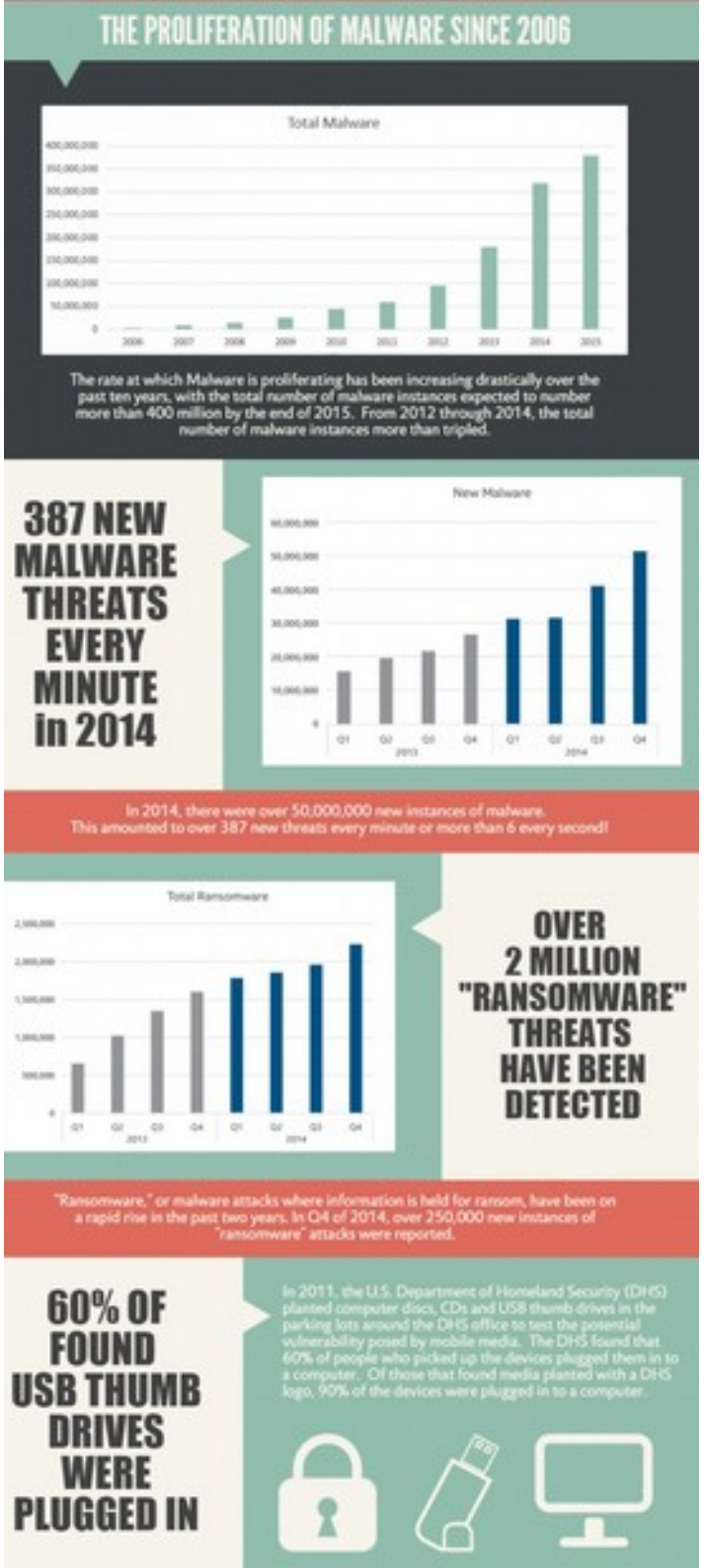
Darkbox®

Network monitoring > Increase security > GDPR ready

DARKbox CYBERSECURITY

Presentazione prodotto

Settembre 2020



Perché Darkbox® ?

Perché antivirus o firewall non bastano più

Darkbox risponde all'aumentato bisogno di cybersecurity

Darkbox risponde al bisogno di controllare e prevenire i rischi derivanti da fenomeni in costante aumento quali:

- PHISHING
- FRODI BANCARIE
- FURTO DI DATI e KNOW-HOW
- INTRUSIONE EMAIL
- ATTACCHI RANSOMWARE e criptaggi
- BITCOIN Mining

Darkbox® è:

GDPR Ready

Articolo 32 del GDPR

- *[Il Titolare] mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;*
- Le misure di prevenzione degli attacchi informatici prevedono un controllo di ciò che accade all'interno della propria rete
- Darkbox effettua il monitoraggio della LAN e segnala traffico anomalo da parte di qualsiasi dispositivo connesso.
- Utilizza software *open-source*

Come funziona ?

