Mathematik gegen Malware

„Die Mathematik als Instrument der Erkenntnis ist leistungsfähiger als alles Andere, dass uns durch den Menschen hinterlassen wurde.“

– **René Descartes,**
französischer Philosoph, Mathematiker und Wissenschaftler

Gibt es Einen Besseren Weg?

Wie Cylance® die Mathematik nutzt, um Malware zu besiegen

Das Problem ist, auch wenn es nur wenige zugeben, dass die Sicherheits-Teams der Unternehmen eine Burg zu verteidigen versuchen, die mit Geheimgängen und Sicherheitslücken durchlöchert ist. Zu Hilfe gezogene Schutzbarrieren bleiben oftmals wirkungslos. Diese Schwachpunkte resultieren aus fehlerhaft programmierter oder technologisch veralteter Security Software, mangelhafter Hardware sowie von Insidern platzierter Hintertüren. Die daraus entstehende Erkenntnis ist, dass Angreifer ohne ernsthafte Gegenwehr den Kampf gewinnen.

Angriffe können unterschiedlichsten von unterschiedlichstem Ursprung und Motivation sein haben und schreiten in Komplexität und Technologie ungehindert voran. Teil dieser Evolution ist, dass moderne Bedrohungen typischerweise Schwachstellen in Anwendungen und Betriebssystemen ausnutzen, um vorhandene Sicherheitsbarrieren zum umgehen. Solche Angriffe post mortem zu entdecken ist äußerst schwierig und der präventive Schutz galt bisher als unmöglich.

Der menschliche Faktor

Um mit modernen Angriffen Schritt zu halten, müssen sich Security-Lösungen pausenlos weiterentwickeln, ohne ein menschliches Eingreifen zu erfordern. Hier kommt der Vorteil der Mathematik und des maschinellen Lernens zum Tragen. Wenn wir anhand von mathematischen Risikofaktoren objektiv einschätzen können, ob eine Datei gut oder bösartig ist, können wir mit diesem Wissen einer Maschine beibringen, in Echtzeit die richtige Entscheidung zu treffen.

Ein mathematischer und maschinenlernbarer Ansatz in der IT-Sicherheit kann unser Verständnis über die Klassifizierung und Ausführung von Dateien fundamental verändern.

Cylance verfolgt diesen Ansatz in seinen Produkten und unterscheidet sich damit grundlegend von allen anderen Anbietern von Sicherheitslösungen. Das Maschinenlernen hat sich als Teilbereich der künstlichen Intelligenz in vielen Industriezweigen wie Gesundheitswesen, Versicherungen und Hochgeschwindigkeitshandel an den Börsenplätzen etabliert, um dort enorme Datenmengen zu analysieren und automatisiert Entscheidungen zu treffen. Der Kern der Technologie von Cylance ist ein massiver und hochskalierbarer Datenprozessor, der ein hochentwickeltes, mathematisches Modell auf enorme Datenmengen in nahezu Echtzeit anwendet.

Anwendung von maschinellem Lernen auf die Klassifizierung von Dateien

In den letzten Jahrzehnten wurde Milliarden von Dateien erstellt – nützlich und bösartige. Über die Jahre haben sich strukturierte Ansätze bei der Erstellung von Dateien ergeben sowie Standards, welche die typische Gestalt einer Dateiart ausmachen. Natürlich gibt es viele unterschiedliche Dateiarten, jedoch sind einheitliche Ansätze und gemeinsame Merkmale vorhanden und die Entwicklung hat gemeinsame Dateisysteme, Computerarchitekturen und Betriebssysteme hervorgebracht.

Diese Gemeinsamkeiten und Eigenschaften manifestieren sich bei allen großen Softwareentwicklern, wie z.B. Microsoft® oder Adobe®, dank standardisierter

Entwicklungsprozesse. Angreifer können nun gleichermaßen diese bekannten Strukturen ebenso für Ihre Kampagnen ausnutzen.

Die Herausforderung ist es nun, all diese Eigenschaften aus Millionen von Dateien und Attributen auszuwerten, um herauszufinden, ob eine einzelne Datei guter oder bösartiger Natur ist.

