Welcome to

Fremtidens it-tendenser

2024

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Codeberg
it-tendenser.tex in the repo security-courses

slides are also available on Github

Plan for today

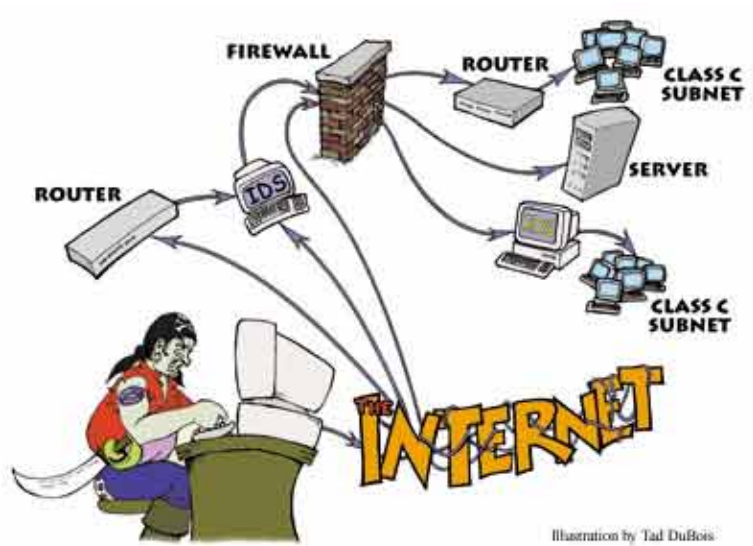
The brave new world of IPv6

Talk about the current world of information technology and security

What a crazy place we are in with a flood of vulnerabilities

Resource shortage – man power, skillz etc.

Every Year



- Same problems last year? Same problems EVERY year
- Data leaks, GDPR, ransomware, ...

Try not to panic, but there are lots of threats

Overlapping Security Incidents

New data breaches nearly every week, these from danish news site version2.dk

Problem, we need to receive data from others

Data from others may contain malware

Have a job posting, yes
- then HR will be expecting CVs sent as .doc files

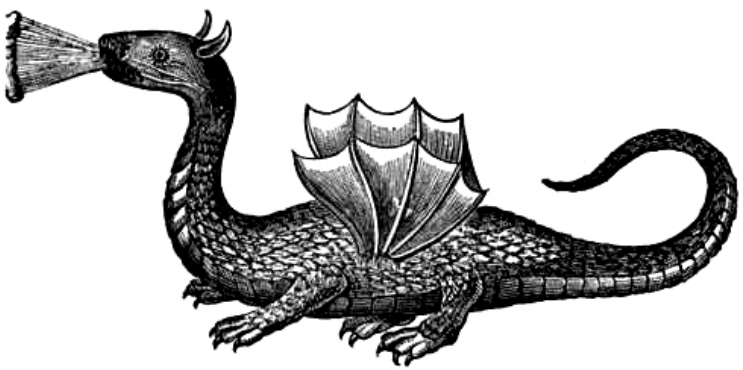
Work together

Learn, Team up, be curious!

We need to share information freely

We often face the same threats, so we can work on solving these together

Principle of Least Privilege



- **Definition 14-1** The *principle of least privilege* states that a subject should be given only those privileges that it needs
- *The Protection of Information in Computer Systems*
  Jerome Saltzer and Michael Schroeder, 1975
  https://en.wikipedia.org/wiki/Saltzer_and_Schroeder%27s_design_principles

Fokus on the basics

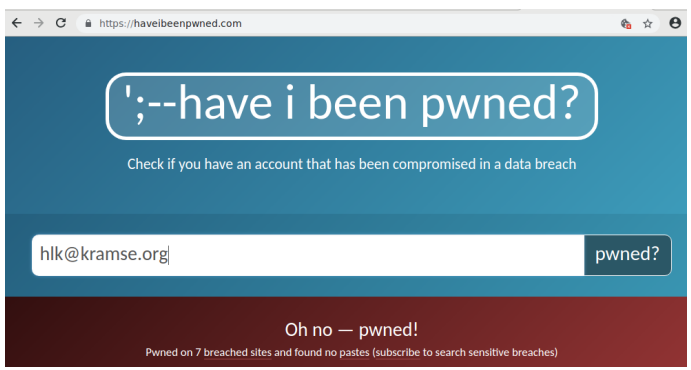
- User management - including administrative users
- Asset management
- Laptop security
- Penetration testing
- Firewalls and segmentation
- VPN everywhere
- TLS and VPN settings, encryption
- DNS and email security
- Syslog and monitorering
- Incident Response and response

