Product Security

Red Hat Enterprise Linux und Container Security

Red Hat Forum Germany 2019

Ansgar Kückes
Chief Architect Public Sector


THE WALKING
DEAD

redhat

roduct Security

AUSGANGSSITUATION KUNDE

- Für die überwiegende Zahl der Kunden ist Security ein **Top Management** (C-Level) Thema
- Viele Kunden unterliegen (mehr oder weniger) einer **Compliance-Pflicht**
- Die meisten Kunden haben ein vitales Interesse an der **Vermeidung von Schäden** im Zusammenhang mit der Verletzung von Schutzzielen (z.B. Verfügbarkeit, Integrität, Vertraulichkeit)
- Schäden können sich kritisch gegenüber der **Business Continuity** auswirken (schließt auch Rufschaden mit ein)
- **Risiken müssen erkannt werden** um geeignete Sicherheitsmaßnahmen zu definieren, ebenso müssen **richtige Entscheidungen** getroffen werden
- Sicherheitsmaßnahmen verursachen Kosten und wirken nicht selten einschränkend, daher muss die **richtige Balance zwischen Kosten und angestrebtem Sicherheitsniveau** gefunden werden
- Bei vielen Kunden bestehen **Sicherheitsstandards**, die zu beachten und umzusetzen sind

WAS KUNDEN BEWEGT

- Welche **Sicherheitsstandards** werden von Red Hat unterstützt, bzw. gegen welche Standards wird zertifiziert?
- Wie kann ich meine **Betriebssystemumgebung** absichern?
- Wie kann ich meine **Cloud-Umgebung** absichern?
- Wie integriere ich in mein **Sicherheits-Ökosystem**?
- Wie kann ich **Security Policies und Strategien** implementieren?
- Wo liegen die Risiken von S**oftware-defined Infrastruktur**, und wie setze ich sicher **Automatisierung** um?
- Wie halte ich meine Systeme auf einem **aktuellen Stand**? Wie gestalte ich mein **Patch Management**?
- Welche **Best Practices** empfiehlt Red Hat als Hersteller um ein angemessenes Sicherheitsniveau herzustellen?
- Wie bilde ich meine **eigenen Experten** aus?

RED HAT SECURITY PHILOSOPHIE

- **Vertrauen schaffen / Security First**
- **Built-in Security / Security by Design**
- Führender **Support** um eingebaute Sicherheits-Features optimal zu nutzen (etwa über Hardening oder Security Guides sowie Consulting-Unterstützung)
- **Sichere Software?** Secure Coding Practices, Test Early, Test Often!
- Mitwirkung in **allen wichtigen Projekten** die sich mit elementaren Sicherheitsfeatures auseinandersetzen (z.B. Linux Kernel-Projekt)
- Mitgestaltung von **Expertendiskussionen** zum Thema Security
- **Zertifizierung von Produkten** gegenüber anerkannten Standards wie Common Criteria bzw. BSI
- Passgenaue Anwendung **gängiger, Red Hat gut bekannter Betriebspraktiken**
- Security für unsere Kunden **konsumierbar und beherrschbar** gestalten

SERVICES

RED HAT OPEN INNOVATION LABS

RED HAT CONSULTING

RED HAT TRAINING + CERTIFICATION

RED HAT SERVICES

DEVELOPER TOOLS

RED HAT JBOSS DEVELOPER STUDIO

RED HAT OPENSHIFT Container Local

RED HAT CONTAINER DEVELOPMENT KIT

RED HAT APPLICATION LIFECYCLE TOOLS

APPLICATIONS AND BUSINESS PROCESSES

MIDDLEWARE AND APPLICATION SERVICES

3scale BY RED HAT

RED HAT JBOSS BPM SUITE

RED HAT JBOSS FUSE

RED HAT JBOSS DATA GRID

RED HAT JBOSS ENTERPRISE APPLICATION PLATFORM

RED HAT JBOSS BRMS

RED HAT JBOSS A-MQ

RED HAT JBOSS DATA VIRTUALIZATION

RED HAT MOBILE APPLICATION PLATFORM

CONTAINER PLATFORMS

RED HAT OPENSHIFT Container Platform

INFRASTRUCTURE SOFTWARE

RED HAT ENTERPRISE LINUX

RED HAT ENTERPRISE LINUX ATOMIC HOST

RED HAT STORAGE

RED HAT OPENSTACK PLATFORM

RED HAT VIRTUALIZATION

PHYSICAL AND CLOUD INFRASTRUCTURE

SECURITY & MANAGEMENT

RED HAT REGISTRY

RED HAT INSIGHTS

ANSIBLE by Red Hat

RED HAT SATELLITE

RED HAT CLOUDFORMS

SECURITY ÜBER DEN GESAMTEN LIFE CYCLE

DESIGN | BUILD | RUN | MANAGE | ADAPT

DESIGN

- RED HAT® CONSULTING Guided Transition
- RED HAT® SERVICES
- RED HAT® TRAINING

BUILD

- RED HAT® OPENSHIFT Container Platform
- RED HAT® CONTAINER DEVELOPMENT KIT
- 3scale BY RED HAT®
- RED HAT® JBOSS® MIDDLEWARE
- RED HAT® MOBILE

RUN

- RED HAT® OPENSTACK® PLATFORM
- RED HAT® VIRTUALIZATION
- RED HAT® ENTERPRISE LINUX® ATOMIC HOST
- RED HAT® ENTERPRISE LINUX®
- RED HAT® STORAGE

MANAGE

- RED HAT® CLOUDFORMS
- ANSIBLE TOWER by Red Hat®
- RED HAT® SATELLITE
- RED HAT® DIRECTORY SERVER
- RED HAT® CERTIFICATE SYSTEM