Aufgrund der enormen Datenmenge, die berücksichtigt werden muss, um eine Tendenz zu erkennen, ist die Auswertung durch Menschen ineffizient und es ist unmöglich, mit dem heutigen Stand der Digitalisierung Schritt zu halten. Tatsächlich aber verlassen sich die meisten Security-Anbieter auf menschliche Analyse und beschäftigen hunderte von Mitarbeitern, um Millionen von Dateien zu klassifizieren und Malware-Analyse zur Signaturerstellung zu betreiben und zu entscheiden, ob eine Datei gut oder schlecht ist.

Menschen haben von Natur aus keine besondere einseitige Spezialisierung und Ausdauer, um hochkonzentriert diese enormen Datenmengen akkurat und schnell zu verarbeiten. Viele Anbieter ergänzen in der Analytik die Verhaltens und Verwundbarkeitsanalyse sowie die Auswertung von „Indicators of Compromise“ (IOC). Diese Techniken haben aber den grundsätzlichen Schwachpunkt, dass die Analyse aus der menschlichen Perspektive und Bewertung heraus vorgenommen werdenund Menschen dazu neigen, Sachverhalte nur zu sehr vereinfacht zu verarbeiten.

Maschinen unterliegen dieser Schwäche nicht und das maschinelle Lernen und das Auswerten großer Datenmengen (Data Mining) erfolgt Hand in Hand. Maschinelles Lernen fokussiert sich auf eine Vorhersage basierend auf Eigenschaften und Merkmalen, die von vorhandenen Massendaten gelernt wurden. Auf diese Weise unterscheidet Cylance maliziöse Dateien von sicheren und vertrauenswürdigen. Data Mining erkennt neue Eigenschaften und Merkmale in Datensätzen, die dann dem zukünftigen Maschinenlernprozess zugeführt werden.

Maschinelles Lernen nutzt einen Vier-Phasen-Prozess: Sammlung, Extraktion, Lernen und Klassifizierung.

„Maschinelles Lernen ist ein Oberbegriff für die „künstliche“ Generierung von Wissen aus Erfahrung: Ein künstliches System lernt aus Beispielen und kann diese nach Beendigung der Lernphase verallgemeinern. Das heißt, es werden nicht einfach die Beispiele auswendig gelernt, sondern es „erkennt“ Muster und Gesetzmäßigkeiten in den Lerndaten. So kann das System auch unbekannte Daten beurteilen.“´ –Wikipedia