Learn technologies, read the manual – don't trust AI will solve everything

Passwords are not random

Source: https://wpengine.com/unmasked/

Your data has already have been owned by criminals



Your data is already being sold, and resold on the Internet

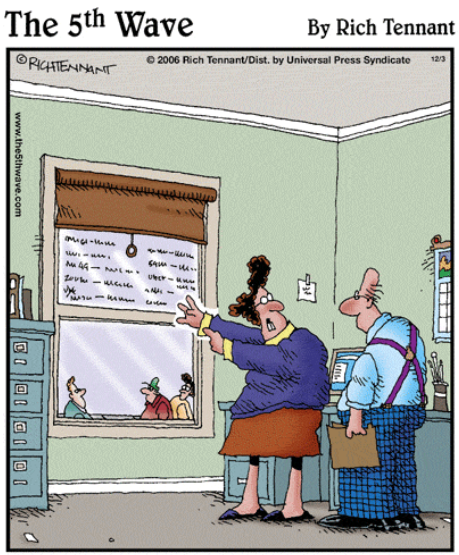
Stop reusing passwords, use a password safe to generate and remember

Check you own email addresses on https://haveibeenpwned.com/

They have an API you can integrate to avoid re-using already leaked passwords

https://www.troyhunt.com/introducing-306-million-freely-downloadable-pwned-passwords/

