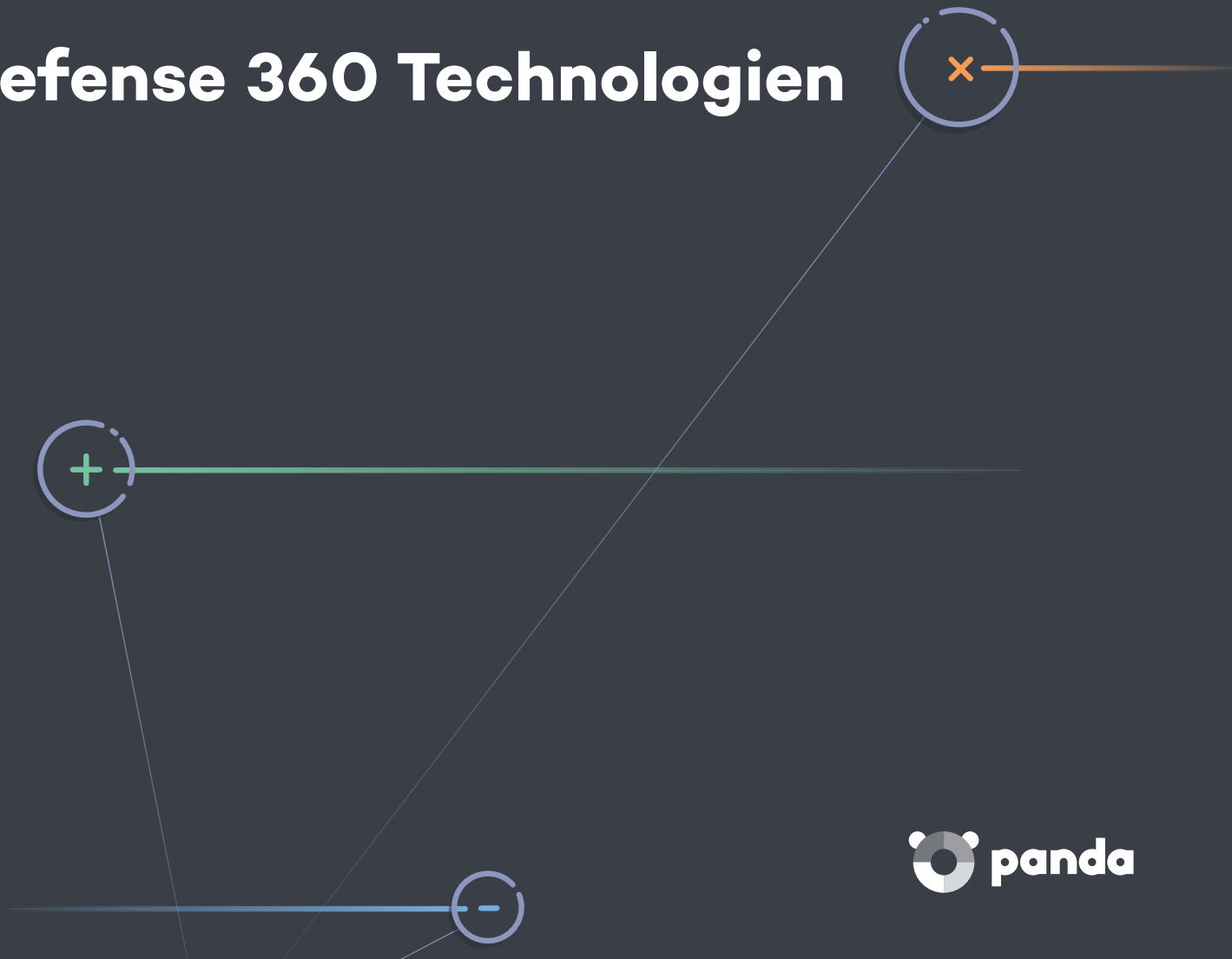
Panda Adaptive Defense 360 Technologien

Managed Detection

Managed Mitigation



panda

Adaptive Defense 360

Inhaltsverzeichnis

1. Technologien und Dienst-leistungen in Panda Adaptive Defense 360.

Einleitung

In diesem Leitfaden wird erläutert, wie die in Panda Adaptive Defense 360 integrierten Technologien und Managed Services zusammenwirken. Die EDR-Funktionen (Endpoint Detection and Response) und die Vorteile der KI-Technologie sind wichtige Unterscheidungsmerkmale.

Die folgende Tabelle zeigt, wie die einzelnen Technologien funktionieren und welche Techniken verwendet werden, um Angriffe so schnell wie möglich zu blockieren. Die Endpoints werden vor einer Kompromittierung geschützt, die Angriffe werden erkannt, eingedämmt und beseitigt, bevor Schaden entstehen kann.

