kaspersky BRING ON THE FUTURE

Sicherheit und unterbrechungsfreier Geschäftsbetrieb

Kaspersky Threat Data Feeds

Über das Produkt
Unsere Data Feeds werden aus zusammengeführten, heterogenen und äußerst zuverlässigen Quellen bezogen, darunter das Kaspersky Security Network, unsere eigenen Webcrawler, unser System zur Botnet-Überwachung (Überwachung von Botnets und ihrer Ziele und Aktivitäten rund um die Uhr, das ganze Jahr) sowie Spam-Fallen, Forschungsteams und Partner.

Dann werden sämtliche zusammengefassten Daten in Echtzeit sorgfältig untersucht und anhand verschiedener Aufbereitungsverfahren präzisiert, z. B. durch statistische Kriterien, Sandboxes, heuristische Engines, Similaritätstools, Erstellung von Verhaltensprofilen, die Validierung durch Analysten und die Verifizierung anhand von Whitelists.

Kaspersky Automated Security Awareness Platform

Über das Produkt
Die Automated Security Awareness Platform (ASAP) basiert auf der umfassenden Cybersicherheitskompetenz von Kaspersky und orientiert sich an anerkannten pädagogischen und psychologischen Erkenntnissen. Durch festgelegte Intervalle zwischen den einzelnen Lernaktivitäten wird sichergestellt, dass einmal erworbenes Wissen sich dauerhaft verfestigt.

Die Lektionen sind kurz und interaktiv aufgebaut, um die natürlichen Lern- und Denkmuster der Teilnehmer optimal zu unterstützen.

Für Administratoren ist Kaspersky ASAP eine einfache, unkomplizierte Möglichkeit, Schulungen durchzuführen. Sie profitieren von automatisierten Lernpfaden mit strukturierten Schulungen und einer Ergebnisauswertung auf Basis von Berichten und Analysen mit konkreten Handlungsempfehlungen.

Mehr Phishing-Bedrohungen in der COVID-19-Krise

Während die Welt sich mit der Coronapandemie auseinandersetzt, versuchen Cyberkriminelle verstärkt, die entstehenden sozialen Spannungen für sich zu nutzen. Laut unseren Daten stehen aktuell mindestens 5 % aller täglichen Phishing-Versuche in Verbindung mit COVID-19. Die Angreifer fälschen beispielsweise Nachrichten von internationalen Institutionen wie der Weltgesundheitsorganisation, um sich Spenden zu erschleichen oder Nutzer zum Download von Malware zu bewegen.

Durch die Integration von Threat Intelligence Feeds mit Informationen zu Phishing-URLs in vorhandene Sicherheitskontrollen wie SIEM-Systeme kann Ihr Sicherheitsteam effektiver auf Phishing-Bedrohungen reagieren. Solche Feeds ermöglichen nicht nur eine automatisierte Auswahl von Sicherheitswarnungen – sie liefern Ihrem Team zusätzlich auch genügend Kontext, um sofort entscheiden zu können, welche Warnungen eingehender untersucht oder für eine genauere Analyse und weitere Maßnahmen an Ihr Team für Vorfallreaktion weitergeleitet werden müssen.

Schutz für Ihr Unternehmen in der Krise

Kaspersky stellt seinen Phishing URL Data Feed jetzt 180 Tage lang kostenlos bereit.* Im Rahmen unseres Phishing Threat Data Feeds erhalten Sie einen Satz von URL-Masken für Phishing-Websites, einschließlich Kontextinformationen. Der Phishing Threat Data Feed umfasst Hunderttausende von Datensätzen und wird alle 10 Minuten aktualisiert.

Jeder Datensatz in jedem Data Feed wird mit umfangreichem Kontext angereichert (Bezeichnungen von Bedrohungen, Zeitstempel, Geolokalisierungsdaten, aufgelöste IP-Adressen infizierter Webressourcen, Hashes, Beliebtheit usw.). Kontextdaten eröffnen den Blick auf das große Ganze und ermöglichen die weitere Analyse und vielfältige Nutzung der Daten. Wenn die Daten in einen Kontext gesetzt werden, liefern sie schneller Antworten auf die Fragen „Wer?“, „Was?“, „Wo?“ und „Wann?“. Außerdem geben sie Aufschluss über Ihre Gegner, sodass Sie rechtzeitig Entscheidungen treffen und die richtigen Maßnahmen für Ihr Unternehmen finden können.