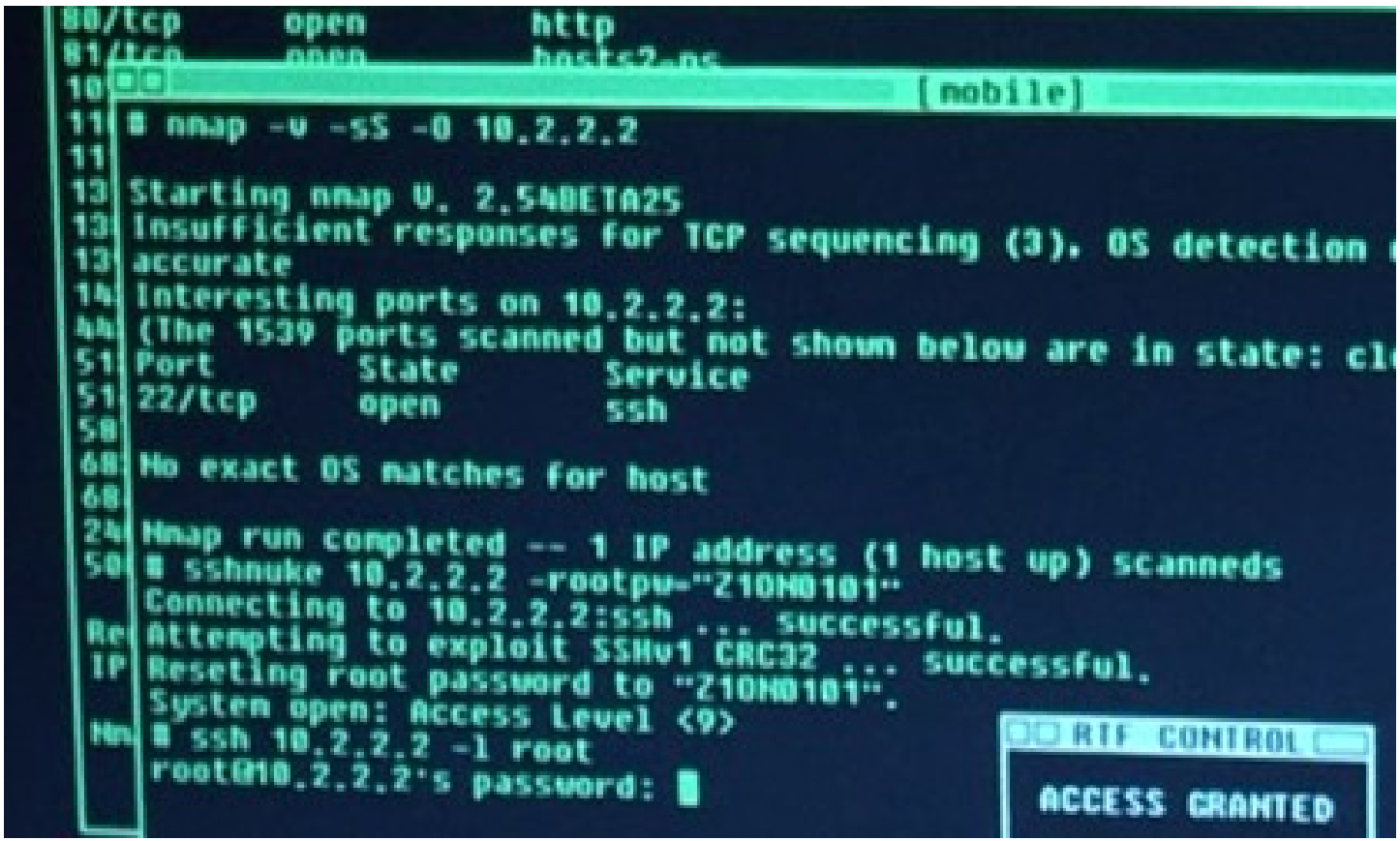
Save the passwords



"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."

- Use password managers! Available as cloud connected, local only, teams based
- You will have to investigate which one to choose, but find one!

Nmap the world



Hackers work all the time trying to break stuff

Blue teams can use hackertools, and become more effecient:

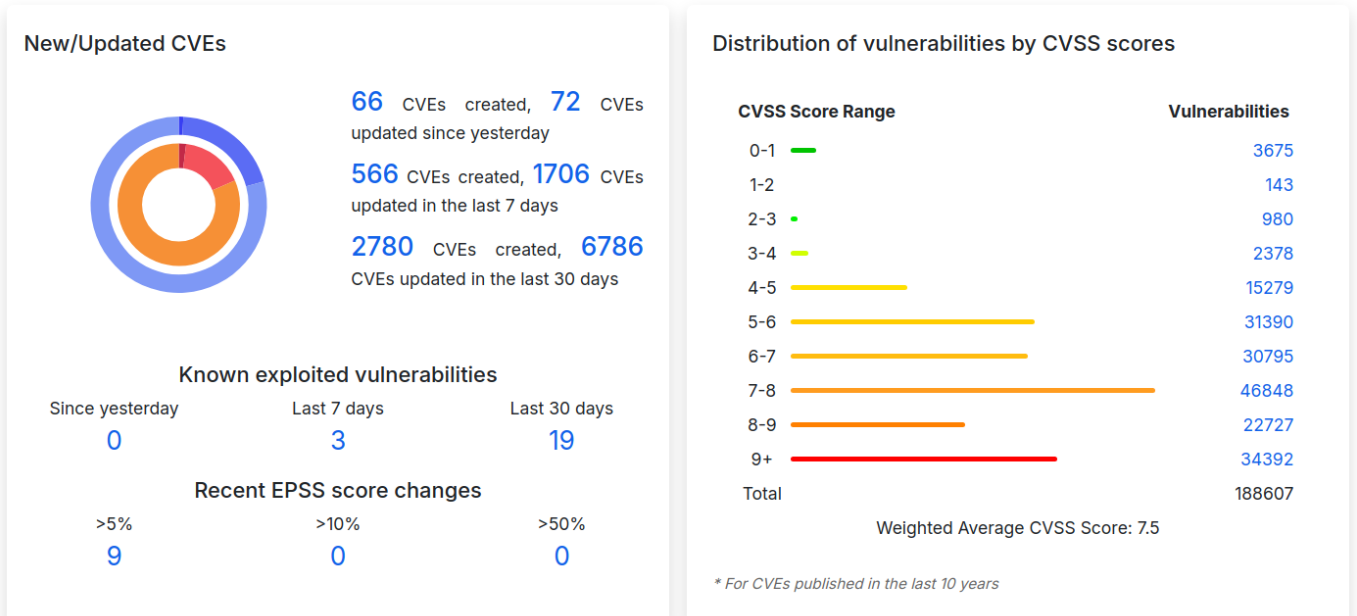
- Nmap, Nping http://nmap.org
- Wireshark - http://www.wireshark.org/
- Aircrack-ng http://www.aircrack-ng.org/
- Metasploit Framework http://www.metasploit.com/
- Burpsuite http://portswigger.net/burp/
- Kali Linux http://www.kali.org