Panda Adaptive Defense 360

Unattended & Managed Services	PREVENT	DETECT	HUNT	INVESTIGATE/ FORENSIC	CONTAIN/ REMEDIATE	ANTICIPATE Avoid Future Attacks
KNOWN & UNKNOWN MALWARE	Traditional EPP technologies [1] 100% Attestation Services [2] Risk-based Application Control: Lock/Hardening mode			Incident Analysis, Event timeline	Execution denied, Managed disinfection	Incident analysis insights Panda Patch Management Advanced Reporting tool Panda Data Control
EXPLOITS Metaexploits, Exploits kits, Exploits in the wild	Pre-execution IoAs of exploits in the wild[3]	Behavioral IoAs in memory[4]	Threat Hunting & Investigation Service (THIS)[7] Feeds new IoAs to the endpoint agents		Compromised process killed, Isolate endpoints	
LIVING-OFF-THE-LAND High confidence malicious activity	Context based pre-execution IoAs (Interpreters, scripts, macros)[5]	Behavioral IoAs with admin tools, scripts, shellcode injections[6]			Execution denied or blocked	

Die in Panda Adaptive Defense 360 integrierten Technologien und Dienste zur Prävention, Erkennung und Reaktion sind:

1. **Technologien zur Endpoint-Prävention** [(1)].
2. **Managed 100% Attestation Service** [(2),] der alle Anwendungen und Binärdateien vor und während der Ausführung klassifiziert, um sicherzustellen, dass nur vertrauenswürdige Executables ausgeführt werden können.
3. **Technologien zur Aufdeckung von Exploits und Living-off-the-Land (LotL) Techniken** [(3, 4, 5, 6)]. LotL-Angriffstechniken ermöglichen es dem Angreifer, unbemerkt bereits vorhandene administrative Anwendungen auf den Geräten und Servern auszunutzen und diese zu missbrauchen.
4. **Managed Threat Hunting Service** [(7)], als Teil der Lösung. Sicherheitsexperten entdecken neue LotL-Techniken und binden diese neuen Erkennungen in den Endpoint-Agenten ein.

2. EPP Technologie Stack

EPP Proactive Technologies Stack	Panda Adaptive Defense 360
Generalist signatures and Heuristics	✓
Cloud Based Lookup to the Collective Intelligence (Threat Intel)	✓
Behavioral analysis & IoAs detection	✓
Firewall, IDS/IPS, Networks packet inspection	✓
Anti-tampering	✓
Device Control	✓
URL Classification & Reputation	✓
Application Control	✓
Antispam, Antiphishing, content filtering for MS Exchange Servers	✓
Mailbox protection & Intelligence Scan for MS Exchange Servers	✓
Vulnerability Assessment & Patching*	✓

*Panda Patch Management

Es besteht ein weit verbreiteter Irrglaube, dass EPP-Technologien nur traditionelle, signaturbasierte Antivirenlösungen sind und durch eine EDR-Lösung ersetzt werden können.

In der Realität kombinieren diese Technologien, neben der signaturbasierten Analyse, auch generische Signaturen, Heuristiken, Firewalls, URL-Reputation, Verhaltens- und IoA-Analysen (Indicators of Attack), Schwachstellenmanagement, Anwendungskontrolle und andere Funktionen, die das Risiko erheblich mindern können.

Präventionstechnologien, die mit EDR-Lösungen zusammenarbeiten, bieten erhebliche Vorteile, unter anderem:

- **Signifikante Risikoreduktion.** Sie müssen keine Datei ausführen, um Malware zu erkennen, und sie benötigen nur eine Internetverbindung, um die Cloud abzufragen.

- **Sehr geringes Ausmaß an false positives.** EPP-Technologien, die eigenständig schützen können, sind in einer großen Anzahl von Endpoints weit verbreitet und so konfiguriert, dass sie false positives minimieren.

- **Performance-Optimierung.** Sie arbeiten zusammen, integriert, um Redundanzen zu vermeiden und die Auswirkungen auf die Leistung der zu schützenden Endpoints zu minimieren.

3. Der 100% Attestation Service

KI als disruptive Innovation im Sicherheitsbereich

Als Teil der Panda Adaptive Defense- und Adaptive Defense 360-Lizenz ist ein Managed Service enthalten, der alle Prozesse, die auf jedem Endpoint ausgeführt werden, als Malware oder vertrauenswürdig einstuft. Der große Vorteil dieses Services besteht darin, dass er sicherstellt, dass nur die vertrauenswürdigen Prozesse ausgeführt werden. Da es sich um einen voll automatisierten Service handelt, erfordert er keine Intervention oder Entscheidung des Endbenutzers, der IT-Verantwortlichen oder des IT-Teams. Der 100% Attestation Service besteht aus drei Schlüsselkomponenten:

1. **Kontinuierliche Überwachung der Endpoint-Aktivitäten, von einer Cloud-nativen Plattform.**

   Die Aktivität jeder Anwendung auf den Endpoints, unabhängig von ihrer Art, wird überwacht und zur kontinuierlichen Klassifizierung an die Cloud gesendet. Auf diese Weise lassen sich Malware-Ausführungen und selbst ausgeklügelte Angriffe wie Supply-Chain-Angriffe verhindern.