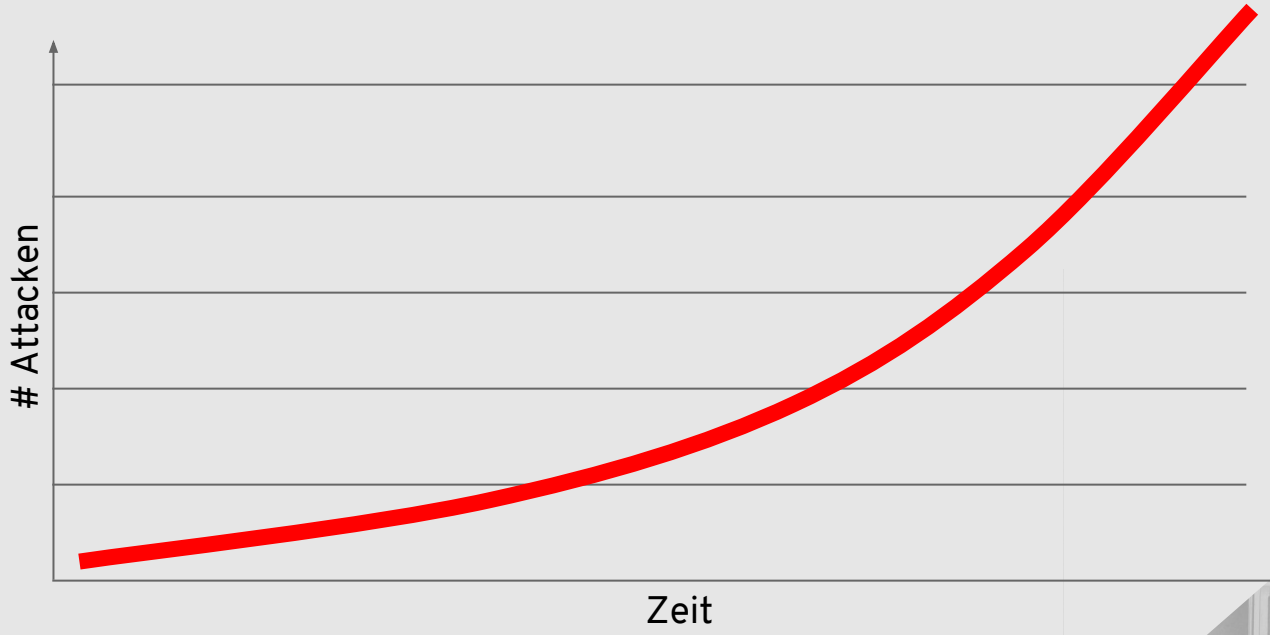
ADAPT

- RED HAT® INSIGHTS
- RED HAT SECURITY ADVISORIES

BEDROHUNGSSITUATION

ENTWICKLUNG VON CYBER-ATTACKEN

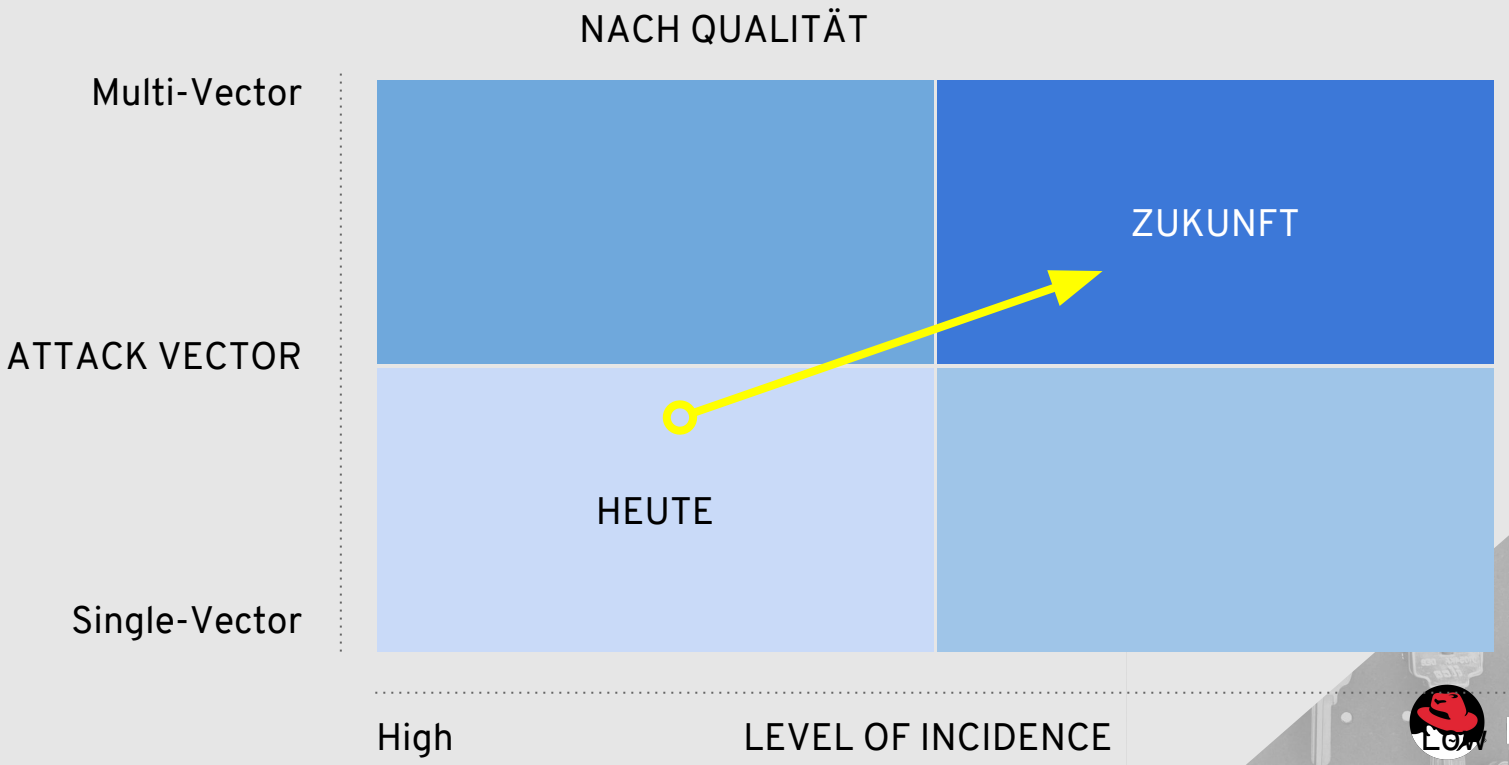
ES GIBT NUR EINE ENTWICKLUNGSRICHTUNG



redhat

Product Security

ENTWICKLUNG VON CYBER-ATTACKEN



redhat
Product Security

KOSTEN

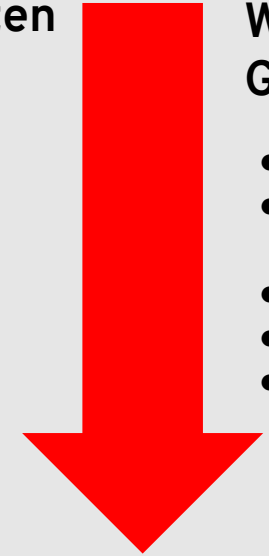
VERURSACHT DURCH SICHERHEITSVORFÄLLE

Durchschnittliche Gesamtkosten je Vorfall sind konstant hoch

2018 $3.7 million*
2017 $3.6 million
2016 $4.0 million
2015 $3.8 million
2014 $3.5 million

*$4.4 million without security automation vs. $1.8 million with full security automation