Most popular hacker tools https://tools.kali.org/ and http://sectools.org/

Hacking is not magic

- Hacking only requires some ninja training
- We have been doing this since 1995 when SATAN was released
- Listen, Plan, Act, Do hacking
- Be curious, and honest – let our students play with fire in special networks

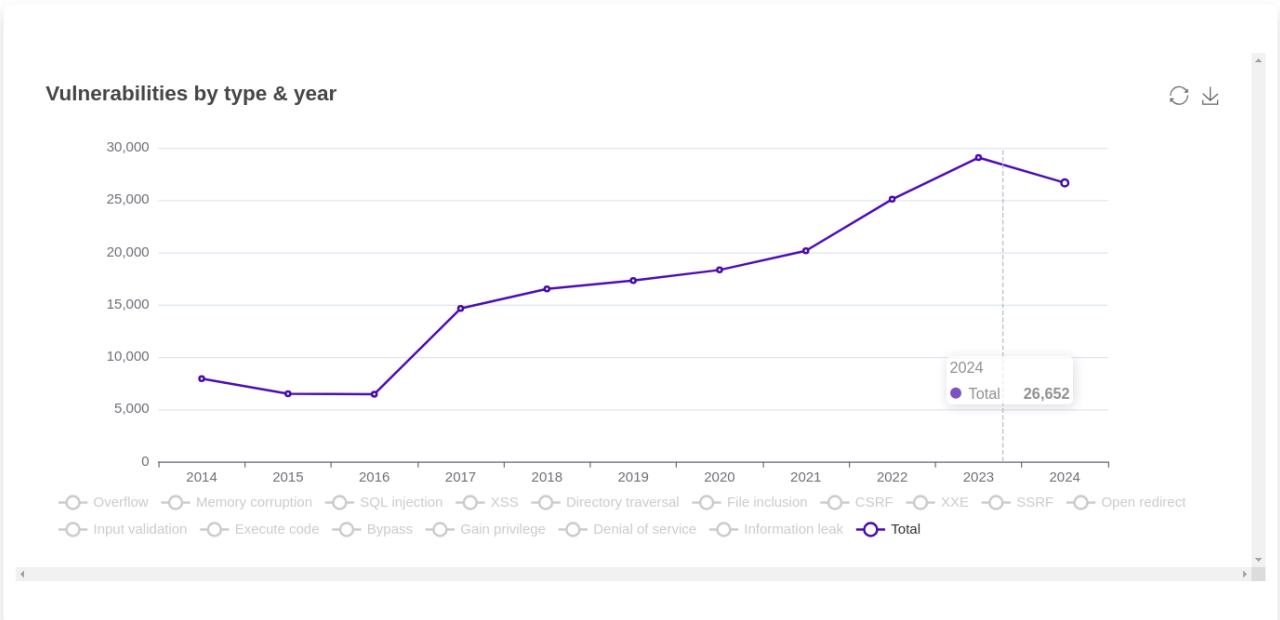
Vulnerabilities are everywhere!



Source: CVEdetails.com on 2024-09-02

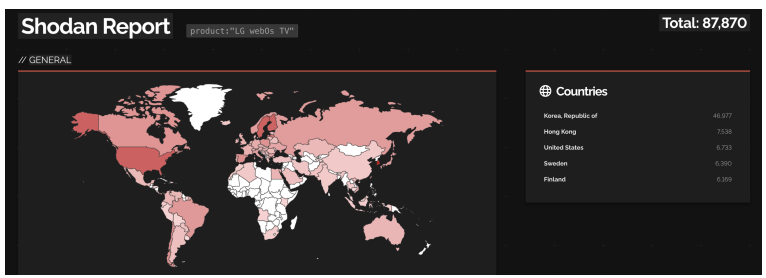
- This is crazy! https://www.cvedetails.com/

Vulnerabilitiesby type & year



Source: CVEdetails.com on 2024-09-02 Graph on the web site is interactive https://www.cvedetails.com/

LG TVs 2024 – CVE-2023-6317 up to CVE-2023-6320



90,000+ LG TVs Vulnerable to Authorization Attacks Due to WebOS Vulnerabilities

Bitdefender Labs has revealed a critical security flaw in over 90,000 LG smart TVs running the company's proprietary WebOS platform.

If exploited, the vulnerability could allow attackers to gain unauthorized access to the TV's functions and potentially the user's home network.