2. **Automatisierte, AI-basierte Klassifizierung.**

   Automatisierte Klassifizierungen werden in einem Cloud-basierten KI-System vorgenommen, in dem ein Array von mehreren ML-Algorithmen ausgeführt wird, die Hunderte von statischen, Verhaltens- und Kontext-Attributen in Echtzeit verarbeiten. Die Attribute werden aus der Telemetrie der geschützten Umgebung und aus einem Satz physischer Sandboxen extrahiert, in denen die ausführbaren Dateien zur Explosion gebracht werden.

Heute liegt die Rate der automatisierten Klassifizierung bei 99,98%, so dass nur 0,02% der Prozesse ein Eingreifen unserer Panda Professionals erfordern. Das KI-Klassifizierungssystem ist daher autark, skalierbar auf große Dateivolumen, arbeitet in Echtzeit und ohne Abhängigkeit vom Input des Endbenutzers.

Was ist physikalisches Sandboxing?

Eine Reihe von Cloud-basierten, maßgeschneiderten Maschinen, die speziell dafür konfiguriert sind, Dateien zu detonieren und Echtzeit-Verhaltens- und Kontextbeobachtungen zu extrahieren.

Wir verwenden physisches Sandboxing anstelle von Virtual Machine Sandboxing, da es zahlreiche bösartige Anwendungen gibt, die VM-aware sind und erkennen, wenn sie innerhalb einer VM ausgeführt werden, wodurch ihr bösartiges Verhalten verhindert wird.

3. Risikobasierte Anwendungskontrolle.

Bezieht sich auf die Betriebsmodi des Protection Agents, der an den Endpoints ausgeführt wird. Es gibt zwei Sicherheitsstufen:

- **Hardening Modus:** verwehrt die Ausführung jeder unbekannten Anwendung oder Binärdatei, die von außen kommt (Web-Downloads, E-Mail, Wechselmedien, entfernte Standorte usw.).

- **Lock Modus:** verwehrt die Ausführung jeder unbekannten Anwendung oder Binärdatei, unabhängig von ihrem Ursprung (aus dem Netzwerk, vom Endpoint selbst oder von außerhalb). Der Modus stellt sicher, dass alle laufenden Prozesse vertrauenswürdig sind.

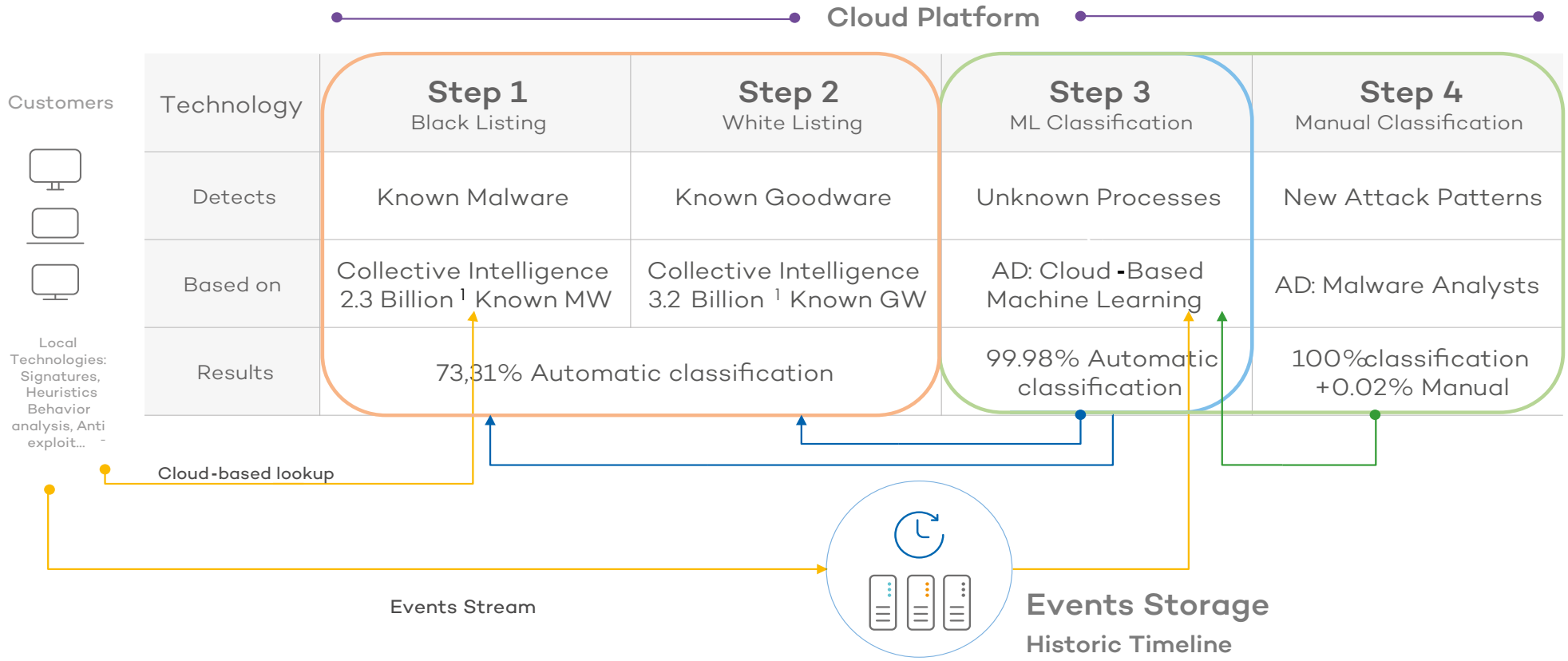
Panda Security's Collective Intelligence.
Eine weitere Schlüsselkomponente, die in einer Cloud-basierten Plattform gehostet wird, ermöglicht den Betrieb des neuen Schutzmodells und steigert die Effizienz des 100% Attestation Service.