Nie war die Sensibilisierung von Mitarbeitern für Cybersicherheit so wichtig wie heute

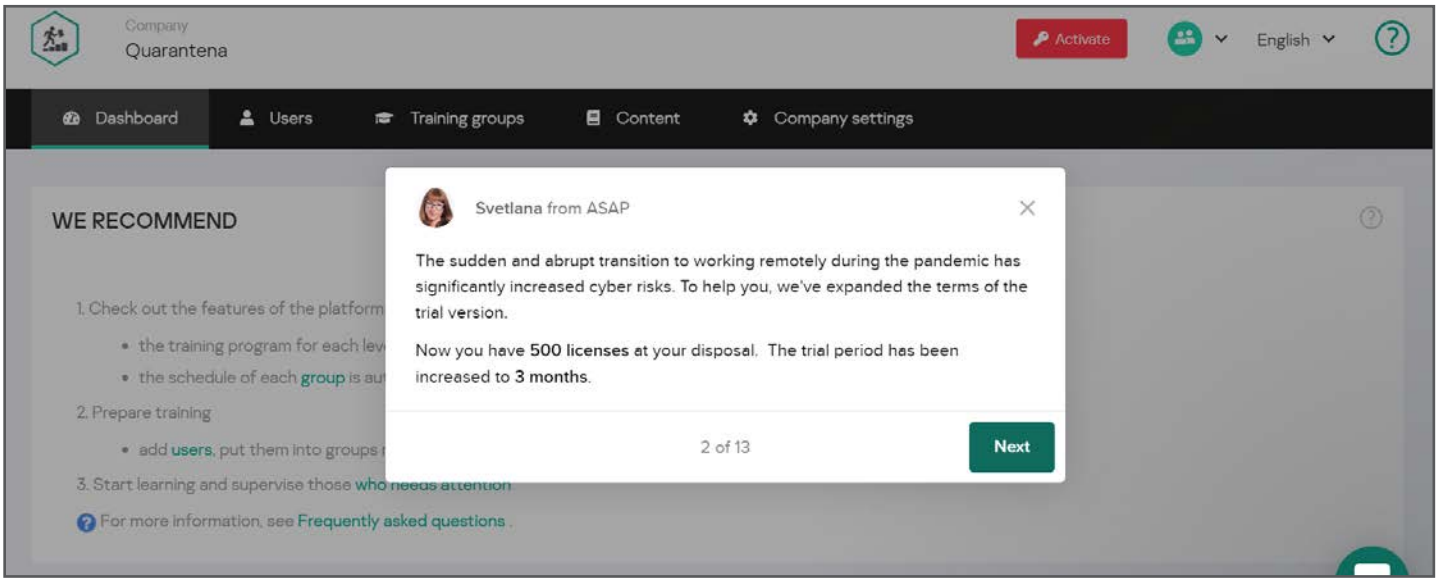
Mehr als 80 % aller Cybervorfälle resultieren aus menschlichen Fehlern und der Faktor Mensch spielt dabei eine immer größere Rolle.

COVID-19 hat die Art und Weise, wie wir arbeiten, nachhaltig verändert – mehr Menschen denn je arbeiten jetzt im Home Office. Auch wenn in einigen Ländern langsam die Normalität zurückkehrt, werden zukünftig weltweit viele Unternehmen auch weiterhin auf Remote-Arbeit setzen.

Trotz dieser Entwicklung haben 73 % aller Mitarbeiter, die während der COVID-19-Pandemie im Home Office arbeiten, keinerlei Cybersicherheitsschulungen von ihrem Arbeitgeber erhalten. Ungeschützte WLAN-Netze, BYOD, potentielle Datenlecks bei Videokonferenzen, unsichere Cloud-Plattformen und viele andere Dinge im Zusammenhang mit der Remote-Arbeit führen zu einer erheblichen Steigerung des Cyberrisikos.