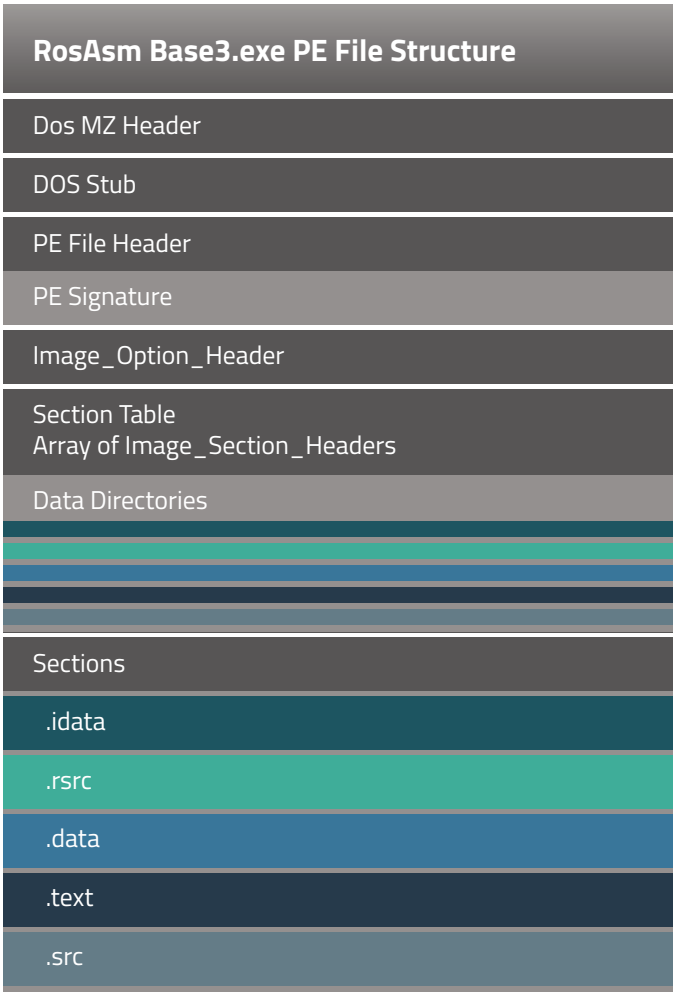
Sammlung

Wie bei der DNS-Analyse oder versicherungsmathematischen Berechnungen beginnt die Dateianalyse mit der Sammlung immenser Datenmengen. In unserem Falle sind dies hauptsächlich ausführbare Dateien, PDFs, Microsoft Word® Dokumente, Java, Flash usw. Diese Dateien werden über Feeds von Industriepartnern sowie öffentlichen und eigenen Datensammlungen zugeführt. Kunden haben auf Wunsch die Möglichkeit, Malware auch automatisiert von ihren Systemen an Cylance zur weiteren Analyse mit Cyclance-Agenten zu übertragen.

Folgendes ist bei der Datensammlung von besonderer Wichtigkeit:

- es werden Dateien mit relevanter Größe gesammelt
- es werden Dateien gesammelt, die eine größtmögliche Bandbreite von Dateitypen und Datei-Erstellern (oder auch Ersteller-Gruppen wie Microsoft® oder Adobe®) darstellt, die Sammlung NICHT VERFÄLSCHT hat, indem zu viele bestimmte
- die Datensammlung muss ausgewogen sein und nicht einseitig sein, weil z.B. nur Dateien eines sehr speziellen Typs gesammelt werden.

Sobald die Dateien zugeführt wurden, werden Sie analysiert und in drei Kategorien unterteilt:: bekannt, geprüft unschädlich/gültig bekannt, geprüft und schädlich sowie unbekannt.



Es ist zwingend erforderlich, dass diese Kategorien ordnungsgemäß gepflegt werden, da Falscheinstufungen zu einem Ungleichgewicht in der Bewertungsbasis führen können.

Extraktion

Die nächste Stufe des Maschinenlernprozesses ist die Extraktion von Merkmalen und Attributen und sie unterscheidet sich grundsätzlich von der Verhaltens- und Malware-Analyse traditioneller Schadcode-Analysten.

Statt auf die Dinge zu achten, die ein Analyst für schädlich erachtet, nutzt Cylance enorme Rechenleistung und Data-Mining-Techniken um das größtmögliche Spektrum an Dateimerkmalen einer Datei zu erhalten. Diese Merkmale können sehr einfach sein, wie die Dateigröße einer ausführbaren Datei oder dem verwendeten Compiler, aber auch komplex, indem z.B. die ersten logischen Transaktionen des ausführbaren Codes analysiert werden. Wir extrahieren dabei die kleinsten anatomischen Merkmale abhängig von den zugrundeliegenden Dateitypen (.exe, .dll, .com, .pdf, java, .a, .doc, .xls, .ppt, etc.).

Die möglichst breit aufgestellte Identifizierung von Attributen eliminiert die eindimensionale Einstufung anhand nur eines Kriteriums (Prüfsumme/File-Hash) der klassischen manuellen Klassifizierung. Die Auswertung hunderttausender Merkmale erschwert es einem Angreifer signifikant, auf einfache Weise einen neuen Schadcode zu produzieren, der nicht durch Cylance erkannt wird. Der Aufwand und die Kosten für den Angreifer steigen, da über Datei-Mutation zwar eine neue Variante (mit einem neuen File-Hash) entsteht, für die keine Signatur bereitsteht, deren grundsätzlichen Merkmale sich aber nach wie vor nicht wesentlich geändert haben.