Die Collective Intelligence repräsentiert den konsolidierten und inkrementellen Wissensspeicher aller Anwendungen, Binärdateien und anderer Dateien, die interpretierbaren Code enthalten, sowohl vertrauenswürdigen als auch bösartigen.

Diese Sammlung von Informationen werden kontinuierlich von KI-Systemen und Analysten in die Cloud gespeist und gleichzeitig von den Lösungen und Services von Panda Security vor jeder Ausführung kontinuierlich abgefragt.

- Die folgende Grafik zeigt, wie die Technologien im Stack nahtlos zusammenarbeiten und die Klassifizierung aller Anwendungen, Binärdateien und Dateien mit interpretierbarem Code in Echtzeit ermöglichen.

So funktioniert der 100% Attestation Service



4. Schutz vor Application Exploits und Living-off-the-Land (LotL)-Angriffen

Die kontinuierliche Überwachung der Aktivität an den Endpoints ermöglicht es dem Agenten, als Sensor zu fungieren und die Cloud-Plattform nicht nur über die ausgeführten Dateien zu informieren, sondern auch über den Kontext der Ausführung (was direkt vorher passiert ist, welcher Benutzer versucht, welchen Befehl oder welche Anwendung auszuführen, welcher Netzwerkverkehr erzeugt wird, auf welche Dateien zugegriffen wird, Parameter, etc.)