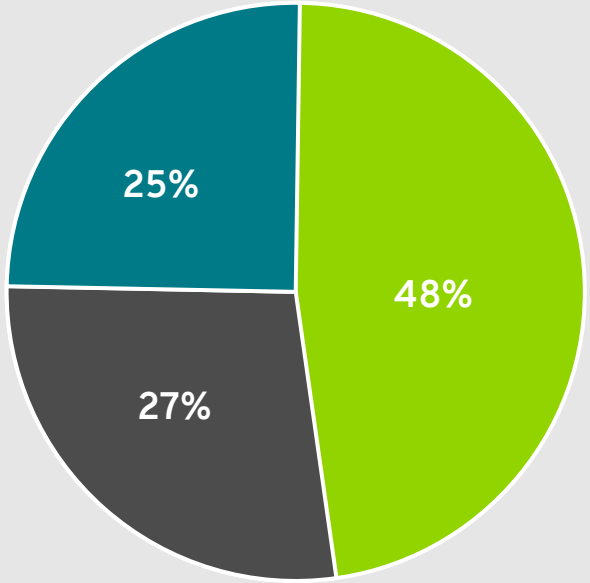
2018 Cost of Data Breach Study: Global, June, 2018. Ponemon Institute LLC© Research Report



Während “Soft”-Kosten das Geschäft beeinträchtigen

- Business Disruption
- Vertrauensverlust bei Mitarbeitern und Kunden
- Brand Erosion
- Verärgerung bei Shareholdern
- etc.

WICHTIGSTE RISIKO-QUELLEN



2018 Cost of Data Breach Study: Global, July, 2018. Ponemon Institute LLC© Research Report

SPECTRE

MELTDOWN

FORESHADOW


STAGEFRIGHT

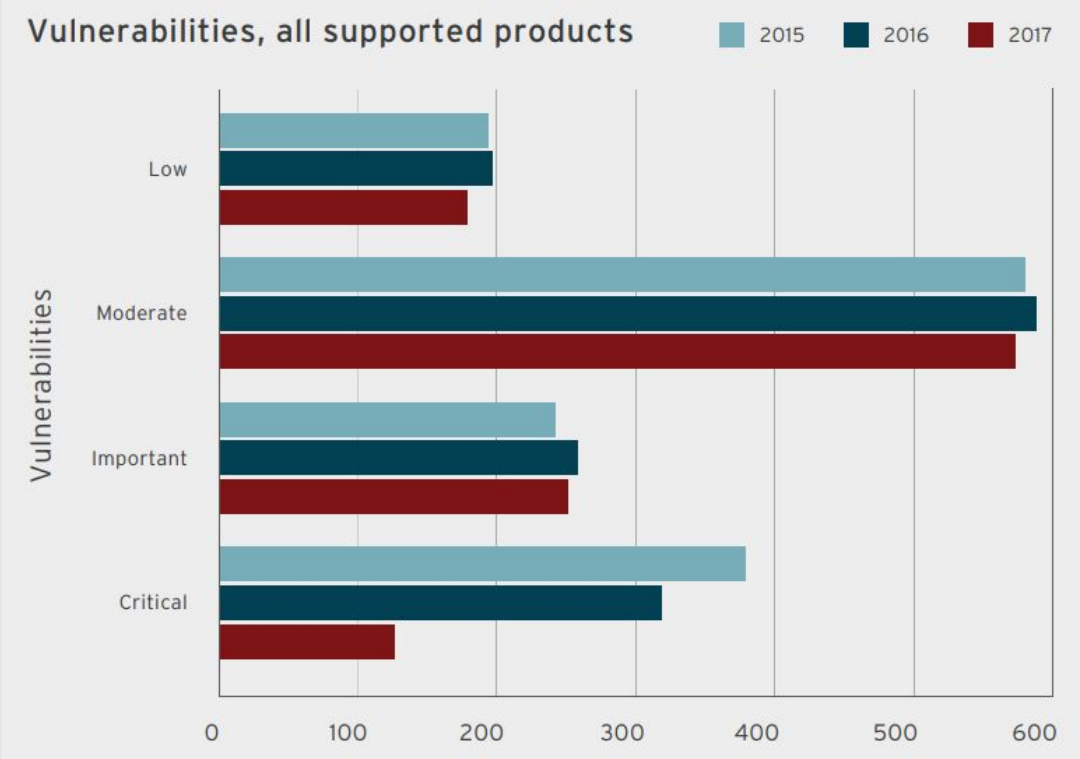

EQUIFAX


FREAK
SSL/TLS Vulnerability

RED HAT PRODUCT SECURITY RISK REPORT

ENTWICKLUNG VON SCHWACHSTELLEN

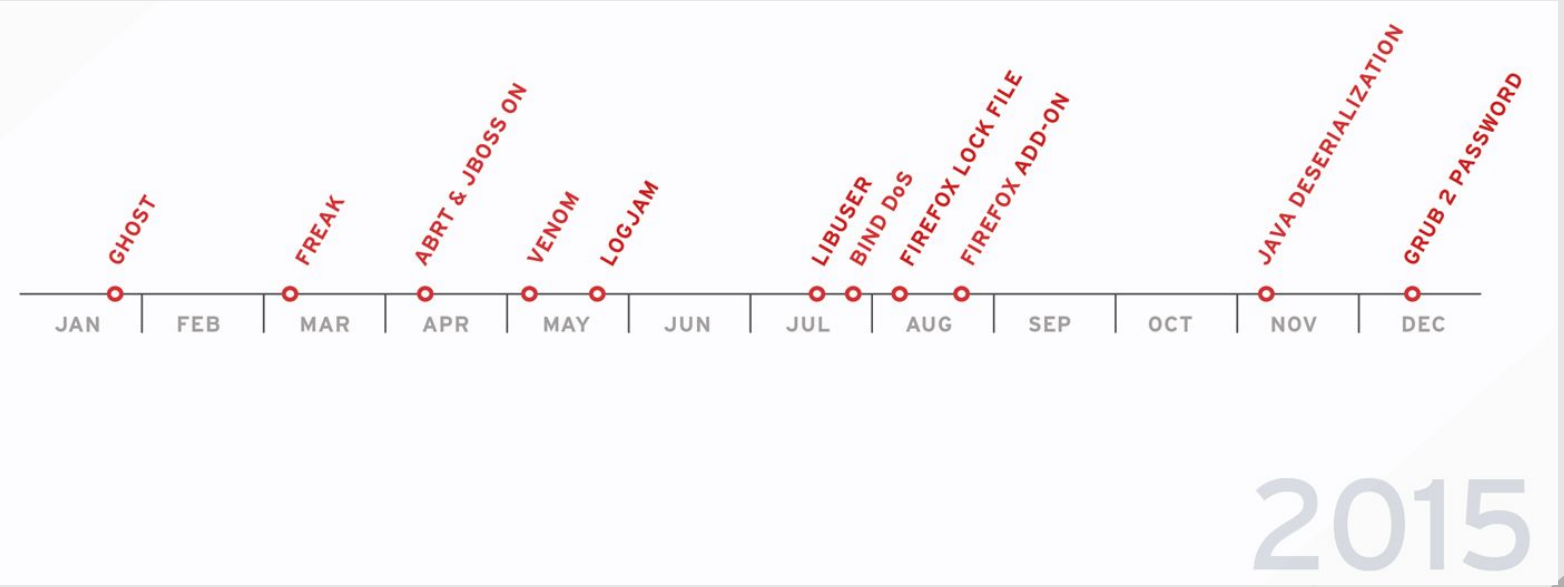
Red Hat Product Security Risk Report: 2017



