HP WOLF SECURITY

HP Endpoint Security Task Isolation – ein anderer Security Ansatz?

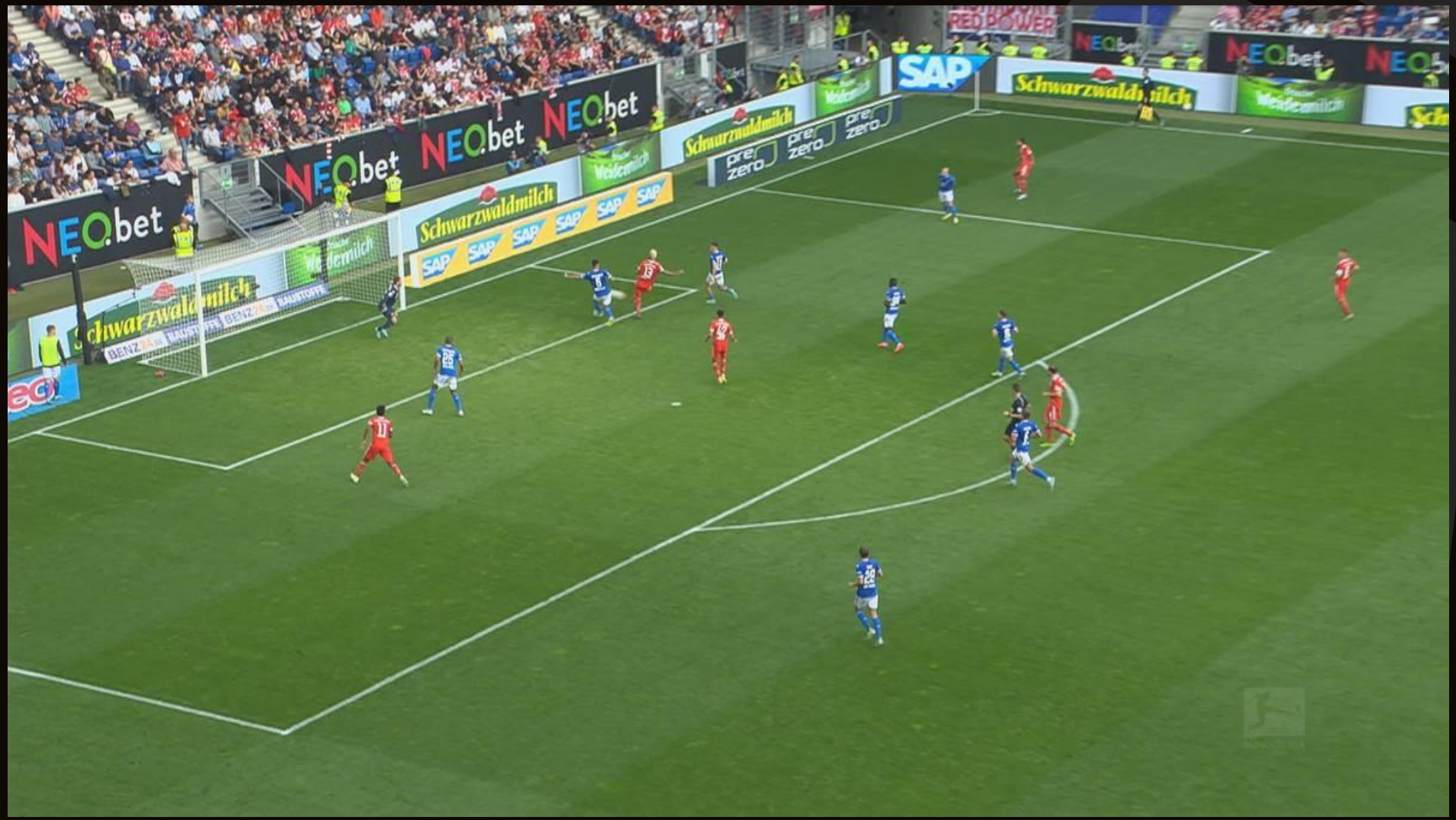
heinz.maeurer@hp.com

HP WOLF SECURITY

IT Security – Allgemein betrachtet

HP WOLF SECURITY

IT Security ist wie Fussball



HP WOLF SECURITY

Etwas Statistik

203 Milliarden Euro ist eine große Zahl. So hoch beziffert der Branchenverband Bitkom den Schaden für die deutsche Wirtschaft, der dieses Jahr durch Cyberkriminalität entsteht.

