WÜRTHPHOENIX

GRAVITATE

NetEye Conference DACH 2024

19. September 2024

Powered by ICINGA

ntopng

Einführung in ntopng und Best Practices

Tobias Goller

Würth Phoenix Solution Architect

NetEye Conference DACH 2024

Agenda

- Was ist ntopng
- News
- Live demo

Was ist ntopng

ntopng ist eine webbasierte Hochgeschwindigkeits-Verkehrsanalyse und Datenflusserfassung.

ntopng wird von einer Softwarefirma aus Pisa, Italien unter der Leitung con Luca Deri entwickelt.

Einige Hauptfunktionen

- Sammeln von Netzwerkverkehr (SPAN Port, NetFlow, sFlow oder IPFIX)

- Web GUI

- Anzeige des Netzwerkverkehrs in Echtzeit mit den aktiven Hosts

- Sortierung des Netzwerkverkehrs nach vielen Kriterien, einschließlich IP-Adresse, Port, Layer-7 (L7), Anwendungsprotokollen, Durchsatz, autonomen Systemen (ASs).

- Erstellung von Langzeitberichten für verschiedene Netzwerkmetriken, einschließlich Durchsatz und L7-Anwendungsprotokolle

- Top-Talker (Sender/Empfänger), Top-ASs, Top-L7-Anwendungsprotokolle

- Hosts geolokalisieren und in einer geografischen Karte überlagern

- Flexible Handhabung von Warnungen durch ein Alarmierungssystem mit externen Endpunkten (Slack, Email, Webhook, ...)

- Layer-7-Anwendungsprotokolle entdecken (Facebook, YouTube, BitTorrent usw.)

- Deep Packet inspection mittels nDPI

- Fokussiert auf Verkehrstransparenz, Cybersicherheit und Malware detection

- Network Device Discovery

Einige Hauptfunktionen

Durch den Einsatz von ntopng können folgende und weitere Probleme analysiert und erkannt werden.

- Welche Verbindungen habe ich in meinem Netzwerk (wer mit was zu wem, usw).
- Bandbreiten Analyse
- SLA Überwachungen mit Providern
- Internet ist langsam oder ist nicht verfügbar
- Status der Switche und Router
- Ist mein Netzwerk sicher (cybersecurity)
- Welche Geräte sind in meinem Netzwerk
- Möglichkeit zur Reporterstellung

NEWS

- ntopng 6.2 verbraucht -60% der Memory im Vergleich zu 6.0
- Unterstützung der influxdb v 2.0
- Behavioural Checks für OT systems
- Wiederspielen (Replay) historischer Abläufe auf einer virtuellen Schnittstelle
- MITRE alerts Klassifizierung
- Neuer WeChat Endpoint
- Hinzufügen weiterer Filtermöglichkeiten zu den Berichten
- Neuer Sicherheitsbericht
- Personalisierung der Berichte

FRAGEN ?

LIVE DEMO