Das Ergebnis dieses Prozesses zur Attributbestimmung und-extraktion, das Datei-Genom, gleicht dem Analyse-Ergebnis von Biologen z.B. für das menschliche Genom. Dieses Dateigenom ist die Basis für die Entscheidung, welche mathematischen Modelle herangezogen werden können um zu bestimmen, welchem Charakter die Datei entspricht,- so, wie die DNS-Analyse Rückschlüsse auf die Charakteristiken und das Verhalten einer Zelle erlaubt.

Lernen

Sobald sämtliche Attribute gesammelt wurden, werden die Datensätze normalisiert und in numerische Werte umgewandelt, die in den statistischen mathematischen Modellen verwendet werden können. An dieser Stelle setzt die Vektorisierung ein und das maschinelle Lernen wird angewendet. Die Nachteile und Störfaktoren der manuellen Analyse (Falschbeurteilung und langsame Verarbeitung) entfallen. Das mathematische Model wird dann von Cylance-Mathematikern anhand der Millionen gewonnen Merkmale entwickelt und geprüft, um eine akurate Vorhersage zur Schädlichkeit einer Datei zu erhalten.

Das Ergebnis sind Dutzende Modelle. Dabei werden viele Modelle parallel entwickelt, einige verworfen, und nur die effektivsten Modelle werden weiterentwickelt und danach in unterschiedlichen Stufen auf Wirksamkeit geprüft.

Die erste Stufe beinhaltet nur einige Millionen bekannter Dateien, während spätere Stufen mehrere Dutzend Millionen Dateien aller Klassifikationen beinhalten. Das finale Modell wird dann aus der Testumgebung in die Cylance-Produktionsumgebung übertragen.

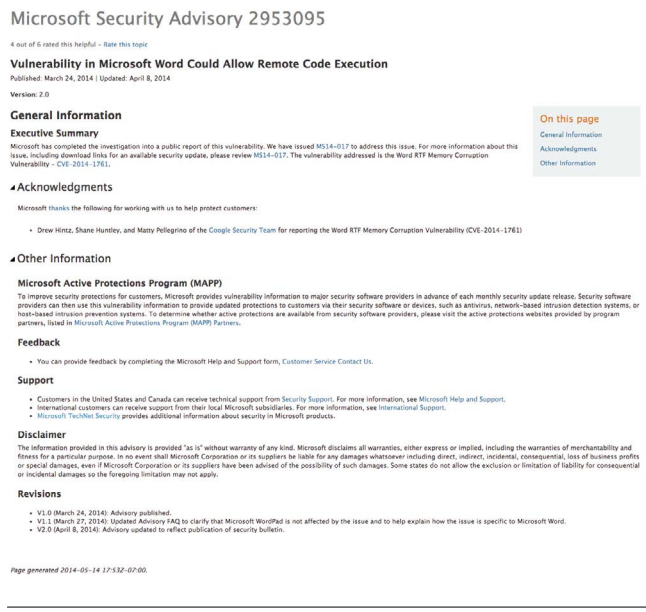
Zu beachten ist dabei, dass Cylance für jede Datei immer tausende von Attributen überprüft, um Schadcode von erwünschten Dateien zu unterscheidet. So identifiziert Cylance Malware unabhängig davon, ob sie gepackt wurde, oder ob sie bekannt oder unbekannt ist - mit einer unerreichten Treffsicherheit. Eine einzelne Datei wird in eine astronomische Anzahl von Merkmalen geteilt und hunderten Millionen anderer Dateien gegenübergestellt, um eine Entscheidung zu treffen, ob diese der Norm entspricht.

Klassifizierung

Nachdem die statistischen Modelle erstellt wurden, können sie in der Cylance Engine verwendet werden, um unbekannte Dateien (die bisher nicht gesehen oder analysiert wurden oder anderweitig durch eine White-oder Blacklist behandelt wurden) zu klassifizieren.

Die Analyse dauert nur Millisekunden und ist aufgrund der hohen Bandbreite der berücksichtigen Dateimerkmale sehr präzise. Aufgrund der Analyse durch statistische Modelle ist das Resultat kein absoluter Wert sondern ein „Confidence Score“, anhand dessen der Kunde einfach die Entscheidung treffen kann, ob die Datei blockiert, in Quarantäne gestellt, überwacht oder weiter analysiert werden soll.

Ein großer Unterschied zwischen dem maschinellen Lernen und dem traditionellen Malware-Analyse-Ansatz liegt darin, dass die Modelle nicht nur gute und schädliche Dateien erkennen, sondern auch verdächtige. Sobald der Confidence Score niedriger als 20% ist und keine weiteren eindeutigen Malware-Merkmale vorliegen handelt es sich um Software, die ein Unternehmen genauer betrachten sollte. Hier handelt es sich häufig z.B. um administrative



Microsoft Security Advisory 2953095

4 out of 6 rated this helpful – Rate this topic

Vulnerability in Microsoft Word Could Allow Remote Code Execution

Published: March 24, 2014 | Updated: April 8, 2014

Version: 2.0

General Information

Executive Summary

Microsoft has completed the investigation into a public report of this vulnerability. We have issued MS14-017 to address this issue. For more information about this issue, including download links for an available security update, please review MS14-017. The vulnerability addressed is the Word RTF Memory Corruption Vulnerability - CVE-2014-1761.

On this page
General Information
Acknowledgments
Other Information

Acknowledgments

Microsoft thanks the following for working with us to help protect customers:

- Drew Hintz, Shane Huntley, and Matty Pellegrino of the Google Security Team for reporting the Word RTF Memory Corruption Vulnerability (CVE-2014-1761)

Other Information

Microsoft Active Protections Program (MAPP)

To improve security protections for customers, Microsoft provides vulnerability information to major security software providers in advance of each monthly security update release. Security software providers can then use this vulnerability information to provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. To determine whether active protections are available from security software providers, please visit the active protections websites provided by program partners, listed in Microsoft Active Protections Program (MAPP) Partners.

Feedback

- You can provide feedback by completing the Microsoft Help and Support form, Customer Service Contact Us.

Support

- Customers in the United States and Canada can receive technical support from Security Support. For more information, see Microsoft Help and Support.
- International customers can receive support from their local Microsoft subsidiaries. For more information, see International Support.
- Microsoft TechNet Security provides additional information about security in Microsoft products.

Disclaimer

The information provided in this advisory is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions

- V1.0 (March 24, 2014): Advisory published.
- V1.1 (March 27, 2014): Updated Advisory FAQ to clarify that Microsoft WordPad is not affected by the issue and to help explain how the issue is specific to Microsoft Word.
- V2.0 (April 8, 2014): Advisory updated to reflect publication of security bulletin.

Page generated 2014-05-14 17:53Z-07:00.

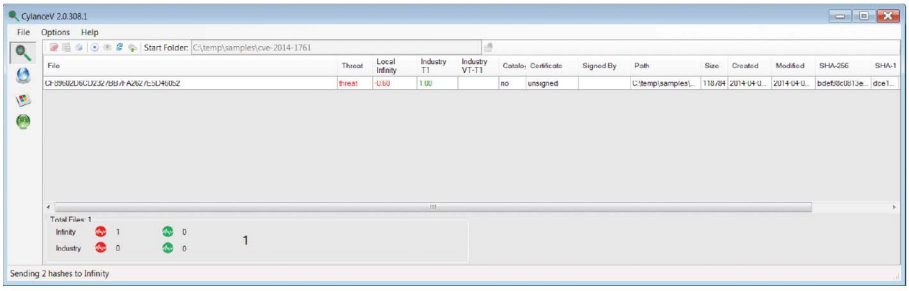
CylancePROTECT® Schlüsselfunktionen

- Schutz und Erkennung von bislang nicht erkennbaren Advanced Threats
- Cloud-verwaltet-aber nicht abhängig von der Cloud-auch für Umgebungen mit sensiblen Daten oder Bereiche ohne Internetanbindung geeignet
- Keine täglichen Signatur- (DAT-) Updates, für die gewöhnlich ein ständiger Zugriff auf das Netzwerk/ Internet benötigt wird
- Extrem niedriger Ressourcenbedarf (RAM und CPU Zeit); der Laufzeitschutz verbessert die Systemleistung erheblich, insbesondere im Vergleich mit traditionellen Lösungen
- Einfach auszurollen und zu managen, über ein intuitives Web Interface