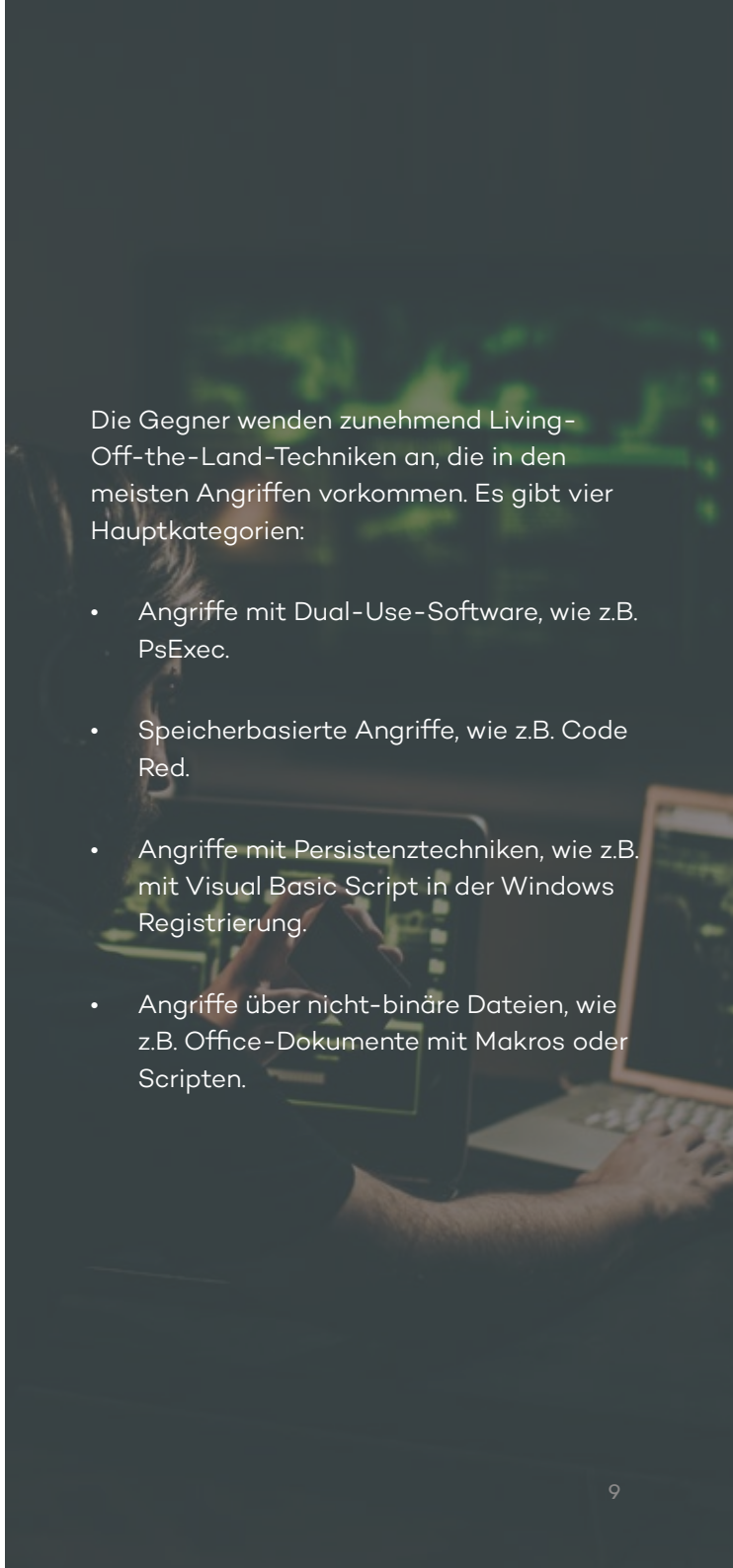
Dies ermöglicht es, zunächst am Endpoint anormales oder verdächtiges Verhalten zu identifizieren und diese als Indicators of Attack (IoAs) zu kategorisieren, mit einem hohen Maß an Sicherheit und ohne false positives.

Häufig sind IoAs mit bestimmten Phasen der Cyber Kill Chain oder mit der Taktik des MITRE ATT&CK Frameworks verwandt[1]:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Das Erkennen von IoAs, bevor Daten exfiltriert (oder im Falle eines Lösegeldangriffs verschlüsselt werden), ist ein sehr effektiver Abwehrmechanismus, insbesondere gegen Living-off-the-Land (LotL)-Angriffe, auch wenn die Endpoints möglicherweise bereits kompromittiert wurden.

Panda Adaptive Defense und Panda Adaptive Defense 360 integrieren innerhalb desselben Schutzagenten einen kompletten Technologie Stack zur Erkennung von IoAs in verschiedenen Angriffsphasen. Es handelt sich dabei keineswegs um statische Technologien, sondern sie werden ständig mit neuen Angriffsmustern und -techniken aktualisiert, die vom Threat Hunting and Investigation Service (THIS) entdeckt werden.



Die Gegner wenden zunehmend Living-Off-the-Land-Techniken an, die in den meisten Angriffen vorkommen. Es gibt vier Hauptkategorien:

- Angriffe mit Dual-Use-Software, wie z.B. PsExec.
- Speicherbasierte Angriffe, wie z.B. Code Red.
- Angriffe mit Persistenztechniken, wie z.B. mit Visual Basic Script in der Windows Registrierung.
- Angriffe über nicht-binäre Dateien, wie z.B. Office-Dokumente mit Makros oder Scripten.

Unter den vielen Angriffsindikatoren, die die der Agent erkennt, finden wir folgende Kategorien:

1. IoAs von Exploits in the wild

Durch diese Verhaltens- und Kontext-IoAs werden sowohl Exploits in the wild, als auch Exploit-Kits erkannt und vor der Ausführung blockiert, wodurch einer der Haupteintrittsvektoren für Angreifer geschlossen wird.

Darüber hinaus werden proprietäre Firewall-Technologien eingesetzt, um Virtual Patching-Funktionen am Endpoint zu implementieren, die durch die Überwachung des eingehenden Datenverkehrs Versuche zur Ausnutzung von Schwachstellen erkennen und blockieren.

