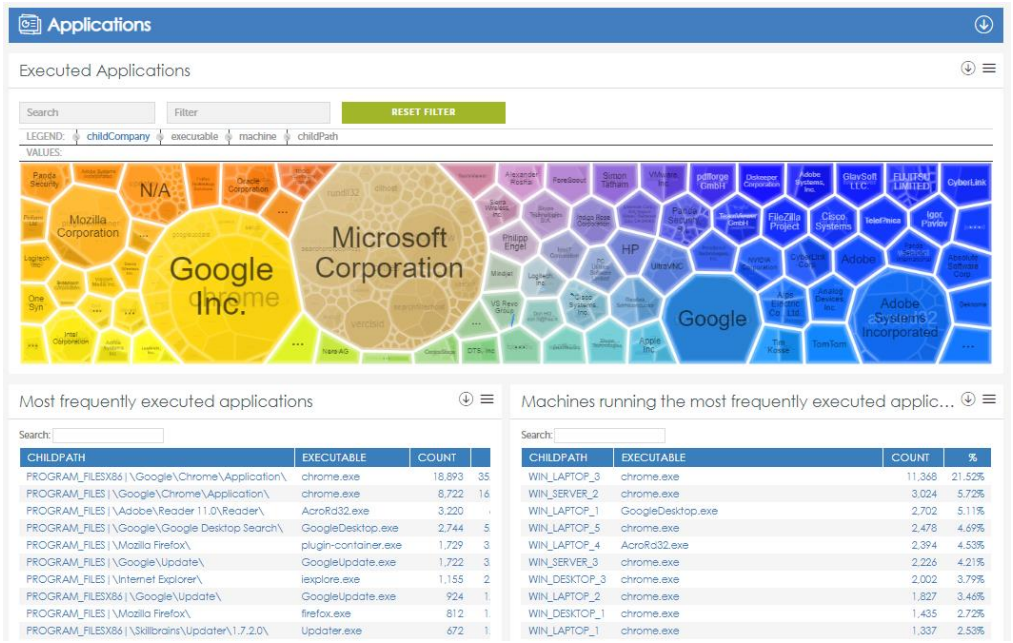
**Integriertes SIEM-Framework**

Über das verbundene SIEM-Tools können diese dann auch weiteren Big-Data-Analysen unterzogen werden.




**Übersicht über alle genutzten Applikationen**

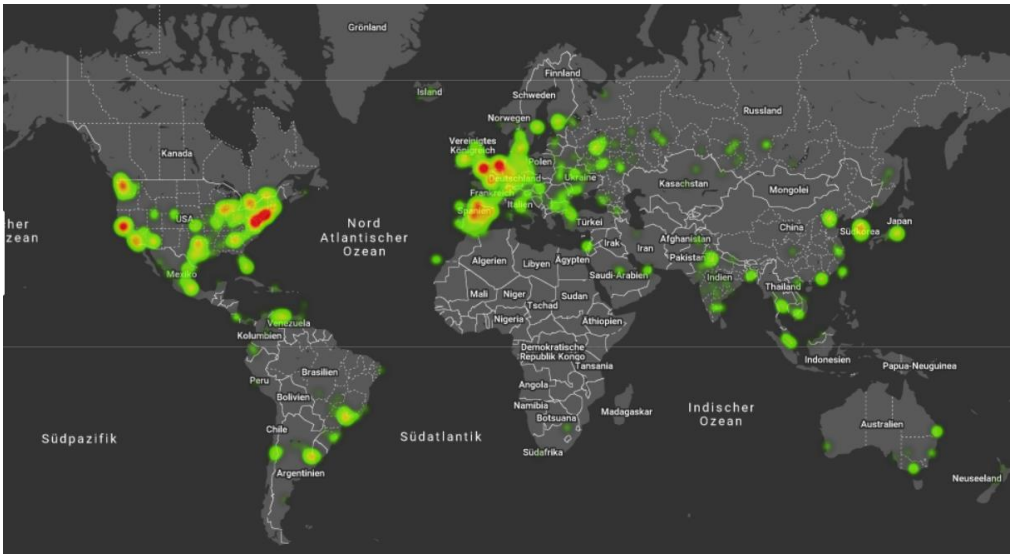
Man erhält einen kompletten Überblick, welche Applikationen im Einsatz sind, welcher Datenverkehr darüber produziert wird, sowohl inbound wie outbound und damit eine sehr gute Indikation, ob es eine Schatten-IT gibt.




