# Netzwerk Security Monitoring im Heimnetzwerk mit der freien SELKS Distribution

29. April 2023
Andreas Herz

(andreas@stamus-networks.com )

19. LINUX INFO TAG

STAMUS NETWORKS

# About

## Andreas Herz

- Senior DevOps Engineer bei Stamus Networks
- Core Team Member im Suricata Team bei der Open Information Security Foundation (OISF)
- Erster Talk beim LIT Augsburg 2007
- Schwerpunkt IT Sicherheit und Open Source

## Stamus Networks

### Eckdaten

- Gegründet 2014 von Eric Leblond und Peter Manev (Suricata Core Team)
- Hauptsitz: Paris (Frankreich) und Indianapolis (USA)
- Weltweit verteiltes Team
- 100% Remote
- Stamus Security Platform (SSP) - Kommerzielle Variante der “Threat Detection, Hunting and Response” Lösung

### Open Source Projekte

- SELKS
- GopherCap - PCAP replay/manipulation
- Suricata Language Server - Signature syntax check
- Security Analyst’s Guide to Suricata - Open-source resource for Suricata users
- SEPTun - Suricata Performance Guides
- Splunk App integration

# Aktuelle Entwicklungen und Herausforderungen

- Vor 15-20 Jahren waren primär Desktop Rechner und Laptops im Heimnetzwerk verbunden
- Mit dem Siegeszug von Smartphones ab ca. 2007 kamen auch Smartphones ins Heimnetzwerk
- Durch IoT wurden v.a. in den letzten 10 Jahren immer mehr kleinere Geräte Teil des Netzwerks
- Smart TV, Streaming Boxen und Konsolen
- SmartHome, PV Anlagen, SmartMeter usw.
- Auch in Unternehmen sei es im Büro/HomeOffice oder der Fabrik steigt die Vernetzung rapide

- Update Politik der Hersteller teilweise sehr fragwürdig
- Sparmaßnahmen in der Produktentwicklung führen zu häufigeren Sicherheitslücken
- Angriffsfläche durch Digitalisierung wandelt sich und steigt
- Ein einziges kompromittiertes Gerät reicht im Netzwerk um Schaden anzurichten
- Neben Sicherheit auch Datenschutzaspekte im Blick

## Zahl der zu pflegenden Geräte steigt massiv

# Netzwerk Monitoring

- Ermöglicht jegliche Netzwerkkommunikation zu beobachten
- Passives Monitoring ohne aktiven Eingriff
    - (Aktiver IPS Modus optional)
- Identifiziert gewollte als auch ungewollte Kommunikation
- Kann kompromittierte Systeme erkennen
- Hilft bei Bestandsaufnahme/Inventarisierung
- Zusätzliche Analyse bei Engpässen oder Netzwerkproblemen
- Erkennung von Lateral Movement
    - z.B. Ransomware auf weitere Systeme
    - Service Discovery von IoT

- Erfordert etwas Aufwand bei der Implementierung
- Zusätzliche Hardware-/Softwarekomponenten notwendig
- Je nach Netzwerk Architektur nur eingeschränkte Sicht
    - Lokale Client to Client Kommunikation
    - Tunneling
- Grenzen bei der Erkennung
    - Verschlüsselte Verbindungen
    - Fehlerhafter Traffic
- Datenschutz

# Möglichkeiten des Netzwerk Monitorings

- Quellen
  - Port Mirroring
  - (ER)SPAN Ports
  - Integration in Routern/Gateways
  - Packetbroker
  - TAP Devices
  - Virtuelle Switches
- Architektur
  - WAN/Internet Uplink (Nord/Süd)
  - Core Router
  - Lokale Switches (Ost/West)
- Analyse
  - All in One
  - Satelliten (Probes/Sensoren) mit zentraler Verwaltung
  - SIEM/XSOAR

- Kosten
  - Managed Switch mit Mirror bereits ab 25 Euro
  - SoC Systeme ab 100 Euro
  - (Laptop/Desktop für erste Gehversuche)
  - Packetbroker + 10-100 Gbit/s Deployments jedoch schnell 5 stellige Kosten
- Know How notwendig zum Einstieg
  - Grundlagen bzgl. Netzwerk und Protokollen
  - Administration von Server Software
- Tiefere Analyse erfordert letztendlich Fachwissen bzw. Expertise (SOC Analyst)

# SELKS

- IDS/IPS/NSM Threat Hunting Distribution
- GPLv3 Lizenz
- Debian als Basis
- Download als .iso (Live oder Installation) oder Docker compose
- Hardware Anforderungen
    - mind. 2-4 CPU Kerne
    - ab 8GB RAM
    - mind. 10GB DISK für das OS
    - ausreichend Speicherplatz für Logdaten
- Zielgruppe Heimanwender und kleine bis mittelgrosse Organisationen
- Support via Discord Chat oder Github
    - https://discord.com/invite/e6GQKGS5HN
    - https://github.com/StamusNetworks/SELKS