Diese Technologie wird beispielsweise zur Identifizierung und Blockierung von Exploits gegen die BlueKeep-Schwachstelle eingesetzt, bei denen innerhalb einer RDP-Sitzung bestimmte Verbindungen aufgebaut werden. Diese Verbindungen, sofern sie nicht blockiert werden, ermöglichen einem Angreifer die entfernte Ausführung von beliebigen Code (RCE).

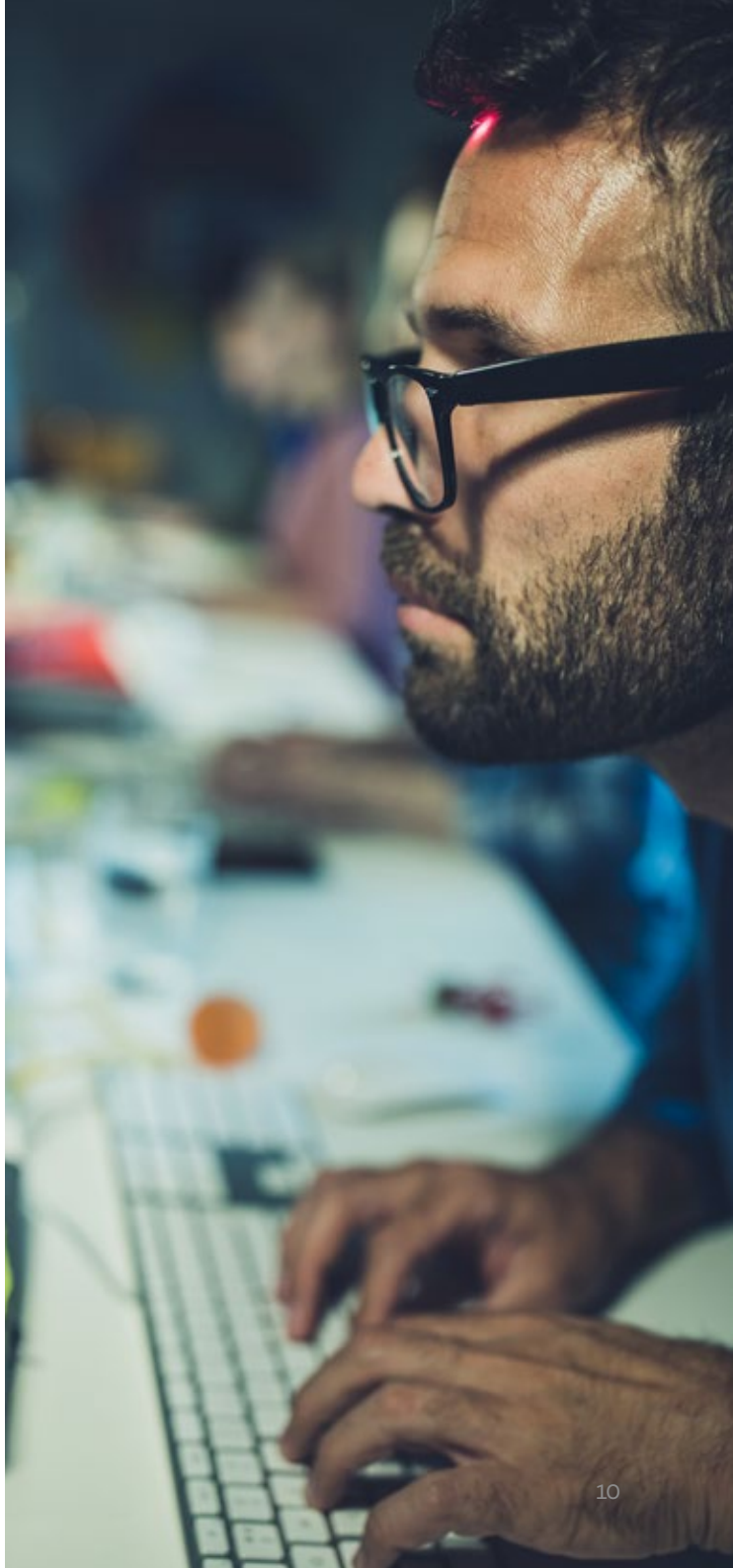
Die Virtual Patching-Technologie erkennt solche Verbindungen und weist sie automatisch ab. Diese Vorgänge werden in der Cloud aufgezeichnet und in der Weboberfläche von Panda Adaptive Defense 360 dargestellt, so dass Administratoren sofort eingreifen können.

Als Eindämmungsmaßnahme können sie Konfigurationsänderungen vornehmen: beispielsweise die Aktivierung der Network Level Authentication (NLA), die Deaktivierung nicht notwendiger RDP-Services an den Endpoints oder das Patchen der Systeme, wenn möglich, um die Angriffsfläche effektiv reduzieren.

