DTS

Managed Firewall Services

Managed Firewall Services

Die schnell wachsende Bedrohungslandschaft verlangt eine dauerhafte Aufmerksamkeit sowie intelligentere und reaktionsfähigere Services für Ihre IT-Sicherheit. Wir bieten mit unserer DTS Managed Firewall einen solchen Service, als ideale Ergänzung für Ihre Cyber Security Strategie. Dabei ermöglichen die nachfolgenden, modularen Bausteine eine kundenindividuelle Kombination der von Ihnen präferierten Bestandteile.

- 24/7 Betrieb & Überwachung ohne Personalaufwand für Sie
- Sofortige Bedrohungsreaktion durch zertifizierte Experten
- Automatisches & detailliertes Reporting
- Vermeidung von teuren Schulungs- & Zertifizierungsmaßnahmen
- Überblick über die überwachten Systeme & Applikationen
- Klar definierte Leistungen & Kosten
- Immer auf dem Laufenden über mögliche Sicherheitsrisiken
- Maximale Kontrolle über Ihr Netzwerk
- 24/7 DTS Security Operations Center (SOC)

DTS Next-Generation Firewall (NGFW) Basisadministration

- Regelwerkunterstützung
    - Konfiguration
    - Plausibilitätsprüfung bei Changes
- Allgemeine Unterstützung
    - VPN Konfiguration
    - Unterstützung bei der Durchführung von PAN-OS-Updates/-Fixes

    (Die DTS NGFW Basisadministration ist ebenfalls inklusive einer Hardware Appliance möglich.)

DTS Next-Generation Firewall (NGFW) Backup Support

- Tägliches Backup der Appliance-Konfiguration
- Unterstützung bei Recovery der Konfiguration
    - 1-stündige Remote-Unterstützung bei einer Wiederherstellung

DTS Next-Generation Firewall (NGFW) Health Check

- Aktive Beobachtung der Appliances durch das DTS Monitoring
    - Einrichtung des Monitoring inkl. Benachrichtigungen bei Fehlermeldung
- Quartalsweise Überprüfung
    - Best Practice Assessment der Policy inkl. Auswertung und Verbesserungsvorschläge
- Überprüfung des Betriebssystems (PAN-OS)
- Empfehlungen bzgl. Releasewechsel
    - recommended PAN-OS Release
    - recommended GlobalProtect Release
    - recommended User ID Agent Release
- Fester technischer Ansprechpartner für die Kontrolle des PAN-OS und des BPA

DTS German WildFire Cloud
Vermehrt umgehen hochentwickelte Cyberangriffe traditionelle Cyber Security Maßnahmen. Herkömmliche Antivirus-Lösungen und Intrusion Preventions sowie zweckgebundene Sandbox-Appliances können hier keinen hochwertigen Schutz mehr leisten. Unsere einzigartige DTS German WildFire Cloud erkennt als Next-Generation Sandbox durch kombinierte, komplementäre Analyseverfahren neuartige Zero-Day-Malware sowie -Exploits und teilt die Informationen für einen vollständigen Schutz mit allen verbundenen Netzwerken, Endpunkten und Clouds.

Die German WildFire Cloud der DTS führt infizierte Dateien in einer skalierbaren virtuellen Sandbox aus und überprüft sie auf schädliches Verhalten durch dynamische sowie statische Analyseverfahren. Alle gängigen Dateitypen werden von WildFire unterstützt, darunter: Microsoft Office Dokumente, EXEs, DLLs, PDFs, Fonts, Java, Android-APK, ZIP, PE-Dateien. Auf diese Weise spürt WildFire unbekannte Malware, Zero-Day-Malware und Exploits auf. Wenn neuartige Bedrohungen entdeckt wurden, bekommt die infizierende Datei automatisch eine Signatur zugewiesen, welche wiederum in nur 5 Min. jedem der mit dem Dienst verbunden ist, bereitgestellt wird – für einen nahezu vollständigen Schutz.

Das Erkennen einer Bedrohung ist der erste Schritt, doch der wahre Wert der German WildFire Cloud liegt im Schutz jedes einzelnen Benutzers und Netzwerks. Durch die schnelle Schutzverteilung kann die rapide Ausbreitung der bislang unbekannten Gefahr und weiterer zukünftiger Variationen ohne zusätzliche Tätigkeit oder Analyse bei allen Nutzern erkannt bzw. blockiert werden. In Verbindung mit dem Schutz vor schädlichen Dateien oder Exploits bieten wir Ihnen zudem eine tiefgehende Analyse der schädlichen abgehenden Kommunikation, störenden Command-and-Control-Aktivitäten mit Anti-C2-Signaturen und den DNS-basierten Callback-Signaturen an. Denn auch diese Informationen fließen zusätzlich in die Palo Alto Networks Datenbanken ein, wo neu entdeckte bösartige URLs automatisch blockiert werden.