Steuereinnahmen des Bundes in 2022
328,4 Milliarden Euro

HP WOLF SECURITY

Etwas Statistik

Aufkommende Trends für 2023

- Angriffe unterhalb des Betriebssystems
- Geräte mit Fernzugriff mehr im Fokus
- Drucker

HP WOLF SECURITY

Etwas Statistik

In 2021 wurden in Deutschland rund 6,2 Milliarden Euro für IT-Sicherheit ausgegeben. Bis 2025 sollen rund 8,9 Milliarden Euro. (Quelle Statista 25.01.22)

HP WOLF SECURITY

Wohin geht das Geld?

EDR, XDR, NDR...

Email Security

Secure Web Gateway

SIEM, SOAR, SOC

PAM

DLP/DLD

Prozessoptimierung?

Mitarbeiterqualifikation?

Hardware Sicherheit?

Supply Chain Sicherheit?

HP WOLF SECURITY

“If you ever do, what you ever did, you will ever get, what you ever got!“

Henry Ford

HP WOLF SECURITY

2 Treffer:

LockBit 3.0 – Eine Ransomware as a Service Gruppe

LockBit sei eine Ransomware-as-a-Service-Gruppe (RaaS), welche von der Entwicklung der Ursprungsversion bis hin zur aktuellen Version 3.0 mehrfach Modifikationen durchlaufen habe. Als Teil des Einschüchterungsprogramms beziehe sich LockBit 3.0 stets auf die Datenschutz-Grundverordnung (DSGVO).

Auch zu den Gründen, wie Prophete als einer der größten Fahrradhersteller Deutschlands in die Insolvenz rutschen konnte, gibt es neue Erkenntnisse. Insolvenzverwalter Sack erklärt: „Am 25. November vergangenen Jahres wurde Prophete Opfer eines Cyberangriffs. Der Angriff führte im Ergebnis dazu, dass für rund drei Wochen keinerlei Produktion, Rechnungsstellung und Auslieferungen erfolgen konnten. Die dadurch entstandenen Verluste wollte niemand mehr tragen.“

Was kostet ein Hack?

Malware für weniger als 10 Euro und in gebrauchsfertigen Kits: Cyberkriminalität wird aus dem "Dark Web" vertrieben

CaaS

Cybercrime as a Service

Was kostet die Beseitigung?

Kostenfaktoren eines Cyberangriffs für Unternehmen:

- Produktivität im Unternehmen findet bei **23 Tagen IT-Ausfall** ca. 17 Werktage nicht statt.
- **Gehälter müssen ohne mögliche Gegenleistungen gezahlt werden**, da Mitarbeiter nicht arbeiten können.
- **Cashflow Probleme** können auftreten, da keine Rechnungen und Forderungen bezahlt werden können.
- **Verträge und Lieferfristen können nicht eingehalten werden**, was zu Vertragsstrafen bei Kunden führen kann.
- Die **Wiederherstellung der Funktionsfähigkeit** durch einen spezialisierten Dienstleister ist nach einem Angriff sehr aufwendig und auch entsprechend kostspielig.
- **Kompromittierte Hardware** muss ggf. komplett ausgetauscht werden.

Quelle: https://inventry.de/kosten-cyberangriff/

HP WOLF SECURITY

Die weiteren Folgen...

Versicherer zu Cyberangriffen: Schäden "im Cyberspace nicht mehr versicherbar"
Versicherungsgesellschaften müssen immer mehr Geld zur Regulierung von Schäden durch Cyberattacken ausgeben. Solche Verträge seien bald nicht mehr finanzierbar.