Darkbox® è un sistema di monitoraggio di rete, basato sull'analisi dei pacchetti.

In una LAN PMI, agisce collegato allo switch principale.

Internet

|

Router

|

Firewall

Main Switch

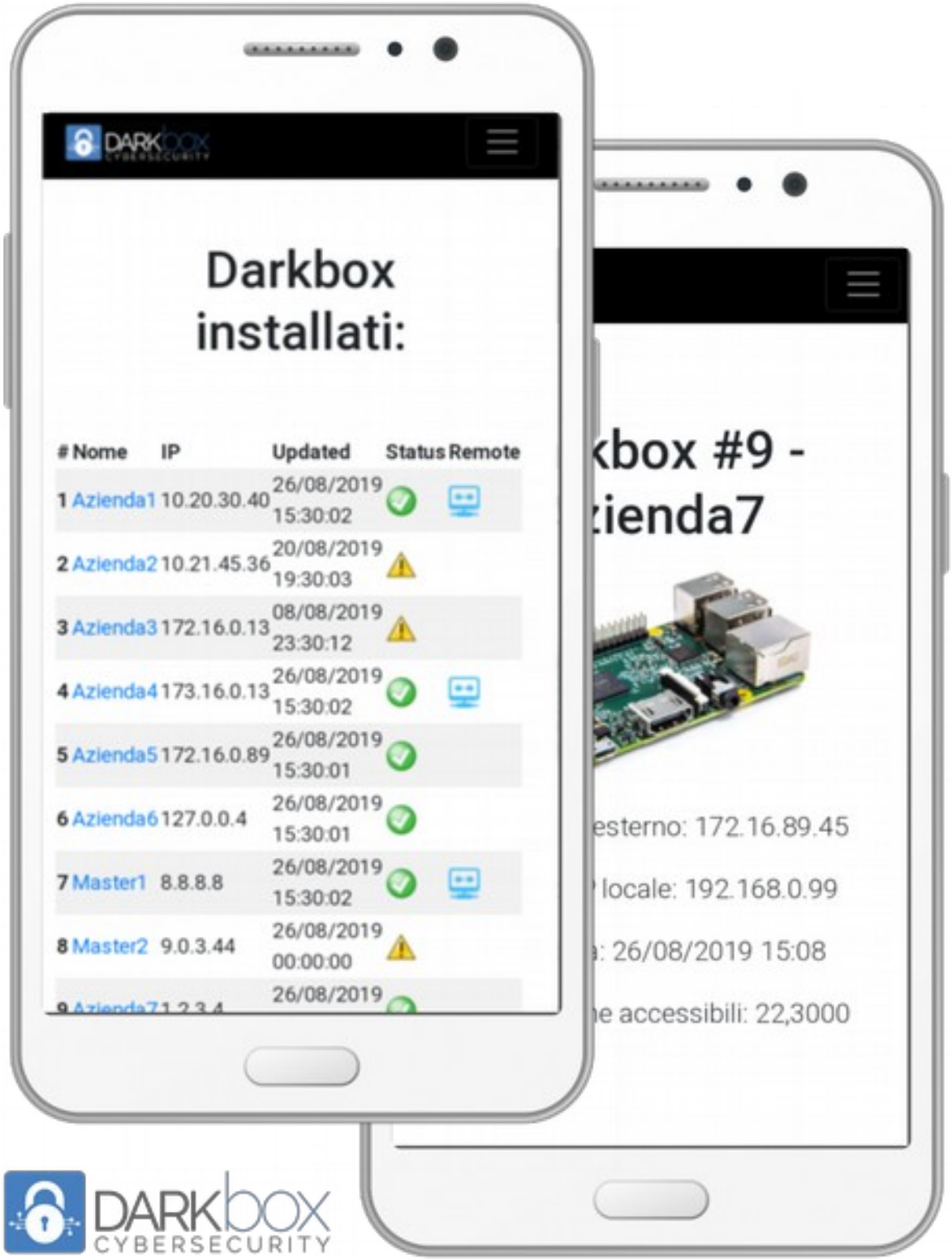
EMAIL ALERTS

REGISTRO ATTIVITA'