2. In-Memory IoAs: dynamische Anti-Exploit-Technologie

Panda Adaptive Defense 360 verfügt über eine dynamische Anti-Exploit-Technologie.

Diese Technologie, die völlig unabhängig von den in Microsoft EMET implementierten Techniken ist, nutzt keine morphologische Analyse der Dateien oder die Implementierung von Schutzebenen, die zu den in Windows fehlenden hinzugefügt werden (ASR-, DEP-, EAF-Techniken usw.), oder zielt auf die Erkennungen spezifische bekannter Schwachstellen ab. Diese Techniken reichen nicht aus, um Cyber-Angriffe zu stoppen, die darauf ausgelegt sind, Input-Vektoren auszunutzen, die mit Zero-Day-Schwachstellen erstellt wurden.



Die dynamische Anti-Exploit-Technologie überwacht das interne Verhalten der Prozesse und sucht nach Anomalien. Dies ist unabhängig von dem im Angriff verwendeten Exploit, sehr effektiv und wird durch eine proprietäre Speicher-Framework-Analyse ergänzt, die zu bestimmten Zeiten einen Speicherabschnitt inspiziert, nachdem bestimmte Ereignisse oder Verhaltensweisen ausgelöst wurden. Auf diese Weise können neue Angriffsmuster unterschiedlicher Art entdeckt werden.

Diese Technologien können wirksam vor jeder Art von Exploit schützen, insbesondere vor Zero-Day-Exploits, die auf folgende abzielen können:

- **Schwachstellen in Webbrowsern:** Internet Explorer, Firefox, Chrome, Opera und andere.
- **Häufige genutzte Anwendungen, die** bei gezielten Angriffen verwendet werden, wie z.B. Java, Adobe Reader, Adobe Flash, Microsoft Office, Multimedia-Player, etc.
- **Schwachstellen in nicht unterstützten Betriebssystemen**, wie zum Beispiel Windows XP und andere.

3. IoAs zur Erkennung von Living-off-the-Land-Angriffen und böswilliger Nutzung von Verwaltungstools.

Um diese Art von Indikatoren zu erkennen, werden Ereignisse von Skripten, die von Skript-Interpretern ausgeführt werden, korreliert (Powershell, Visual Basic, Javascripts, etc.), sowie Makro/Skripte in MS Office, WMI-Aktivität, etc.

Weitere Indikatoren sind enthalten, um die Ausführung bestimmter Prozesse durch andere je nach Kontext zu verweigern, wobei Angriffe ohne Malware mit Hilfe von administrativen Werkzeugen und Befehlszeilensequenzen blockiert werden. Auch einige andere In-Memory-Angriffe werden erkannt, wie z.B. das Erkennen von Code-Injektionen in den Speicher ohne Dateien auf der Festplatte.

5. Der Threat Hunting Service
Erkennen des Unerkennbaren

Der in Panda Adaptive Defense und Panda Adaptive Defense 360 enthaltene Threat Hunting and Investigation Service wird vollständig von den Analysten von Panda Security betrieben und verwaltet.

Sie arbeiten mit einer Cloud-nativen, proprietären Plattform für Threat Hunting und Incident Response, um L1-, L2- und L3-Analysten sowie Hunter und Responder zu koordinieren und so MTTD und MTTR (Mean Time To Detect und Mean Time To Respond) zu minimieren.

Analysten können zudem neue Regeln erstellen, um neue IoAs abzubilden. Diese vertrauenswürdigen IoAs können an die Endpoints übertragen werden und schützen so früh wie möglich vor Angreifern, die andere Kontrollmechanismen mit Techniken wie fileless Attacks, LotL, etc. umgehen.

Diese neuen Angriffsindikatoren sind das Ergebnis eines kontinuierlichen Prozesses: zur Aufdeckung von Bedrohungsakteuren, der sich auf fortschrittliche Datenanalysen, unsere eigene Threat Intelligence sowie das Fachwissen unserer Analysten stützt.

Dieser Service beinhaltet die gesamte Cyber Intelligence, die wir dank unserer jahrelangen Erfahrung in der Bedrohungsforschung perfektionieren konnten. Entscheidende Faktoren waren dabei die Aufzeichnung des Verhaltens von Anwendungen, Benutzern und Maschinen seit mehr als 30 Jahren, sowie unsere Allianzen mit internationalen Organisationen wie der Cyber Threat Alliance, mit der wir Indikatoren für Bedrohungen (IoAs und IoCs) und die entsprechenden Reaktionen austauschen.