redhat

Product Security

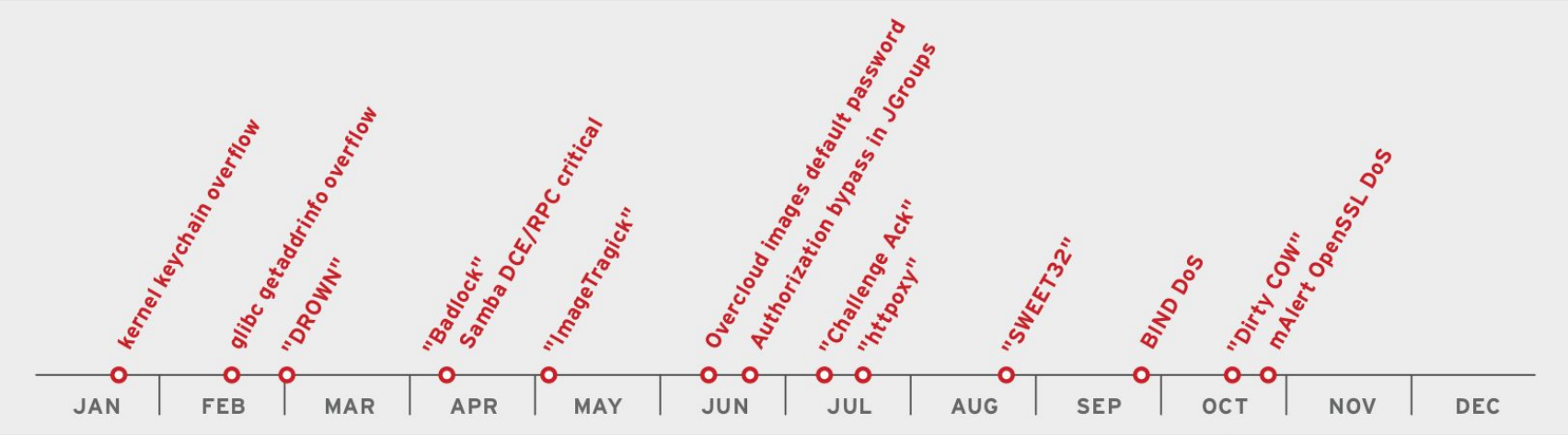
WICHTIGSTE SCHWACHSTELLEN 2015



redhat

Product Security

WICHTIGSTE SCHWACHSTELLEN 2016

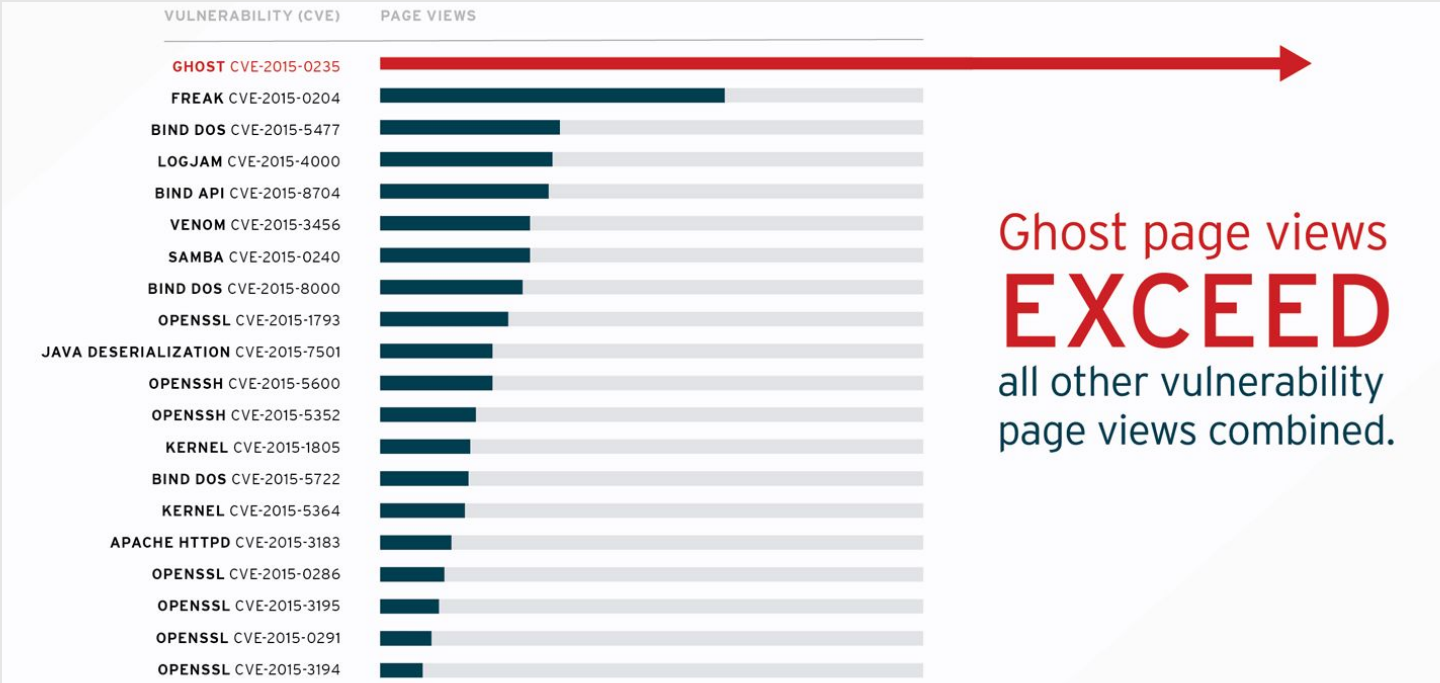


redhat

Product Security

TRANSPARENZ ÜBER SECURITY REPORT

Red Hat Product Security Risk Report: 2015



redhat

Product Security

TOP 5* RED HAT CVEs IN 2017

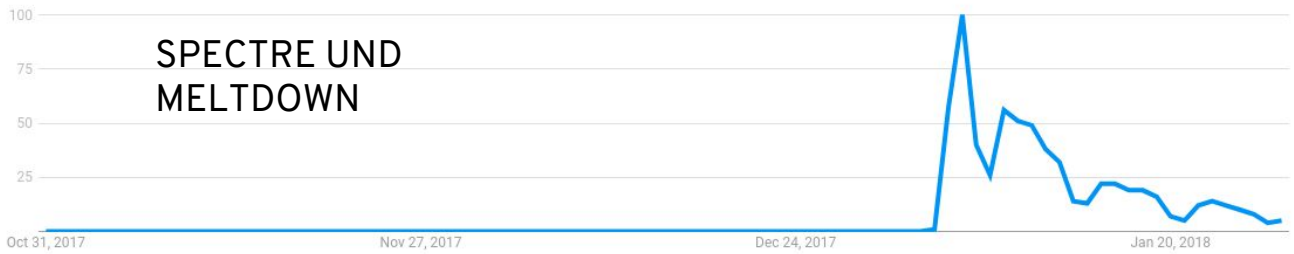
CVE	DAYS EMBAR-GOED	DAYS TILL FIRST ERRATUM	# OF ERRATA	CVSS SCORE	IMPACT
CVE-2017-1000364 (kernel)	40	0	13	7.4	Important
CVE-2017-7494 (Samba)	15	0	5	7.5	Important
CVE-2017-1000253 (kernel)	11	0	10	7.8	Important
CVE-2017-1000367 (sudo)	8	0	2	7.8	Important
CVE-2017-6074 (kernel)	5	0	15	7.8	Important