Utenti della rete

LAN MONITORING

DARKbox CYBERSECURITY



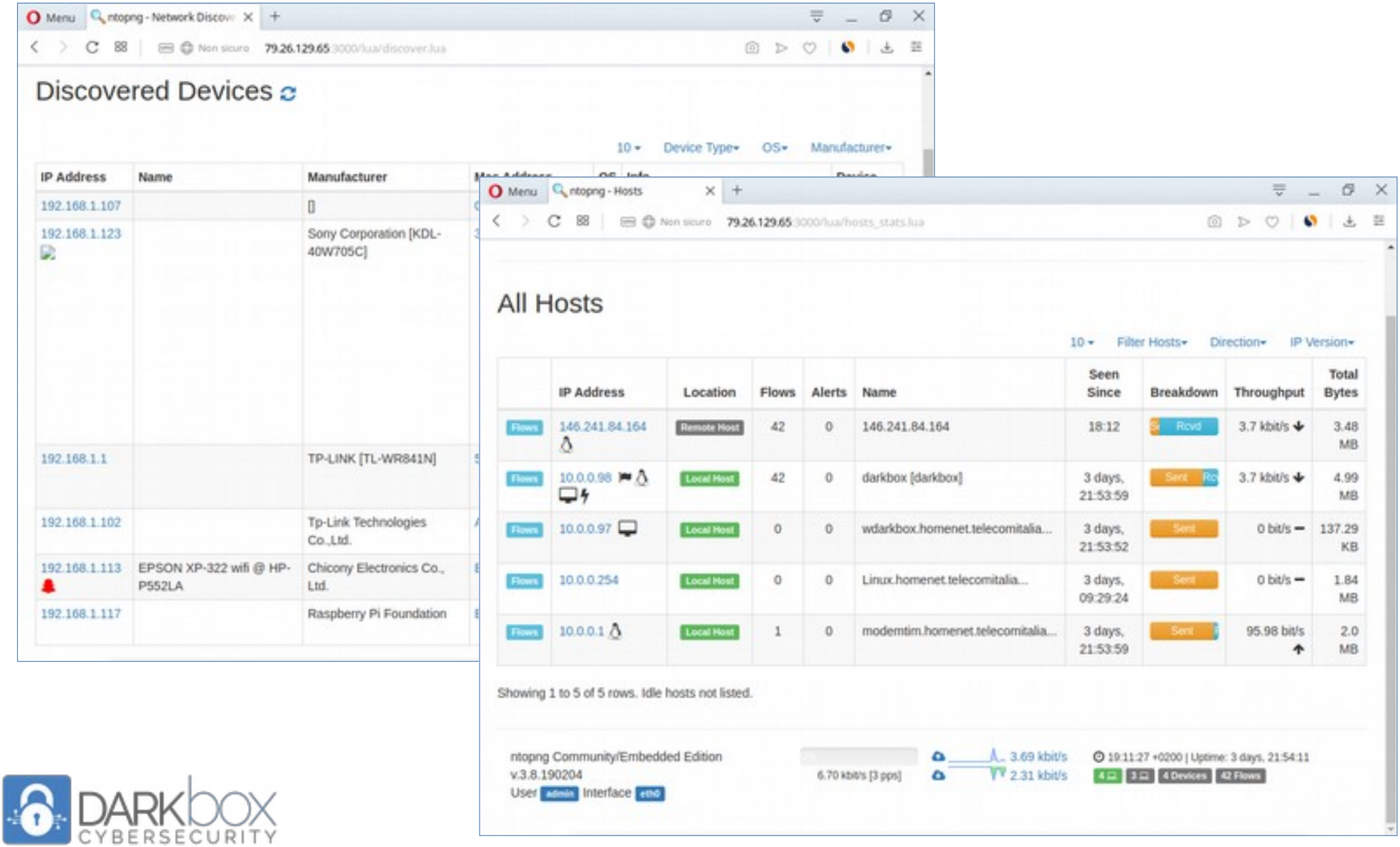
Cosa può fare ?

- Stato di salute della rete
- Allarmi MALWARE
- Allarmi traffico anomalo da singoli IP
- Registra tutti i dispositivi che accedono
- Controlla traffico eccessivo
- Registra l'attività
- Trasmette allarmi via EMAIL