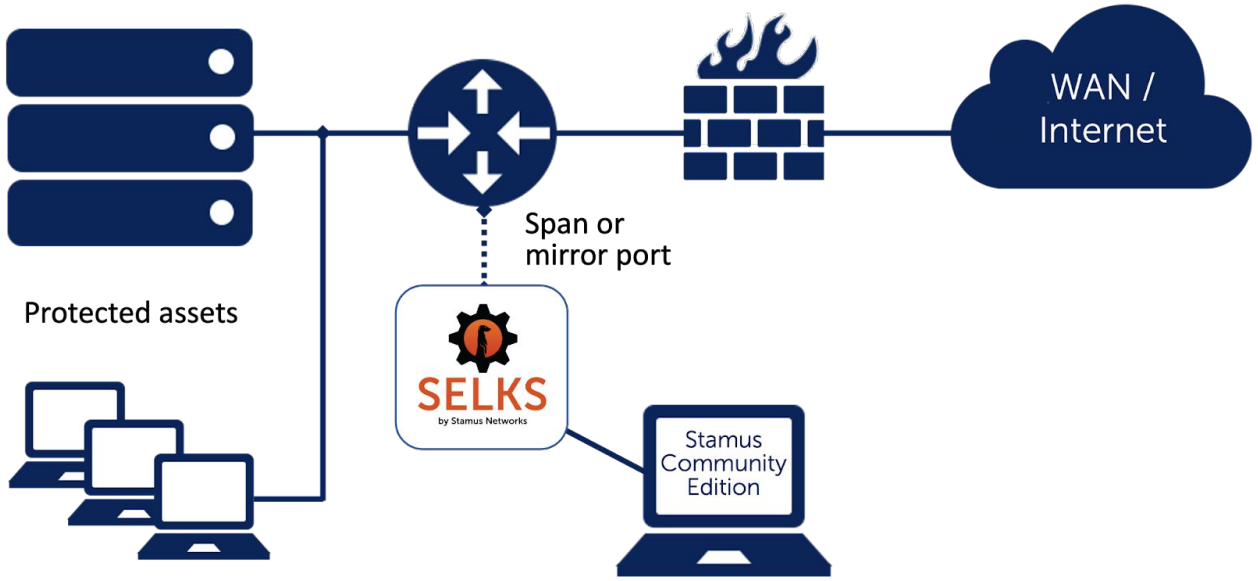

- **S**uricata
- **E**lasticsearch
- **L**ogstash
- **K**ibana
- **S**tamus Community Edition

Weitere integrierte Open Source Tools sind Arkime, EveBox und CyberChef

# SELKS Übersicht


Source: Stamus Networks

# SELKS Integration



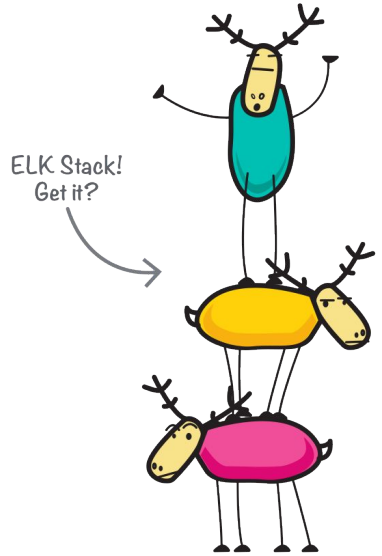
# Suricata

- Intrusion Detection/Prevention System (IDS/IPS)
- Network Monitoring System (NSM)
- GPLv2 Lizenz
- Unterstützt durch die gemeinnützige OISF
- Release 1.0 in 2010
- Release 7.0 geplant in 2023
- Community getrieben
- Signatur basierte Detektion (IDS/IPS)
- Metadaten Generierung (NSM)


- Umfangreiche Logging Möglichkeiten
  - JSON (EVE) als primäres Dateiformat
  - Feingranulare Auswahl der Details
- Support für Linux, BSD und Windows
- Dedizierte Protokollparser
- Filestore extrahierter Dateien
- Full Packet Capture (FPC)
- Conditional PCAP (ab 7.0)
- High Performance Optimierung
  - Deployments bis 100Gbit/s bekannt
  - Unterschiedliche Packet Capture Modi unterstützt

# ELK

- Elasticsearch
  - Verteilte Volltextsuche
  - JSON Format
  - RESTful
  - Hochverfügbarkeit und Lastverteilung
  - Dual License (ehemals Apache 2.0)
- Logstash
  - Sammeln von Logdateien
  - Parsen, Transformieren und weiterleiten an Elasticsearch Instanzen
- Kibana
  - Visualisierung von Elasticsearch
  - Filter, Dashboards, Suche




**E** Elasticsearch

**L** Logstash

**K** Kibana

# Stamus Community Edition (CE)

- Open Source Variante der Stamus Appliance
  - Integriert Teile der Enterprise Variante
- Web UI
- Verwaltung von Suricata Signatur Quellen und “Threat Intelligence” Quellen
- Upload und Verwaltung von eigenen Signaturen und IoC Daten
- Threat Hunting Interface
- Filterung und Limitierung von Suricata Alerts
- Visualisierung von Suricata Alerts, Events und Statistiken
- Direkter Zugriff und Integration von
  - Kibana
  - EveBox
  - CyberChef

# DEMO

Im 3 Schritten bereit zum nachvollziehen:

- git clone https://github.com/StamusNetworks/SELKS.git
- cd SELKS/docker
- ./easy-setup.sh -i eth0

# Danke

andreas@stamus-networks.com

STAMUS NETWORKS