*Am intensivsten diskutierte Schwachstellen

Red Hat Product Security Risk Report: 2017

BEISPIEL SPECTRE UND MELTDOWN

Interest over time



Interest by region

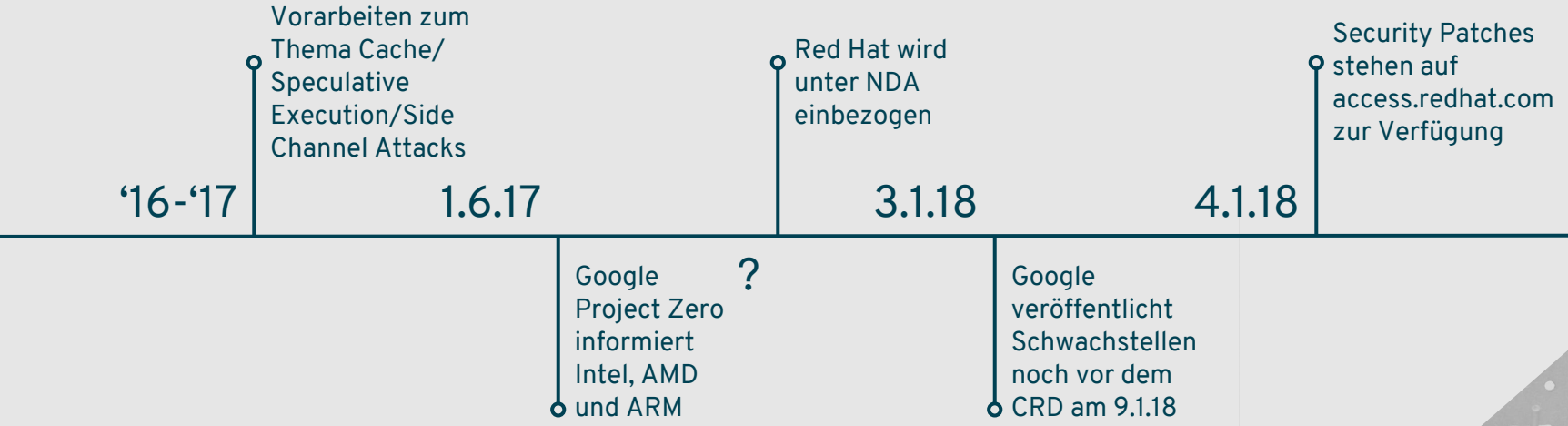
Region

1	St. Helena	100
2	Singapore	91
3	Austria	83
4	Switzerland	80
5	Germany	72

Include low search volume regions

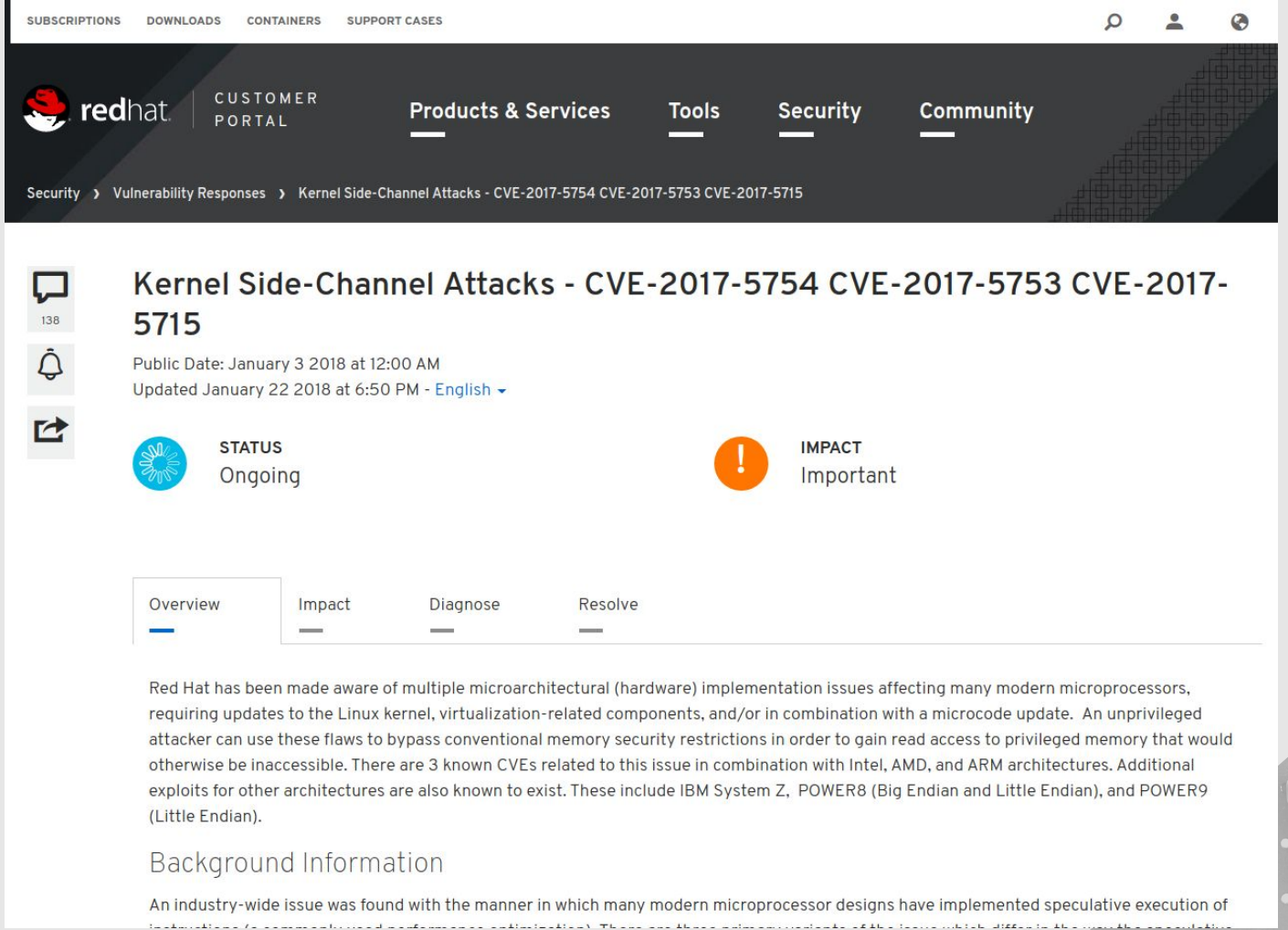
1-5 of 56 regions

TIMELINE



redhat

Product Security


SUBSCRIPTIONS
DOWNLOADS
CONTAINERS
SUPPORT CASES
redhat.
CUSTOMER PORTAL
Products & Services
Tools
Security
Community
Security › Vulnerability Responses › Kernel Side-Channel Attacks - CVE-2017-5754 CVE-2017-5753 CVE-2017-5715
138
Kernel Side-Channel Attacks - CVE-2017-5754 CVE-2017-5753 CVE-2017-5715
Public Date: January 3 2018 at 12:00 AM
Updated January 22 2018 at 6:50 PM - English
STATUS
Ongoing
IMPACT
Important
Overview
Impact
Diagnose
Resolve
Red Hat has been made aware of multiple microarchitectural (hardware) implementation issues affecting many modern microprocessors, requiring updates to the Linux kernel, virtualization-related components, and/or in combination with a microcode update. An unprivileged attacker can use these flaws to bypass conventional memory security restrictions in order to gain read access to privileged memory that would otherwise be inaccessible. There are 3 known CVEs related to this issue in combination with Intel, AMD, and ARM architectures. Additional exploits for other architectures are also known to exist. These include IBM System Z, POWER8 (Big Endian and Little Endian), and POWER9 (Little Endian).
Background Information
An industry-wide issue was found with the manner in which many modern microprocessor designs have implemented speculative execution of

“Containers Are Not Just Small Virtual Machines; They Need New Security Strategies”

Ten Basic Steps To Secure Software Containers
Forrester, April 2017

WARUM SIND CONTAINER SO UNGLAUBLICH POPULÄR?

- Konsistente, systematische Verwendung von **Images** (Dev + Ops)
- Erheblich verbesserte **Resource Utilization**
- Sehr viel schnellere **Start/Stop-Zyklen**
- Deutlich besser Ausnutzung von **Software Lizenzen**
- Fachanwendungen können mit (nahezu) **sämtlichen Dependencies** in Images gepackt werden
- Entwicklungs- ,Test- und Produktionsumgebungen sind wesentlich **homogener**
- Container Life-Cycle ermöglicht **agile Entwicklung** and **Continuous Integration/Continuous Delivery (CI/CD)**
- Perfektes Environment für die Implementierung von **Microservices**

TYPISCHE CONTAINER BEDROHUNGEN

- In Containern versteckte Schwachstellen
- Überwindung der Isolation (Escaping)
- Cross-Container Attacken
- Attacken innerhalb von Containern
- Angriffe auf das Host Container Management
- Nicht vertrauenswürdige Quellen für Images
- Schwachstellen im Kernel
- Fortgeschrittene Hardware Attacken
- Github
- Denial of Service und Ressourcenverknappung
- New Code Problem

RED HAT CONTAINER SECURITY TECHNIKEN

- Trusted images from trusted sources
- Image signing
- Host OS hardening
- Security Context Constraints (SCC)
- Kernel/user/network namespaces
- Least privileges
- Mandatory access control / SELinux
- Cgroups
- Syscall filtering with seccomp
- Read-only mounting
- Secure mounts
- Storage isolation
- Multitenant security
- Workload isolation by node
- Container health index
- Frequent container updates
- Secure container registry (RBAC etc.)
- Source2Image (S2I)
- Secrets encryption (Vault)
- Communication encryption (SSL, TLS)
- Image scan without running the image (OpenSCAP, Atomic Scan)
- Automatic pentesting
- Runtime monitoring
- Handle vulnerable images, prevent images from running (CloudForms)
- PKI / Certificate management
- Separation of container and management
- API management
- Integration with security ecosystem