Vorgehensweise der German WildFire Cloud:

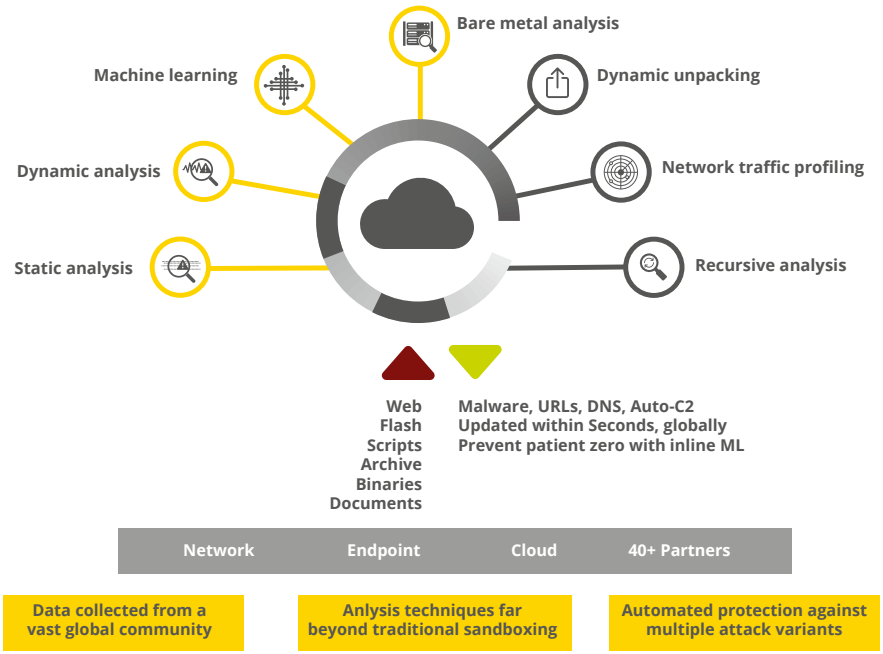
1. Reduzierung der Angriffsfläche durch aktive Sicherheitskontrollen.
2. Blockierung der bekannten Bedrohungen durch dauerhafte Überwachung des Traffics, der Ports und Protokolle.
3. Schnelle Aufdeckung der unbekannten Bedrohungen durch Durchführung und Überwachung der wirklichen Verhaltensweisen von eingehenden, unbekannten Inhalten.
4. Automatische Entwicklung neuer Schutzmaßnahmen mit anschließender Integration in die Abwehrmechanismen aller WildFire-Nutzer.

Zusätzlich versorgt WildFire Sie mit integrierten Protokollen, Analysen und Einsichten in WildFire-Ereignisse auf der zentralen Administrationsoberfläche. Dadurch haben Sie die Möglichkeit, die im Netzwerk beobachteten Ereignisse umgehend zu untersuchen und zu korrelieren. Die Informationen liefern wichtige Erkenntnisse über z. B. sondierte Domains, erstellte Dateien oder betroffene Registrierungseinträge. Somit können Sie die Daten, welche Sie für frühzeitige Untersuchungen und Reaktionsmaßnahmen auf Vorfälle benötigen, schnell lokalisieren sowie anschließend in Aktionen wie Protokollanfragen oder benutzerdefinierte Signaturen umsetzen.

Zur Unterstützung der IT-Security und zur Aufdeckung von infizierten Hosts bietet WildFire auch:

- Ausführliche Analysen zu jeder böswilligen an WildFire gesandten Datei, einschließlich sowohl client- als auch netzbasierte Tätigkeiten
- Sitzungsdaten, welche mit der böswilligen Malware in Verbindung stehen, einschließlich Quelle, Bestimmungsort, Anwendung, User-ID, URL, usw.
- Zugang z. B. zu originalen Malwaresamples zwecks Rekonstruktion bzw. Nachbildung und zu allen PCAPs aus den dynamischen Analyse-Sessions
- Eine Analyse liefert viele Gefährdungshinweise, durch die gezielt gegen die Bedrohungen vorgegangen werden kann

Die Lösung wird in unseren eigenen zertifizierten Rechenzentren betrieben. Sie können die German WildFire Cloud ohne zusätzliche Hardwarekosten durch Ihre bestehenden Palo Alto Networks Firewalls nutzen und erhalten somit den Zugang zu den dynamisch skalierten Malware-Analysen sowie der automatischen Verteilung von Schutzmaßnahmen. Durch den redundanten Aufbau der Umgebung in den zwei deutschen DTS Rechenzentren garantieren wir Ihnen eine Sicherheitslösung, welche den deutschen Regularien bzw. der Konformität nach dem BSI sowie der DSGVO entspricht. Alle verdächtigen Dateien werden übertragen. Nach der Analyse werden gutartige Dateien vernichtet, während schädliche Dateien für weitere Analysen archiviert bzw. sicher aufbewahrt werden. Wir bieten als einziges deutsches Unternehmen eine virtuelle Malware-Analyse-Sandbox nach deutschem Recht an.



USPs der DTS German WildFire Cloud:

- Skalierbare, virtuelle Malware-Analyse-Sandbox
- Erkennt bislang unbekannte Malware, Zero-Day-Malware & Exploits in infizierten Dateien
- Unterstützt alle gängigen Dateitypen
- Automatische Informations- & Schutzverteilung innerhalb von nur 5 Min.
- Ohne zusätzliche Hardwarekosten durch bestehende Palo Alto Networks Firewalls nutzbar
- Bereitstellung, Betrieb & Betreuung in den zertifizierten DTS Rechenzentren
- Einzige virtuelle Malware-Analyse-Sandbox nach deutschem Recht

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

www.dts.de
info@dts.de