Source: https://cybersecuritynews.com/lg-tvs-vuauthorization-attacks/

D-Link NAS devices accessible via “backdoor” account CVE-2024-3273

92,000+ internet-facing D-Link NAS devices accessible via “backdoor”

A vulnerability (CVE-2024-3273) in four old D-Link NAS models could be exploited to compromise internet-facing devices, a threat researcher has found.

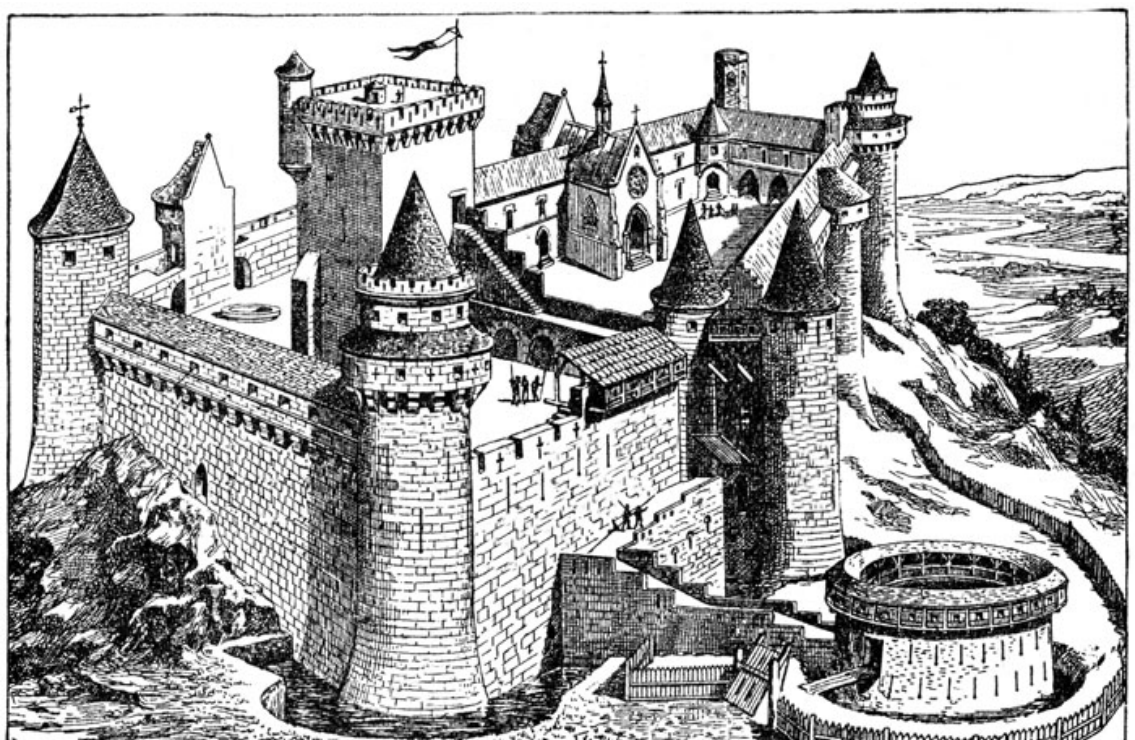
The existence of the flaw was confirmed by D-Link last week, and an exploit for opening an interactive shell has popped up on GitHub.

“The vulnerability lies within the `nas_sharing.cgi` uri, which is vulnerable due to two main issues: a backdoor facilitated by hardcoded credentials, and a command injection vulnerability via the system parameter,” says the discoverer, who goes by the online handle “netsecfish”.

The “backdoor” account has messagebus as the username and doesn’t require a password.

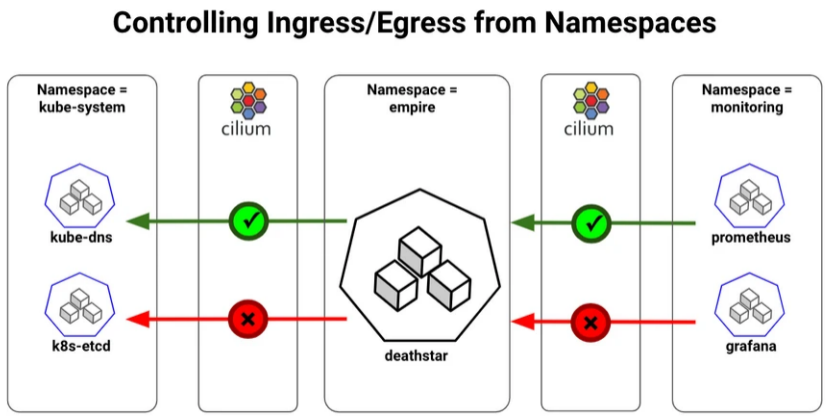
Source: https://www.helpnetsecurity.com/2024/04/08/cve-2024-3273/