RED HAT CONTAINER SECURITY TOOLBOX

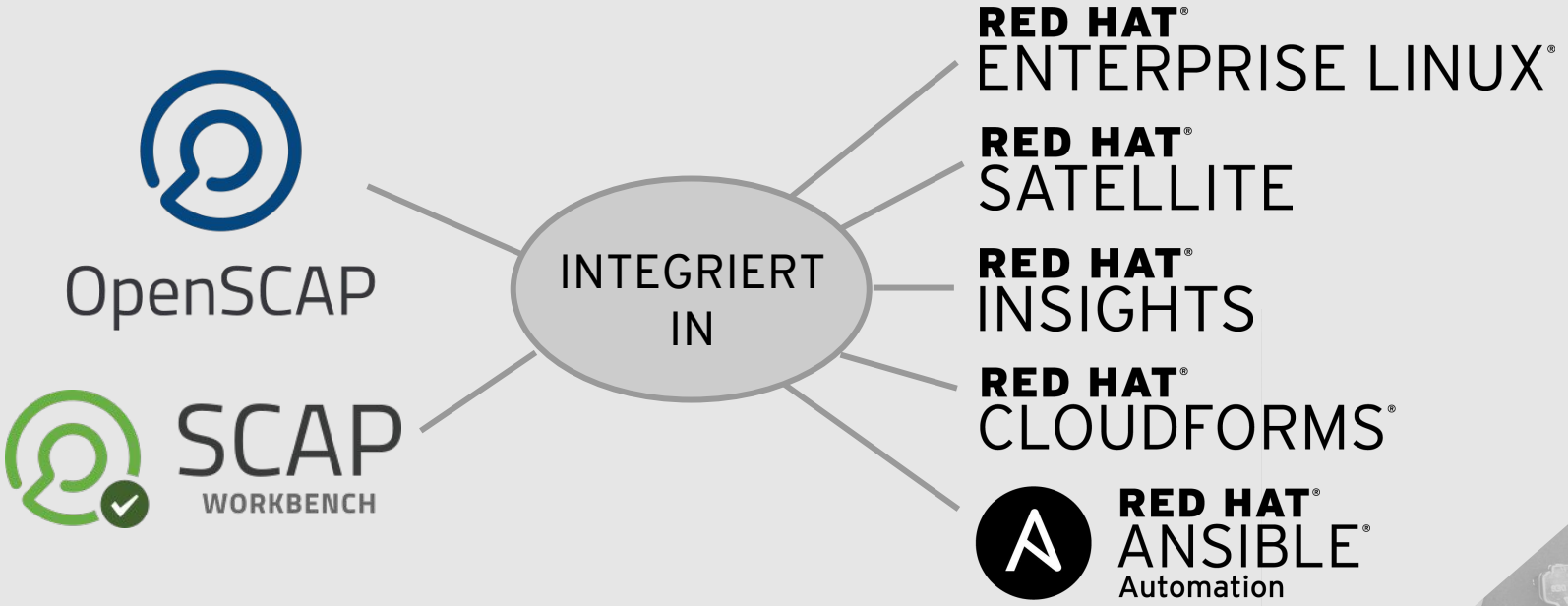
redhat

Product Security

WICHTIGE SECURITY MECHANISMEN IN RHEL

OPENSCAP UND CONTAINER CATALOG

SCANNEN MIT OPENSCAP



redhat
Product Security

TRANSPARENZ ÜBER CONTAINER CATALOG

Grade A: Alle bekannten kritischen oder wichtigen Errata sind umgesetzt

Grade B: Alle bekannten kritischen Errata > 7 Tage und alle wichtigen Errata > 30 Tage sind umgesetzt

Grade C: Alle bekannten kritischen Errata > 30 Tage und alle wichtigen Errata > 90 Tage sind umgesetzt

Grade D: Alle bekannten kritischen Errata > 90 Tage und alle wichtigen Errata > 365 Tage sind umgesetzt

Grade E: Alle bekannten kritischen oder wichtigen Errata > 365 Tage sind umgesetzt

Grade F: Es sind kritischen oder wichtige Errata > 365 Tage nicht umgesetzt oder der Container hat das Ende seines Lebenszyklus erreicht

redhat

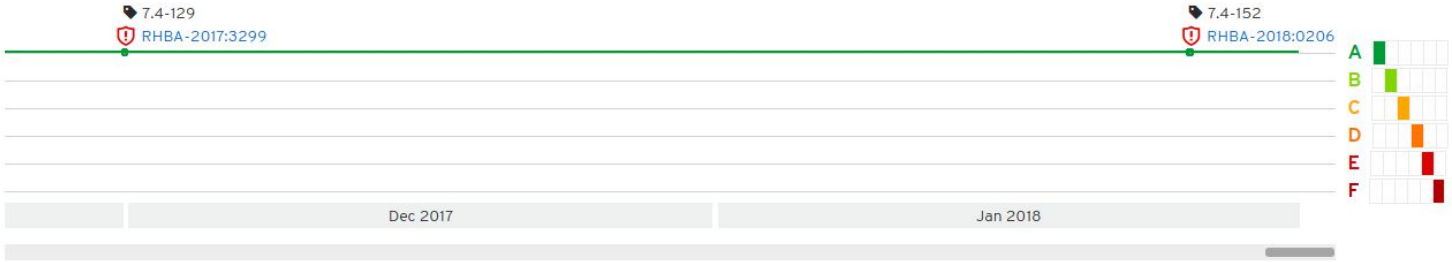
Product Security

Red Hat Enterprise Linux 7 ☆

by Red Hat, Inc. | in Product Red Hat Enterprise Linux

`registry.access.redhat.com/rhel7` Updated 6 days ago 7.4-152 : Health Index A

Overview | Get this image | Tech Details | Documentation | Tags



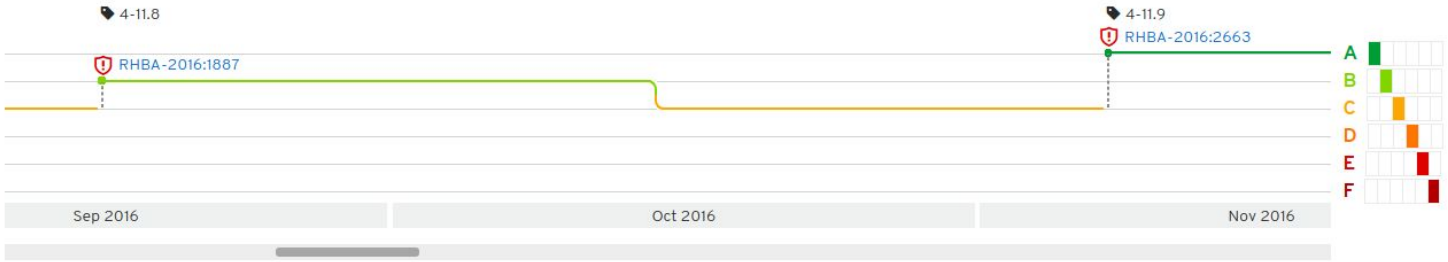
Tag Name	Date Pushed	Image Advisory	Health Index	Docker Image ID
7.4-152 7.4 latest	6 days ago	RHBA-2018:0206	A	d01d4f01d3c4
7.4-129	2 months ago	RHBA-2017:3299	A	cf55adcfe21a
7.4-120	3 months ago	RHBA-2017:2975	A	db7a70a0414e
7.4-113	4 months ago	RHBA-2017:2844	A	549b1c5d7a44

Platform for building and running Node.js 4 applications ☆

by Red Hat, Inc. | in Product Red Hat Enterprise Linux

`registry.access.redhat.com/rhscl/nodejs-4-rhel7` Updated 2 days ago 4-12 : Health Index A