Daneben lässt sich auch erkennen, wo gescriptete Applikationen eingesetzt werden, z.B. Powershell, Python .. u.a., ebenso lassen sich Remote-Verbindungen analysieren. Dies liefert in der Summe Indikationen dazu, ob eventuell Anomalien oder atypische Nutzung/Verhalten vorliegen.

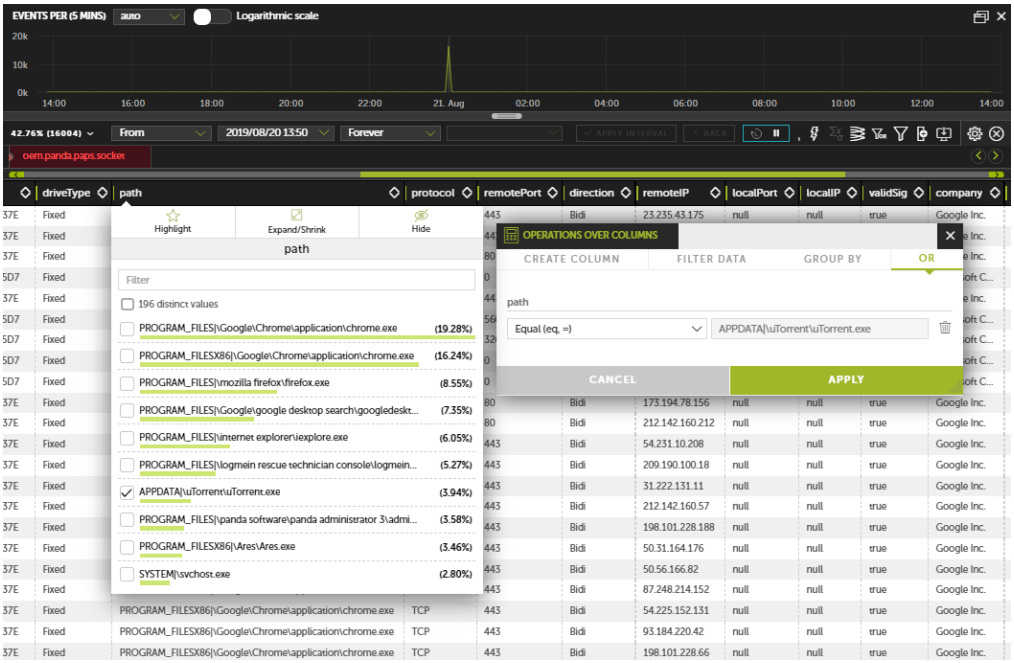
**Analyse des Outbound-Datenverkehr**

Etwaige Verdachtsmomente oder unzureichende Konfigurationen im Perimeter-Schutz lassen sich schon frühzeitig erkennen, denn häufig erfolgen gezielte Attacken über einen längeren Zeitraum in mehreren Etappen.




**SIEM für KMUs**

Hinsichtlich der individuellen Analyse sind kaum Grenzen gesetzt. Neben den vorgefertigten Abfragen lassen sich diese anpassen oder neu erstellen, diese als Vorlagen definieren und darüber Alarme einstellen, die bei voreingestellten Schwellwerten informieren.




Optional ist es auch möglich, Alarme mit automatisierten Folgeaktivitäten zu versehen, um im Verdachtsfall präventiv einzugreifen. Diese Features sind aber nicht im Standard verfügbar.