HP WOLF SECURITY

Risiko Mensch

Inherentes Risiko

Die Schnittstelle zwischen Mensch und Maschine bleibt Einstiegstor Nummer 1 – mehr als 85% aller Angriffe starten beim Faktor Mensch. Denn: Mitarbeitende lassen sich auch beim Einsatz der vielfältigsten Tools immer ähnlich angreifen – über emotionale Manipulation und Social Engineering.

HP WOLF SECURITY

Wie HP unterstützen kann

Security ist in unserer DNA

Mehr als 20 Jahren Innovation im Bereich der Endpunktsicherheit

Festlegung von Industriestandards für Endgerätesicherheit
Etablierte Standards für TPM, BIOS, Firmware Resilience

HP LABS | TRUSTED COMPUTING GROUP | NIST National Institute of Standards and Technology | ISO

Wegweisende hardwaregestützte Sicherheit

Enge Sicherheitspartnerschaften, um den Stand der Technik in der Branche voranzutreiben (Intel®, AMD® und Microsoft®)

HP | Bromium

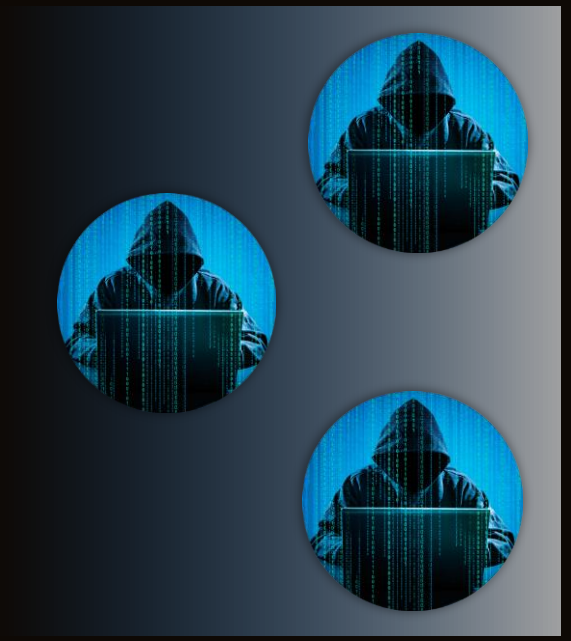
Verbesserte Sicherheit mit Bromium

HP WOLF SECURITY

HP Security Technologie: Wolf Security

HP WOLF SECURITY

Der Endpoint ist die erste Verteidigungslinie



HP WOLF SECURITY

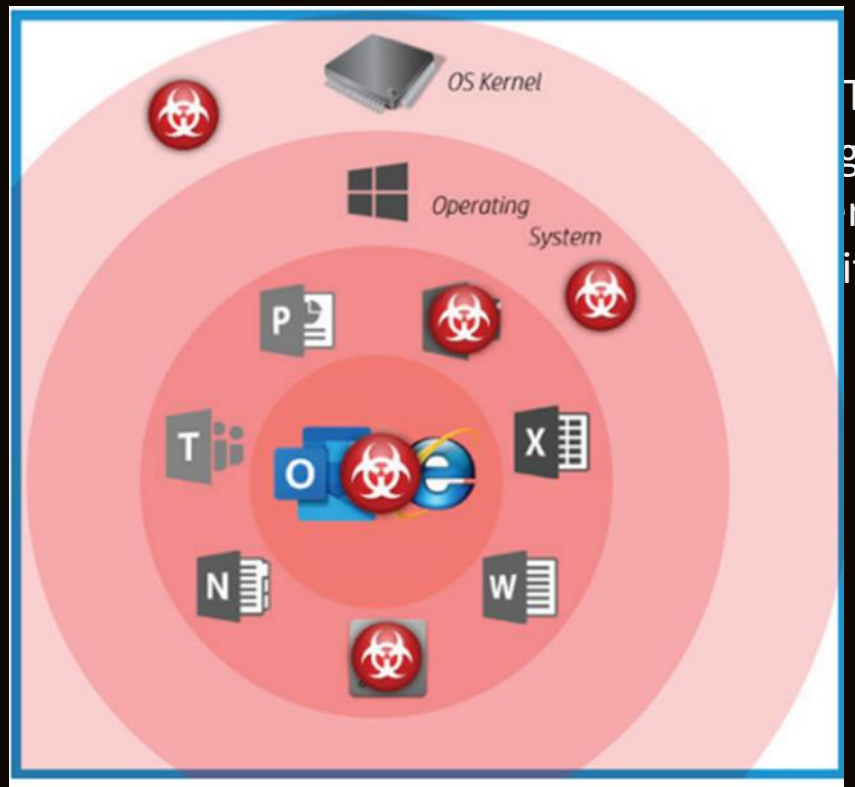
Hardware agnostische Technologie

Sure Click Enterprise

Threat Containment

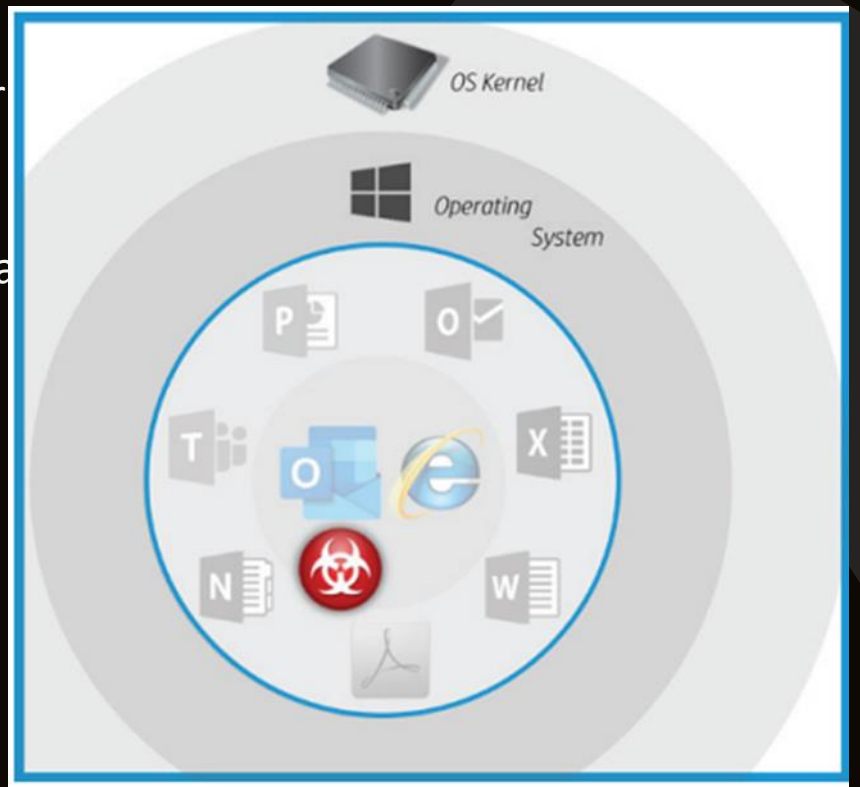
Sure Click Enterprise

Task Isolation



Herkömmliche Security-Lösungen ("Detection")

