



Strengthen Your Kubernetes

Unmask Hidden Threats with Runtime Security

Stockholm
Cloud Native &
Container Day

Two major components

Supply chain scanning

Vulnerabilities / Compliance

Runtime Security

Network / Processes / File protection

Supply chain scanning

Pattern based

Vulnerability

- Pipeline
- Platform
- Registry
- Host nodes

Compliance

- CIS
- GDPR
- PCI
- NIST
- HIPPA
- *Custom

Admission control

- CVE Aware
- Registry control
- Complex rules
- alert/enforce

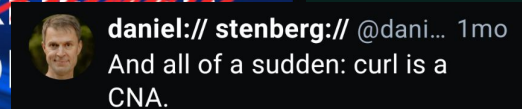
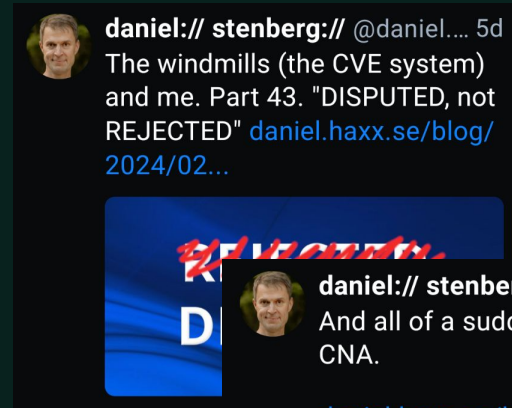
To consider regarding CVE:s

False positive / False negative

Requires CVE remediation

Prioritize patching:


- CVE scoring
- Are they relevant in my implementation?
- Are they relevant in my stack?
- Are they relevant at all?



daniel.haxx.se/blog/2024/01...



kernel.org Added as CVE Numbering Authority (CNA)

Links that redirect to external websites  will open a new window or tab depending on the web browser used.

News February 13, 2024

kernel.org is now a **CVE Numbering Authority (CNA)** for any vulnerabilities in the Linux kernel as listed on kernel.org, excluding end-of-life (EOL) versions.

To date, **361 CNAs** (359 CNAs and 2 CNA-LRs) from **40 countries** and 1 no country affiliation have partnered with the CVE Program. CNAs are organizations from around the world that are authorized to assign **CVE Identifiers (CVE IDs)** and publish **CVE Records** for vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. kernel.org is the 193rd CNA from USA.

kernel.org's Root is the **MITRE Top-Level Root**.

Two major components

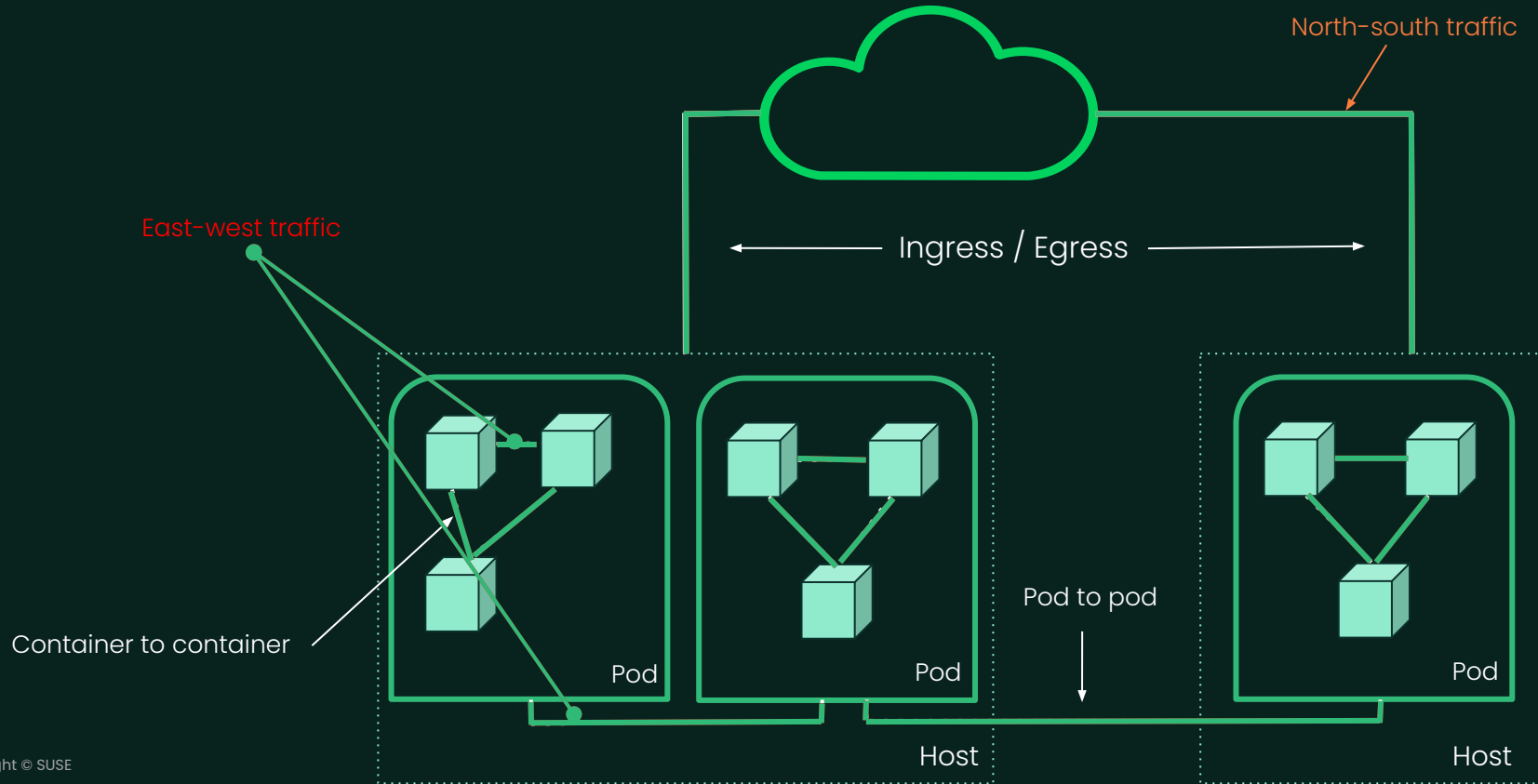
Supply chain scanning

Vulnerabilities / Compliance

Runtime Security

Network / Processes / File protection

Kubernetes Networking



Supply chain scanning & Runtime security

Pattern based

Vulnerability

- Pipeline
- Platform
- Registry
- Host nodes

Compliance

- CIS
- GDPR
- PCI
- NIST
- HIPPA
- *Custom

Admission control

- CVE Aware
- Registry control
- Complex rules
- alert/enforce

Layer 7 Network

- Deep packet inspection
- Layer 7 validation
- Known network attacks
- Packet capture

Workload security

- Image drift prevention
- Network segmentation
- Process segmentation

IDP(?)

- Intrusion detection
- Intrusion prevention
- Privilege escalation
- Container escape

Runtime security

To consider regarding runtime security

- Blacklist / Whitelist
- eBPF
- Sidecar
- Host agent
- Image "agents"
- Cloud native / Security as Code

Supply chain security vs Runtime security

Comparing CI/CD vulnerability scanning to Zero-Trust runtime security

Supply chain security

- Requires CVE ID is published
- Requires CVE remediation
- No protection vs. Zero-Day or insider
- Inconsistent - Is the CVE a threat in my environment
- Requires automation tools & integration
- No control of actual runtime, proc, file or net
- Source code analyzers can't connect "sources & sinks" when analyzing dependencies in raw code.

Behavior-based Zero-Trust

- Application behavior defines Zero-Trust rules
- No CVE # required, uses app behavior as signature
- No CVE Remediation? Zero-Trust blocks non-app behavior!
- Effective vs Zero-day, insider and unpatched CVEs
- Full visibility of any proc, file and network
- Can block and/or alert any anomalous behavior and any source/sink correlation

Two major components

Supply chain scanning

Vulnerabilities / Compliance

Runtime Security

Network / Processes / File protection



NeuVector

Full Lifecycle Container Security

Enterprise-grade container security

Safeguard your cloud native applications from build to deployment with vulnerability scans, image assurance, runtime security and network segmentation.

Zero trust protection

Ensure your environment's integrity with strict policies that protect assets, control access and implement continuous verification.

Straightforward compliance

Achieve regulatory compliance and governance with built-in audits and reporting. Simplify incident investigations with real-time visibility across detailed logs and reports.

Easy integration with DevOps

Seamlessly incorporate robust security into existing DevOps workflows with automated security policies and CI/CD pipeline integration.



Thank you

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

Frankenstrasse 146

90461 Nürnberg

www.suse.com

© SUSE LLC. All Rights Reserved. SUSE and the SUSE logo are registered trademarks of SUSE LLC in the United States and other countries. All third-party trademarks are the property of their respective owners.



NeuVector

BY SUSE