Defense in depth



Picture originally from: http://karenswhimsy.com/public-domain-images

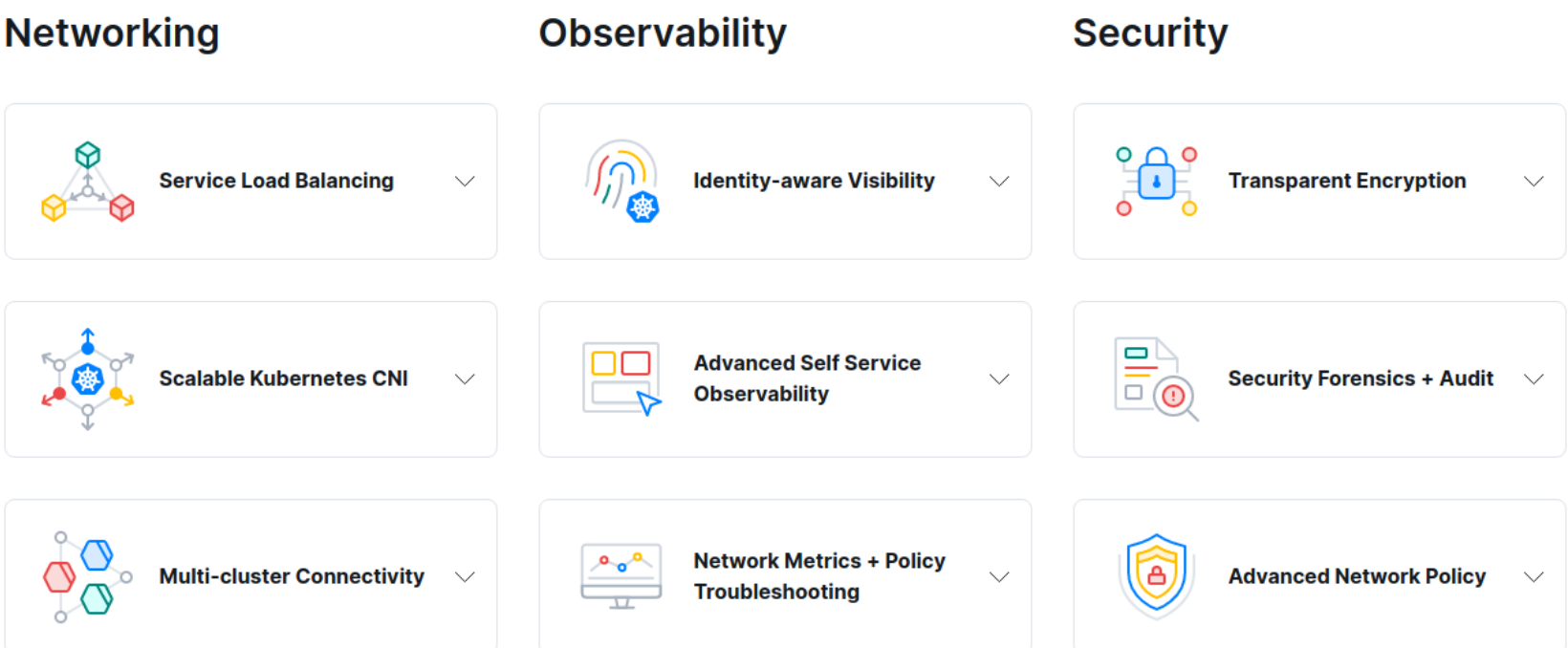
Cloud Security is here, and needed – Cilium overview



Kubernetes provides Network Policies for controlling traffic going in and out of the pods. Cilium implements the Kubernetes Network Policies for L3/L4 level and extends with L7 policies for granular API-level security for common protocols such as HTTP, Kafka, gRPC, etc

Source: picture and text from https://cilium.io/blog/2018/09/19/kubernetes-network-policies/

Security is more than blocking!



- A lot of features relate to *security*

Expect Incidents – train Incident Response

- We know there will be security incidents
- We know you will be tasked at handling it!

Lifeguard training photo by Margarida CSilva on Unsplash

Questions

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse