



NGAF

Panduan Pengujian Neural-X

Version 8.0.13



Content

1. Deskripsi Dokumen.....	2
2. Prinsip Neural-X	2
2.1 Bagaimana Neural-X bekerja bersama dengan AF	2
2.2 Neural-X mendukung melakukan pemeriksaan dan penghapusan data apa saja yang masuk.....	2
2.3 Dari mana data aturan Neural-X berasal	3
2.4 NGAF memiliki basis aturan yang tersimpan secara lokal. Mengapa perlu pergi ke Neural-X untuk pengujian? Bolehkah mengirim aturan tersebut langsung ke database lokal NGAF	3
2.5 Jika ada aturan baru dengan risiko tinggi, apakah perlu menunggu intranet untuk mengupload data, dan akankah itu menimbulkan masalah setelah pencocokan	4
2.6 Batasan aturan database NGAF yang disebutkan sebelumnya, jika traffic harian saya sangat besar dan aturan yang dikeluarkan oleh Neural-X sangat besar, apakah itu juga akan memenuhi basis aturan lokal.....	4
3. Konfigurasi Neural-X	4
4. Tampilan Efek Neural-X.....	5
5. Tindakan Pencegahan	6

1. Deskripsi Dokumen

Neural-X adalah platform analisis keamanan data besar yang dibuat oleh Sangfor. Neural-X menanggapi secara langsung transformasi dinamis nama domain berbahaya dan mengidentifikasi kamuflase nama domain berbahaya, seperti ancaman tingkat lanjut DGA dan komunikasi tunnel yang canggih. Oleh karena itu, dokumen ini terutama memandu NGAF8.0.5 dan yang lebih baru tentang cara mengaktifkan fungsi Neural-X secara efektif dan dapat memverifikasi efek pengenalan Neural-X.

2. Prinsip Neural-X

Penjelasan prinsip berikut akan dilakukan dalam bentuk FAQ untuk menjawab pertanyaan yang mungkin ditanyakan oleh pengguna di situs pengguna.

2.1 Bagaimana Neural-X bekerja bersama dengan AF

- 1) NGAF memeriksa data yang dilewati sesuai urutan. Ketika menemukan bahwa di database lokal tidak ada cocok, NGAF mengunggahnya ke Neural-X untuk memeriksa apakah itu adalah data yang berisiko.
- 2) Ketika Neural-X memeriksa bahwa datanya adalah data yang berisiko, ia akan mengirim aturan dari cloud ke NGAF, kemudian perangkat NGAF akan memiliki kemampuan perlindungan dari risiko tersebut.
- 3) Bagian lainnya adalah botnet. Setelah mengupload ke cloud, jika tidak ada aturan yang sesuai di cloud, maka akan dianalisis berdasarkan lalu lintas data dan langsung memberikan hasil analisis ke NGAF untuk dibuang. Analisis Neural-X menggunakan mesin pendeteksi seperti sandbox, diproses oleh beberapa mesin secara paralel.

2.2 Neural-X mendukung melakukan pemeriksaan dan penghapusan data apa saja yang masuk

- 1) Neural-X dapat mendukung deteksi data yang terkait dengan botnet, termasuk nama domain DGA dan nama domain yang tidak dikenal.
- 2) Neural-X dapat mendukung data yang terlibat dalam keamanan antivirus, dan file yang dilaporkan oleh mesin keamanan terdeteksi.
- 3) Dapat mendukung tautan URL, file unduhan ftp, tautan berbahaya dari badan surat untuk dideteksi.

2.3 Dari mana data aturan Neural-X berasal

Data aturan Neural-X memiliki lebih banyak sumber untuk terus memperkaya kemampuan deteksi, yang dicontohkan oleh beberapa yang umum sebagai berikut:

- 1) didapat dari lalu lintas ancaman dengan menerapkan honeypots di Internet dan otomatisasi analisis untuk membentuk data intelijen ancaman Neural-X
- 2) dapat Melalui pengadaan data eksternal dari beberapa perusahaan keamanan terkenal, mesin identifikasi dan analisis yang diteliti sendiri membentuk informasi ancaman dari Neural-X itu sendiri.
- 3) Memperkaya database intelijen ancaman Neural-X dengan berbagi dan bertukar data intelijen ancaman dengan perusahaan keamanan terkenal untuk waktu yang lama.
- 4) 4 Cara otomatis dan artifisial terus memantau dan menganalisis peristiwa berisiko tinggi / hot spot di Internet untuk membentuk informasi ancaman Neural-X.

2.4 NGAF memiliki basis aturan yang tersimpan secara lokal. Mengapa perlu pergi ke Neural-X untuk pengujian? Bolehkah mengirim aturan tersebut langsung ke database lokal NGAF

- 1) Alasan utamanya adalah basis aturan lokal NGAF memiliki batasan ukuran, dan ada ratusan juta basis aturan di Neural-X, sehingga tidak dapat dikirimkan ke basis aturan lokal.

- 2) Selain banyaknya basis aturan, Neural-X mengintegrasikan banyak mesin pendeteksi cloud. Jika beberapa data tidak dapat dicocokkan dengan basis aturan, itu akan mendeteksi status risiko melalui mesin pendeteksi. Mesin pendeteksi berbasis cloud ini tidak dapat melakukan integrasi di NGAF dalam waktu singkat.

2.5 Jika ada aturan baru dengan risiko tinggi, apakah perlu menunggu intranet untuk mengupload data, dan akankah itu menimbulkan masalah setelah pencocokan

Tidak, analisis big data global Neural-X kami akan mendapatkan beberapa peristiwa berisiko tinggi / peristiwa baru, Ini juga secara proaktif memberikan aturan dan menyelesaikan pengiriman aturan dalam 5 menit tanpa perlu pencocokan data intranet. Menjamin ketepatan waktu pembaruan aturan acara baru tersebut.

2.6 Batasan aturan database NGAF yang disebutkan sebelumnya, jika traffic harian saya sangat besar dan aturan yang dikeluarkan oleh Neural-X sangat besar, apakah itu juga akan memenuhi basis aturan lokal

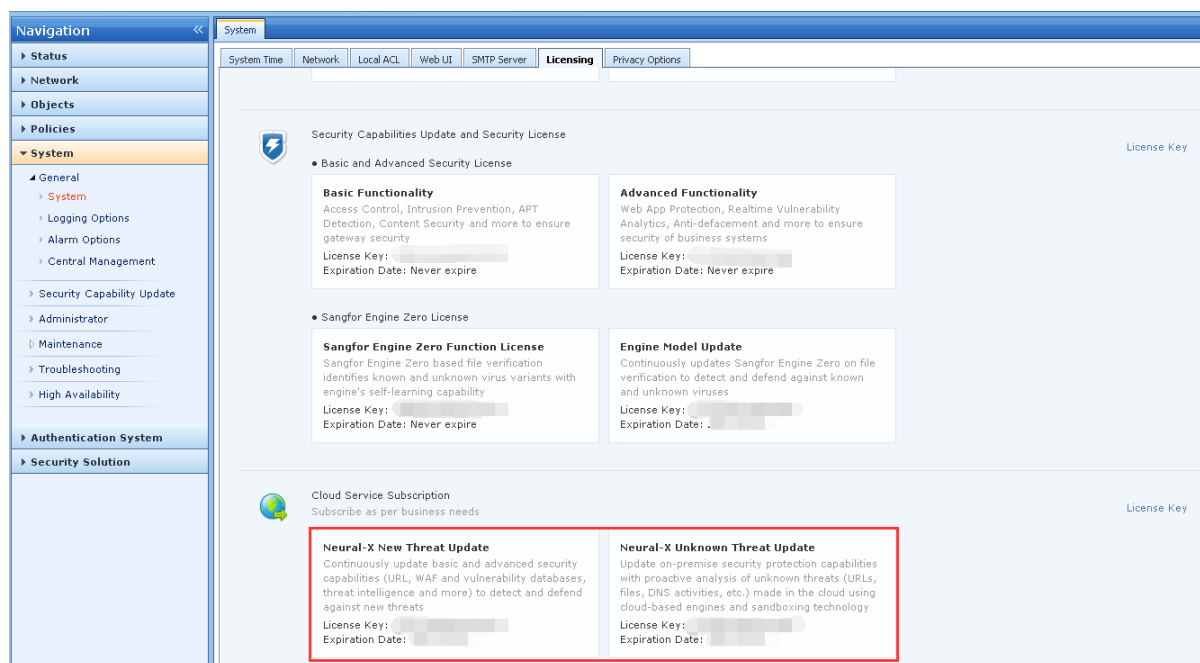
Tidak, karena kita memiliki mekanisme perulangan yang sesuai, ketika entri aturan mencapai jumlah tertentu, di background akan ada proses algoritma untuk memberikan aturan yang belum cocok untuk jangka waktu tertentu, dan menghapus aturan tersebut dari perpustakaan lokal.

3. Konfigurasi Neural-X

Neural-X tidak perlu dikonfigurasi secara terpisah, Neural-X akan tersedia jika memiliki tiga kondisi berikut:

- 1) Versi perangkat dalam AF8.0.5 atau lebih tinggi.

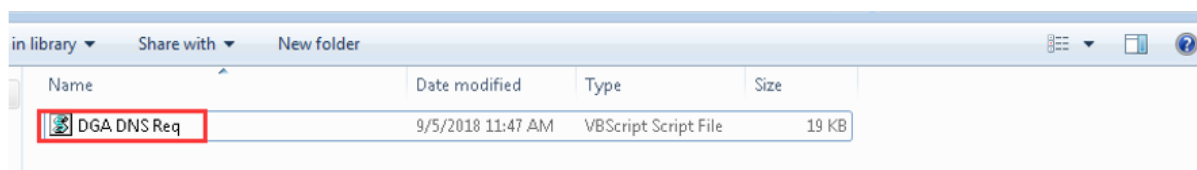
- 2) Perangkat dapat terhubung ke Internet secara normal, dan data pengguna LAN yang mengakses Internet akan melewati NGAF.
- 3) Kunci lisensi Neural-X perangkat telah dinyalakan. Buka System > General > System > Licensing, dan periksa detail kunci lisensi:



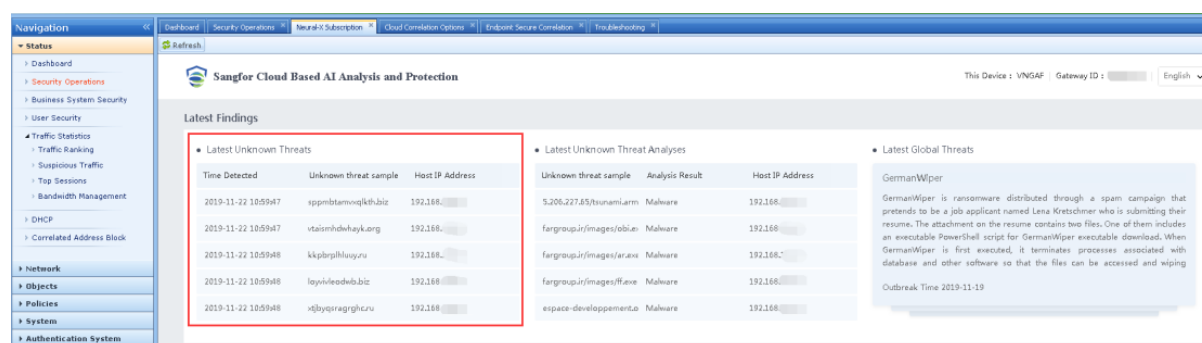
4. Tampilan Efek Neural-X

Jika efek fungsi diuji di lapangan, diperlukan beberapa data akses abnormal akan dilaporkan ke cloud untuk pemrosesan respons, jadi di sini kami menyediakan skrip untuk akses otomatis ke nama domain DGA, lihat [DGA DNS Req. vbs] di toolkit. Unggah alat ke PC yang memiliki akses Internet dan lalu lintas akan melewati NGAF. Langkah-langkahnya adalah sebagai berikut:

- 1) Skrip diunggah ke PC uji. Setelah diunggah, skrip langsung dijalankan. Setelah URL dijalankan, itu akan berhenti secara otomatis:



- 2) Setelah 6-15 menit, buka Security Solution > Cloud Correlation > Neural-X Subscription dan periksa apakah ada log terkait (NGAF 8.0.13 telah memindahkan layanan ke Korelasi Cloud, Anda dapat memeriksa Status > Security Operations jika tidak menggunakan NGAF versi 8.0.13), seperti gambar di bawah ini:



5. Tindakan Pencegahan

- 1) Log deteksi Neural-X membutuhkan waktu 6 menit hingga 15 menit untuk menghasilkan log, jadi perlu ada waktu tunggu.
- 2) Pembuangan Neural-X dari nama domain DGA hanya dianalisis dan dilacak, dan tidak akan dicegat. Oleh karena itu, pengguna perlu memeriksa terminal melalui killing tool.
- 3) Alat skrip DGA DNS Req.vbs hanya alat tes sementara, yang merupakan nama domain DGA, tidak akan membahayakan pengguna LAN, Anda dapat mengklik kanan untuk membuka txt untuk melihat konten kode secara rinci. Jika Anda membutuhkan skrip tes, Anda dapat menghubungi dukungan sangfor.



Hak cipta (c) Sangfor Technologoes Inc. Hak cipta dilindungi oleh undang-undang.

Dilarang menyebarkan atau memproduksi ulang sebagian dari atau seluruh dokumen ini tanpa persetujuan tertulis dari Sangfor Technologies Inc.

SANGFOR adalah merek dagang dari Sangfor Technologies Inc. Semua merek dagang dan nama dagang lain yang disebutkan dalam dokumen ini adalah milik dari pemegangnya masing-masing.

Segala upaya telah dilakukan dalam mempersiapkan dokumen ini untuk memastikan keakuratan konten, namun semua pernyataan, informasi, dan rekomendasi dalam dokumen ini bukan merupakan jaminan dalam bentuk apa pun, tersurat maupun tersirat. Informasi dalam dokumen ini dapat berubah tanpa pemberitahuan. Untuk mendapatkan versi terbaru, hubungi pusat layanan internasional SANGFOR Technologies Inc.