Ihr Unternehmen kann sich vor diesen Bedrohungen nur wirksam schützen, wenn Ihre Mitarbeiter die grundlegenden Regeln der Cybersicherheit kennen. Genau hierfür bieten wir die Kaspersky Security Awareness-Schulungen an.

* Das Angebot gilt vom 12. Mai bis zum 1. Juli 2020.

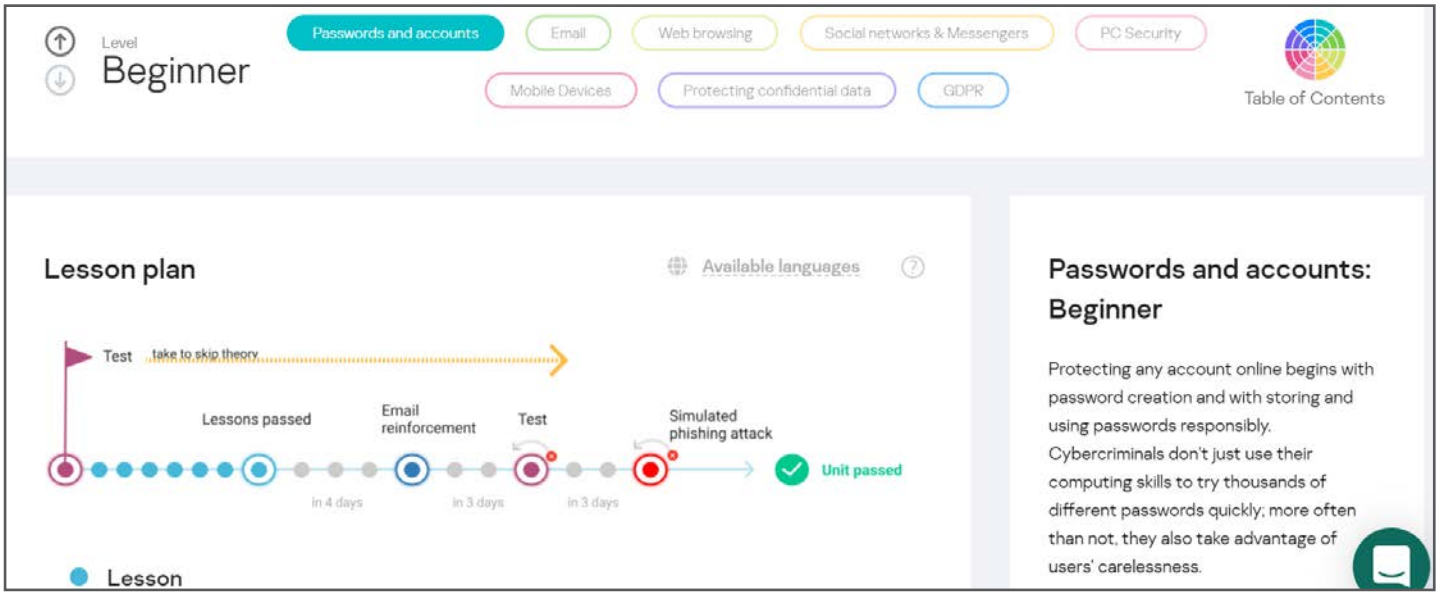


Jetzt handeln

Unternehmen mit maximal 500 Mitarbeitern können die Kaspersky Automated Security Awareness Platform (ASAP) jetzt 3 Monate lang kostenlos nutzen.**

ASAP vermittelt Ihren Mitarbeitern die wichtigsten Cybersicherheitsgrundlagen, unter anderem zu Themen wie Passwörtern und Konten, E-Mail, Internet und DSGVO.

Registrieren Sie sich einfach noch heute für ein kostenloses Administratorkonto unter www.k-asap.com. Wenn Sie die Schulungen auf mehr Mitarbeiter ausweiten oder fortgeschrittenere Themen behandeln möchten, können Sie jederzeit bei Kaspersky oder einem unserer Partner eine Upgradelizenz für Ihr Konto erwerben.



** Das Angebot gilt vom 12. Mai bis zum 12. Juli 2020.

Kaspersky Security Awareness: kaspersky.de/awareness
Cyber Threats News: https://de.securelist.com/
IT Security News: https://www.kaspersky.de/blog/category/business/
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.de