DARKbox CYBERSECURITY

Monitoraggio della rete

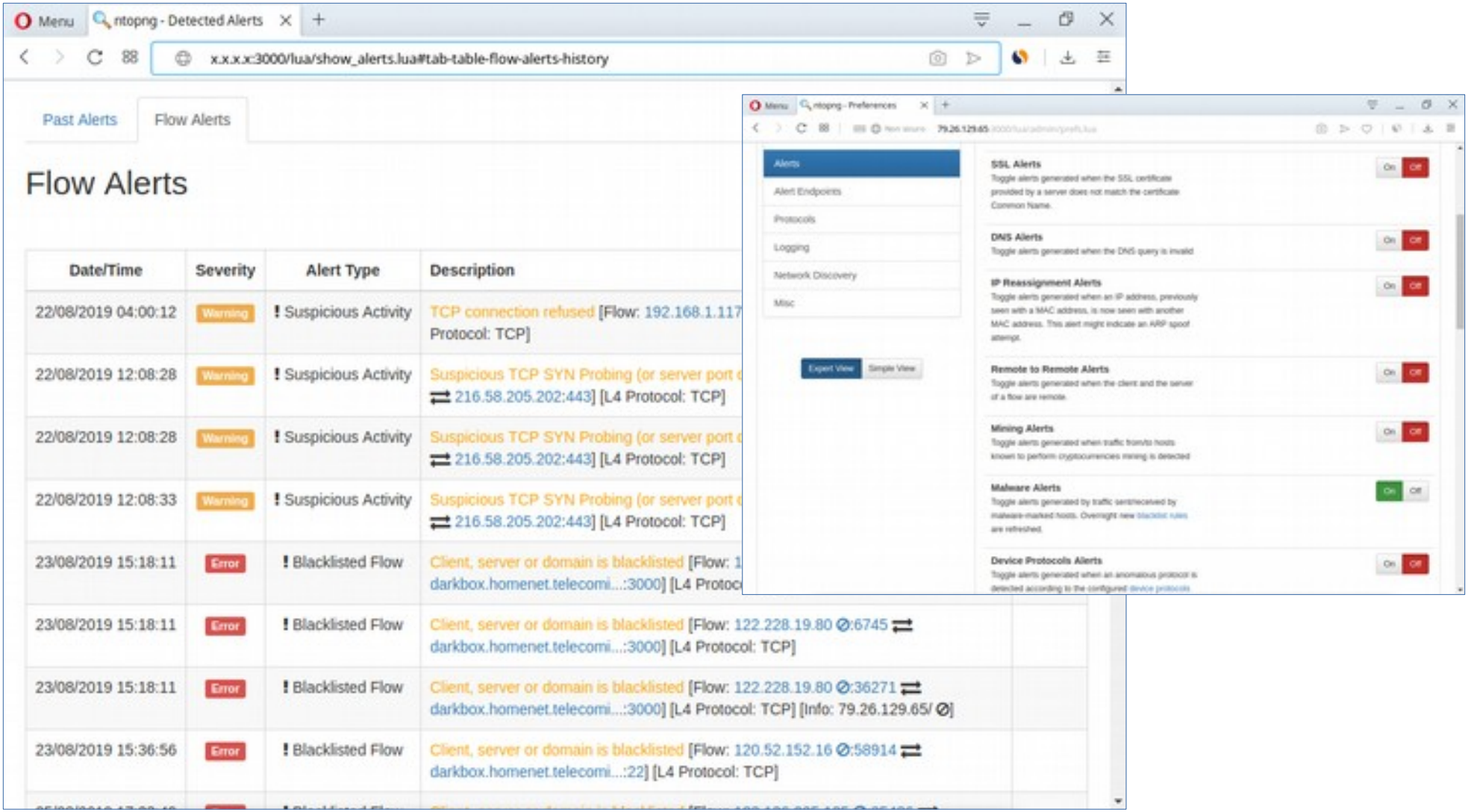
Scansione la rete locale e traccia tutti i dispositivi connessi



DARKBOX CYBERSECURITY

Allarmi via e-mail

Segnala le anomalie con livelli di *alerts* programmabili



DARKBOX CYBERSECURITY

Darkbox® in sintesi...

controlla e previene i cyber-attacchi di nuova generazione

Darkbox, facile da installare e con funzioni modulari:

- PROTEGGE DA VIRUS e MALWARE in maniera completamente diversa da ciò che fanno antivirus o firewall;
- AUMENTA LA SICUREZZA della rete, soddisfacendo i requisiti del GDPR
- SEGNALA COMPORTAMENTI ANOMALI o traffico eccessivo da parte di pc, tablet o smartphone connessi alla rete aziendale
- effettua BACKUP sicuri dei dati più sensibili
- rispetta la PRIVACY, perché controlla il traffico per tipo e protocollo

DARKbox CYBERSECURITY

Darkbox® in dettaglio...

Scheda tecnica

Il funzionamento di Darkbox si basa sull'analisi del traffico di rete e sul monitoraggio dei pacchetti, utilizzando la libreria open-source libpcap (C/C++ library for network traffic capture, tcpdump.org).