Task Isolier
gemeldete
rung.
it von Signa



HP Wolf Security: Isolierung über Secure Micro VM

ACTIONABLE DASHBOARDS AND REPORTS

Intuitive dashboards, plus drill-down for detailed reporting and threat analysis

Summary Report

Executives and Business Stakeholders

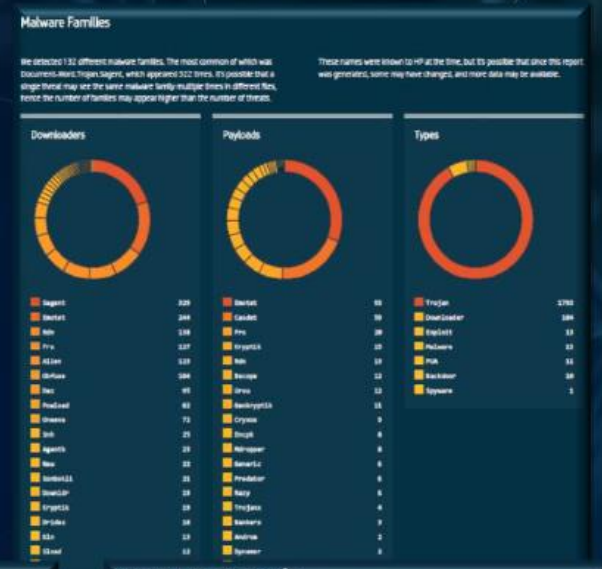
Operational Dashboard

Desktop Operations Team

Threat Dashboard

SOC Analysts and Incident Responders

Workflow-based threat triage with augmented threat intelligence provides relevant context for faster identification of true positives



*MITRE does not claim ATT&CK enumerates all possibilities for the types of actions and behaviors documented as part of its adversary model and framework of techniques. Using the information contained within ATT&CK to address or cover full categories of techniques will not guarantee full defensive coverage as there may be undisclosed techniques or variations on existing techniques not documented by ATT&CK.

HP WOLF SECURITY

UND WAS SAGT DAS BSI DAZU?

Ausführung potentiell gefährlicher Inhalte in gekapselten Umgebungen

Eine weitere Schutzschicht kann die Ausführung potentiell gefährlicher Inhalte in gekapselten Umgebungen, insbesondere (Mirco-) VMs, sein. Dabei wird eine temporäre Arbeitsumgebung gestartet, welche regelmäßig wieder gelöscht oder zurückgesetzt wird. Wenn Dokumente und Dateien aus unsicheren Quellen in einer virtuellen Umgebung (VM) geöffnet werden, müsste entsprechende Schadsoftware aus dieser VM ausbrechen, um das eigentliche System zu infizieren. Entsprechende (Micro-) VMs können beispielsweise auch das Öffnen von Links aus E-Mails abdecken. Selbstverständlich müssen auch entsprechende Lösungen, welche (Micro-) Virtualisierung anbieten aktuell gehalten werden. Zum einen können Betriebssystem-Updates zu Problemen führen, zum anderen kann nur so verhindert werden, dass Schadprogramme aus der VM ausbrechen können

Quelle: BSI Maßnahmenkatalog Ransomware - Arbeitspapier

HP WOLF SECURITY

Vielen Dank!

HP WOLF SECURITY

The following lists summarize the supported file extensions (or MIME types) which have been tested and certified to work.

	Supported File Formats
Microsoft Word	.doc,.docm,.docx,.dot,.dotm,.dotx,.rtf,.odt,.wps,.wpd,.wbk
Microsoft Excel	.xl,.xlsb,.xlsm,.xlsx,.xlam,.xltm,.xltx,.xls,.xlt,.xla,.xlm,.xlw,.csv,.ods,iqy,.slk
Microsoft PowerPoint	.ppt,.pptm,.pptx,.pps,.ppsm,.ppsx,.pot,.potm,.potx,.ppa,.ppam,.thmx,.odp
Adobe Acrobat Readers	.pdf
Archive Utility (ZIP)	.zip,.zipx,.jar,.rar,.arj,.7z,.cab,.tar,.xar,.bz2,.Z,.gz,.taz,.tbz,.tbz2,.tgz,.txz,.xz
Photoviewer	.jpg,.jpeg,.png,.bmp,.ico,.tiff,.tif,.dib,.wdp,.gif
Notepad	.txt,.log
Windows Media Player	.3g2,.3gp,.3gp2,.3gpp,.aac,.adt,.adts,.aif,.aifc,.aiff,.asf,.asx,.au,.avi,.m1v,.m2t,.m2ts,.m2v,.m3u,.m4a,.m4v,.mid,.midi, .mod,.mov,.mp2,.mp2v,.mp3,.mp4,.mp4v,.mpa,.mpeg,.mpg,.mpv2,.mts,.rmi,.snd,.ts,.tts,.wav,.wm,.wma,.wmv,.wmx,.wpl,.wvx
Browsers	.xml,.htm,.html
Scripts/Executables	.exe,.scr,.bat,.cmd,.hta,.js,.jse,.vbe,.vbs,.wsf,.ps1,.lnk