6. Zertifizierungen, Auszeichnungen und Mitgliedschaften

Panda Security erhält regelmäßig Auszeichnungen für Schutz und Leistung von Virus Bulletin, AV-Comparatives, AV-Test und NSSLabs. Panda Adaptive Defense hat bei der Bewertung für den Common Criteria-Standard die EAL2+-Zertifizierung erhalten.

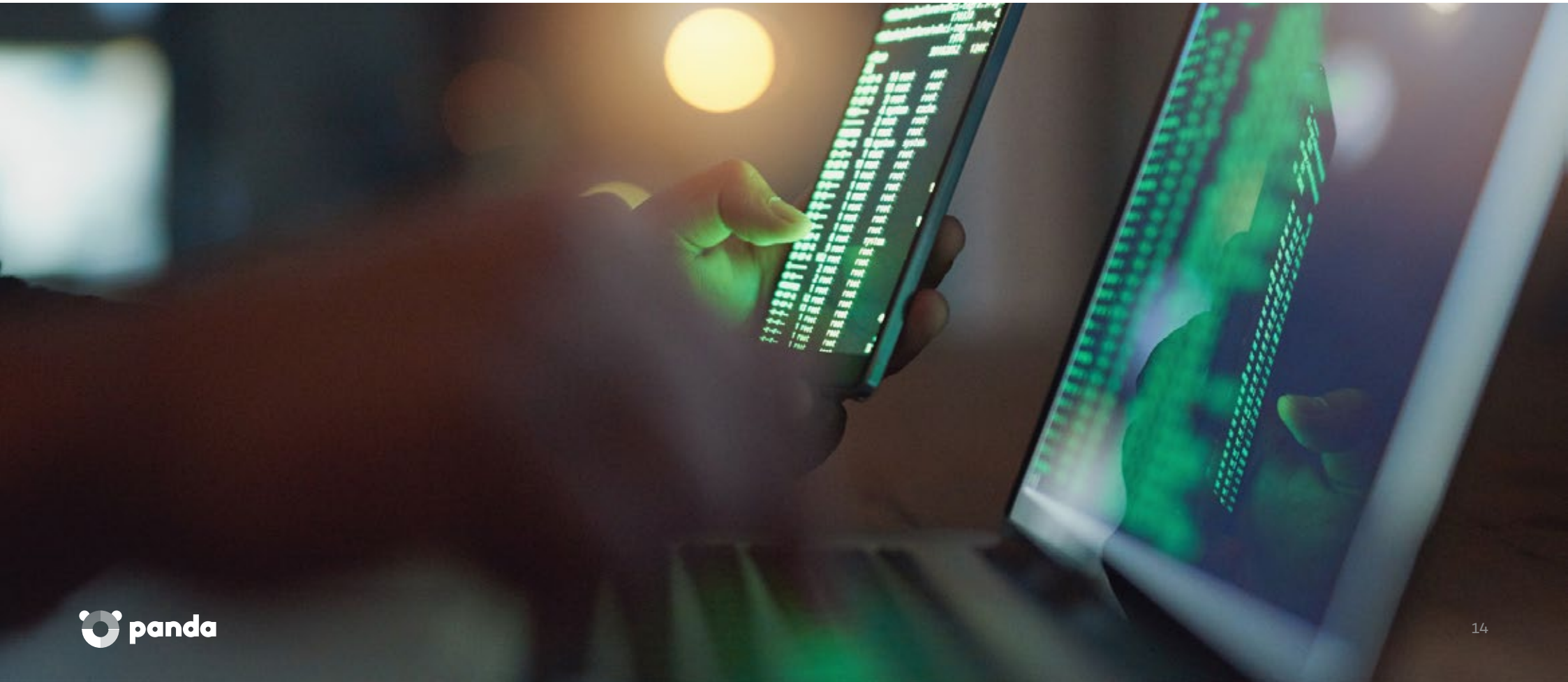
Panda Security wurde im Gartner Magic Quadrant für Endpoint Protection-Plattformen (EPP) 2018 als „Visionär“ anerkannt.

MITGLIED

Anmerkungen:

1. Angriffe auf die Supply-Chain sind eine neue Bedrohung, die auf Entwickler und Softwareanbieter abzielt. Ziel ist es, durch Infizierung von legitimen Anwendungen auf Quellcodes zuzugreifen, Prozesse zu erstellen oder Mechanismen zu aktualisieren, um Malware zu verbreiten.

2. MITRE ATT&CK Framework: **https://attack.mitre.org/**



Panda Adaptive Defense 360

Limitless Visibility, Absolute Control

pandasecurity.com

panda

Weitere Informationen unter:

pandasecurity.com/de/business/adaptive-defense/

Rufen Sie uns an:

02065 961-200

Kontaktieren Sie uns per E-Mail:

vertrieb@de.pandasecurity.com

panda