Il dispositivo, collegato allo switch principale, è in grado di intercettare il traffico, analizzarlo in tempo reale, segnalare o bloccare i comportamenti ritenuti dannosi e tenere un registro (30 gg.) delle informazioni acquisite. Il dispositivo registra le informazioni su due livelli, "*warnings*", ovvero eventi degni di nota che presentano un qualche livello di rischio e "*dangers*", eventi ritenuti pericolosi che vengono bloccati (eliminando il pacchetto TCP/IP, se possibile) e segnalati via e-mail.

Il sistema è in grado di rilevare e segnalare i seguenti eventi:

- collegamento di nuovi dispositivi in rete;
- errori nelle richieste al DNS;
- errori nei certificati HTTPS;
- flussi "remoto su remoto", quando la rete controllata ospita traffico dall'esterno verso l'esterno;
- attività di mining di bitcoin effettuata da dispositivi della rete monitorata;
- flussi di grandi dimensioni in download e upload;
- prevenzione di malware, sulla base del traffico indirizzato a particolari indirizzi IP presenti in blacklist aggiornata quotidianamente;

Darkbox è in grado anche di riconoscere il traffico generato dall'attività di oltre 250 applicativi molto diffusi (L7 protocol), come chat (WhatsApp, WeChat, Telegram, ecc.), cloud (Dropbox, BitTorrent), streaming (YouTube, Netflix ecc.). Per tale traffico possono essere impostati allarmi di vario livello. Oltre che come sistema di prevenzione, Darkbox registra tutte le attività di rete, che possono essere utilmente consultate in fase di *incident response*.

Per funzionare è richiesto il collegamento ethernet verso il gateway della rete da monitorare. L'installazione ottimale prevede il collegamento a switch dotati di port replication. La gestione è centralizzata, Darkbox si collega periodicamente al server attraverso VPN, per comunicare il suo stato (acceso, aggiornato, ecc.). Da remoto sono possibili sia la gestione che il monitoraggio.

Dicono di noi...

Il Sole 24 Ore, 12 marzo 2019
SICUREZZA INFORMATICA > REALTA' ECCELLENTI

20 Martedì 12 Marzo 2019 Il Sole 24 Ore

Speciale SICUREZZA INFORMATICA - Realtà Eccellenti

I vostri dati sono al sicuro?

Il recente boom del CYBER CRIME rende la sicurezza informatica una responsabilità dell'intera organizzazione e non solo un ruolo dell'IT manager. I dati della vostra azienda sono veramente al sicuro? Le protezioni perimetrali (firewall, IDS), antivirus e politiche restrittive di accesso vi proteggono da comportamenti incauti di dipendenti o clienti ? La CYBER SECURITY richiede un nuovo approccio, mediante l'identificazione degli ostacoli, l'attenzione ai rischi futuri e la necessità di lavorare con *un unico partner per la sicurezza*. Darkbox si occupa dal 2002 di Digital Forensic, offre consulenza a Forze dell'Ordine e Autorità Giudiziaria in materia di prevenzione e investigazione di crimini informatici e fornisce soluzioni per network & mobile security. L'azienda è specializzata nel *penetration testing* per l'individuazione di falle di sicurezza nella rete aziendale e nei dispositivi mobili. Scopri tutti i nostri servizi su www.darkbox.it

DARKbox CYBERSECURITY

Il Sole 24 Ore, 10 marzo 2020
OBIETTIVO SICUREZZA: tecnologie, intelligence e cybersecurity

Il Sole 24 Ore Martedì 10 Marzo 2020 25

Speciale OBIETTIVO SICUREZZA: TECNOLOGIE, INTELLIGENCE E CYBERSECURITY - Realtà Eccellenti

Darkbox contro i rischi cyber

I dispositivi tradizionali come Firewall e Antivirus non sono più sufficienti per una protezione adeguata della rete aziendale. Darkbox, pensato per gli attacchi di nuova generazione, aumenta la sicurezza in linea con quanto disposto dal GDPR in materia di tutela dei dati. Cos'è Darkbox? Un piccolo dispositivo che, collegato allo switch principale, monitora la rete analizzando i pacchetti e il tipo di traffico, traccia i dispositivi e segnala i comportamenti anomali tramite e-mail. Ma il rischio Cyber non è eliminabile al 100%. Se succede un danno? Darkbox non è solo hardware ma un sistema integrato di servizi. Da quest'anno Darkbox si avvale della collaborazione con distributori di polizze cyber risk che riconoscono uno sconto sul premio. In questo modo si completa l'intero perimetro del rischio cyber con l'aumento della sicurezza e il risarcimento in caso di danno, compresi i costi per l'assistenza e il ripristino della rete.
www.darkbox.it

DARKbox CYBERSECURITY www.darkbox.it