Werkzeuge, die Anwender nutzen, um Sicherheitsrichtlinien oder Mechanismen zu umgehen oder Systeme zu missbrauchen. Somit gibt es keine ungeschützte Grauzone mehr zwischen dem, was Malware-Analysten als Schadcode ansehen und Whitelist-Anbieter als gut/nützlich klassifizieren.

Cylance und die Bedrohungen der realen Welt

Cylance verhinderte den Microsoft Word RTF (CVE-2014-1761)-basierten Zero-Day Malware Angriff, bevor er im Feld gesehen wurde und ohne Vorkenntnisse. Cylance konnte die Malware bereits im März 2014 in Quarantäne stellen–im April wurde sie zum ersten Mal auf malwr.com gesichtet–worden, dort allerdings ist sie auch nur 4 von 51 AV-Herstellern bekannt. Die Cylance Engine erkannte den Exploit (a2fe8f03adae711e1d3352ed97f616c7) unmittelbar-ohne Updates oder Signaturen-wie in dem Screenshot auf Seite 4 gezeigt.

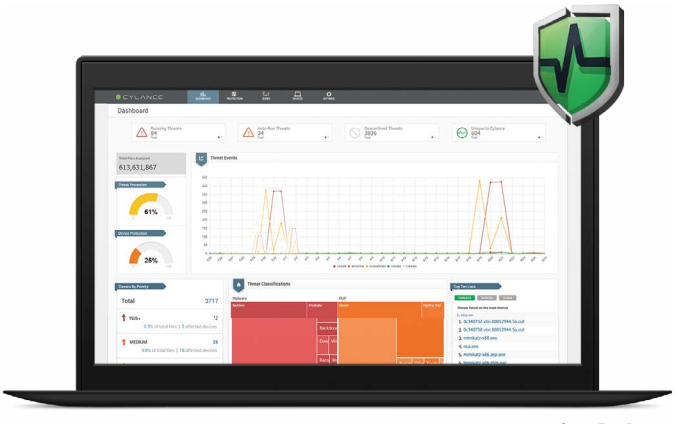


Zukunftsfähige Sicherheit

Durch die Anwendungen mathematischer Modelle auf dem Endpunkt übertrifft die Cylance-Engine alle herkömmlichen Methoden der Malware-Erkennung und Prävention mit Leichtigkeit. Unsere Mission ist es, die Ausführung von bösartigen Dateien zu stoppen, bevor sie Schaden anrichten können. Mit diesem Ansatz bleibt der Endpunkt sicher, selbst wenn die Datei auf der Festplatte vorliegt.

CylancePROTECT®

CylancePROTECT ist unsere Lösung, die Möglichkeiten der Cylance Engine nutzt, um die Ausführung von Advanced Persisten Threats (APT), Malware und Exploits zu verhindern - in Echtzeit und auf jedem Endpoint einer Organisation.



CylancePROTECT bietet Echtzeit-Erkennung und Prävention von Malware. Es arbeitet anhand der Analyse einer potentiellen Malware-Dateiausführung sowohl im Betriebssystem als auch in den Speicherbereichen und kann so auch die Übergabe von maliziöser Payload verhindern. Der Arbeitsspeicher-Schutz arbeitet, ohne die Leistung des Systems negativ zu beeinflussen und stärkt die dem Betriebssystem eigenen Schutzmechanismen wie DEP, ASLR und EMET. Er ergänzt mit einem zusätzlichen Schutzwall, der bestimmte Verhaltensmuster erkennt und stoppt, die typischerweise von Exploits angewendet werden.

Diese zwei Kernfunktionen werden von einer Vielzahl zusätzlicher Funktionen ergänzt, die Unternehmen benötigen, u.a.:

Über Cylance

Cylance ist das erste Unternehmen, das für die Cyber-Security künstliche Intelligenz, Algorithmik und maschinelles Lernen anwendet und damit die Art und Weise signifikant und nachhaltig verbessert, wie Unternehmen, Behörden und Regierungen sowie Endnutzer proaktiv die schwierigsten Sicherheitsprobleme der Welt lösen. Mit einem bahnbrechenden, prädiktiven Analyseprozess identifiziert Cylance schnell und präzise, welche Dateien sicher sind und welche eine Bedrohung darstellen, und klassifiziert nicht einfach nur in Black- oder Whitelists. Durch die Kopplung von komplexem maschinellen Lernen und künstlicher Intelligenz mit einem einzigartigen Verständnis für die Denkweise eines Hackers bietet Cylance die Technologien und Dienstleistungen an, die wirklich prädiktiv und präventiv gegen fortgeschrittene Bedrohungen wirken.

- Granulare Whitelisten und Blacklisten
- Audit-Mode (nur erkennen und alarmieren)
- Schutz vor Manipulation durch Anwender (Self-Protection)
- Vollständige Kontrolle über Konfigurationen und Updates über die Management-Konsole

CylanceV™

CylanceV ist ein Incident Response- und Forensik-Werkzeug, welches Kunden eine nahtlose Integration in SOC, CSIRT, Helpdesk usw. ermöglicht. Es ist ein kompaktes und leicht zu integrierendes Werkzeug zur Dateianalyse und skaliert in allen Leistungsbereichen.

Es wird in zwei Formen angeboten, zum einen als REST API, welches direkten Zugang zur Cylance Engine ermöglicht. Die API kann z.B. über Python eingebunden werden (Beispiele hält Cylance für Sie bereit) und bindet die Cylance-Secure Cloud in die Analyse ein.

Die zweite Form ist ein lokal zu verwendendes Programm, das die Attribut-Extraktion und die statistischen Modelle beinhaltet und auf Windows oder Linux verwendet werden kann. Hierbei erfolgt die Analyse lokal, ohne dass Dateien in die Cylance Secure Cloud übertragen werden müssen.

Somit stellt CylanceV das ideale Werkzeug zur unternehmensweiten schnellen und zielgerichteten Jagd nach Malware dar, welches auf maschinellem Lernen basiert.

Cylance Consulting

Das Cylance Consulting Expertenteam unterstützt Unternehmen auf verschiedene Weise. Zum einen kann es vorhandene Schwachstellen aufdecken, bereits manifestierte und bisher unerkannt gebliebene Malware aufspüren, und einen sicheren Betriebszustand herstellen, Best-Practice-Richtlinien bei der Einrichtung der Lösung anwenden, um Angriffe zu erkennen – und zu verhindern – bevor sie Schaden anrichten können.

Verfügbare Dienstleistungen:

- Kompromittierungs-Audits
- Penetrationstest
- Computer-Forensik
- Spezialisierte Dienstleistungen für Betreiber kritischer Infrastrukturen, Embedded Systems, Industrial Control Systems (ICS)
- Sichere Anwendungsentwicklung

Das Beratungsteam von Cylance nutzt die Power der Cylance-Engine für alle Dienstleistungen, wodurch die Berater umfassende Einblicke erhalten und Analysen durchführen können, was anderen Anbietern nicht möglich ist.

Zusammenfassung

Cylance ist überzeugt, dass mathematische Modelle, künstliche Intelligenz und maschinelles Lernen der Schlüssel zu einer sicheren Zukunft sind. Alle Produkte und Dienstleistungen, die wir anbieten, sind direkt mit der Cylance-Engine verknüpft, um einzigartige Treffsicherheit und einen tiefen Einblick in die Landschaft der modernen IT-Sicherheitsbedrohungen zu geben. Das kontinuierliche Lernen und Trainieren immer neuer Daten in die Cylance-Engine stellt sicher, dass die Lösung immer zukunftssicher ist, ohne ihre Effizienz im Laufe der Zeit zu verlieren–auch dann nicht, wenn die Angreifer ihre Strategien und Taktiken ändern.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE™

20161129