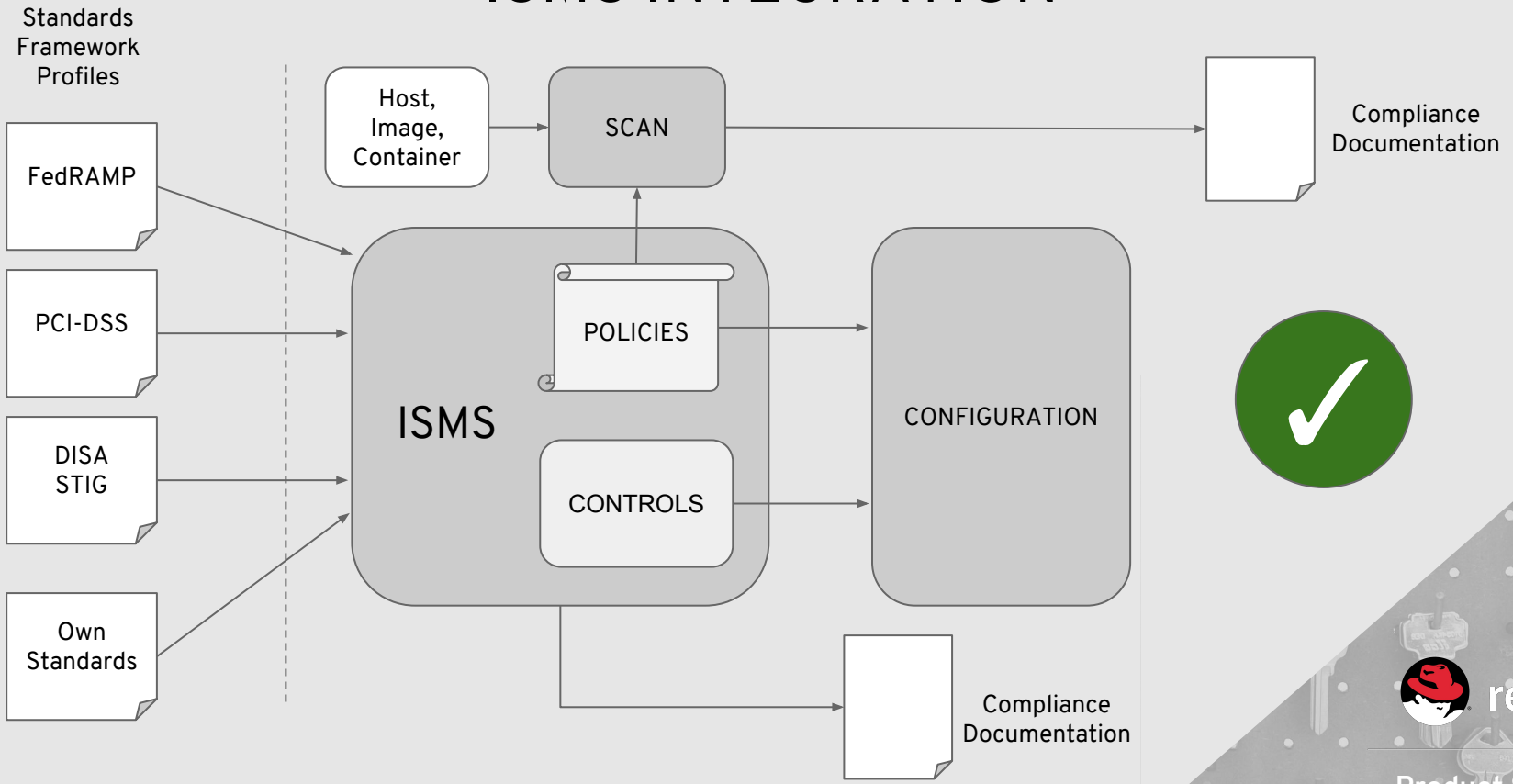
Overview | Get this image | Tech Details | Documentation | Tags



Tag Name	Date Pushed	Image Advisory	Health Index	Docker Image ID
4-12 4 latest	2 days ago	RHBA-2018:0228	A	ec769a524bd9
4-11.29	22 days ago	RHBA-2018:0072	B	3f816656bada
4-11.28	2 months ago	RHBA-2017:3333	B	04d8833ebb08
4-11.26	3 months ago	RHBA-2017:3191	B	a6679fab1888

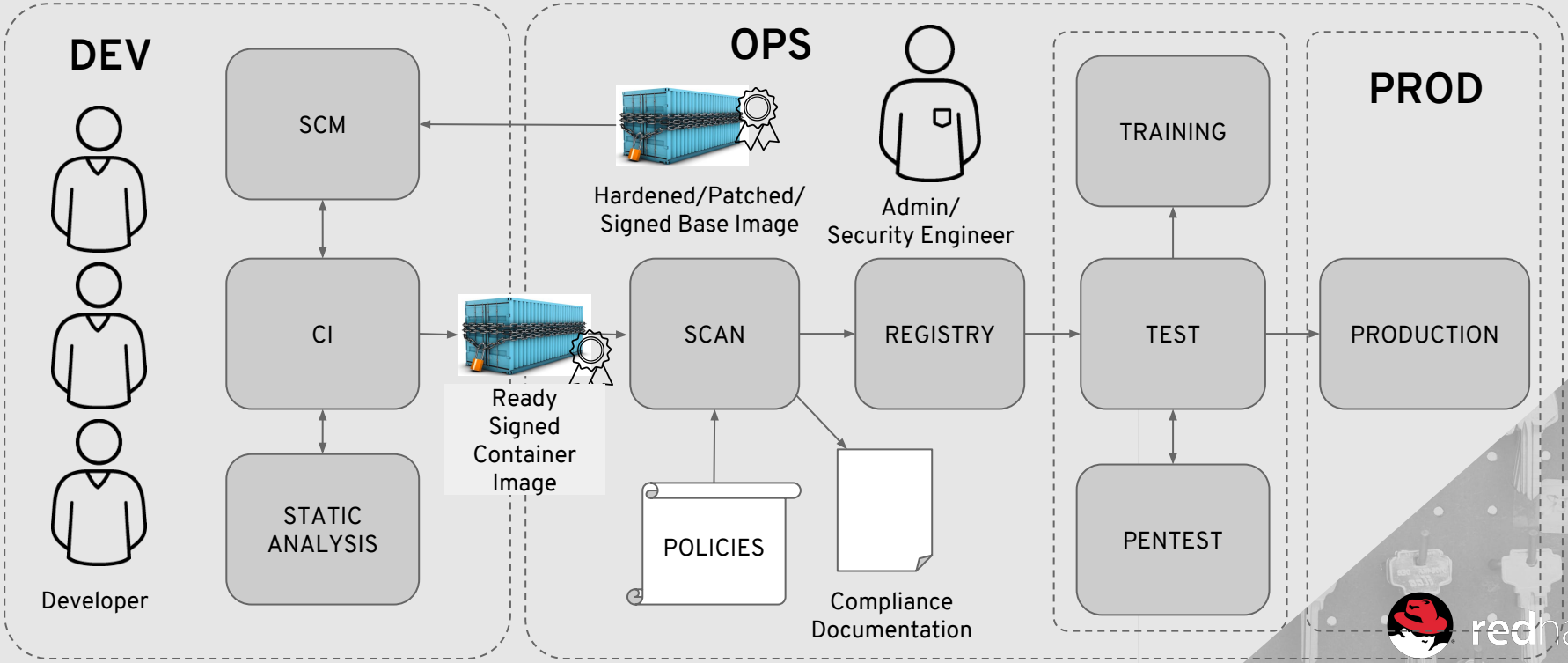
BEST PRACTICES

ISMS INTEGRATION



redhat
Product Security

CI/CD MIT CONTAINERN (DEVSECOPS)



FAZIT

RISIKEN PROFESSIONELL BEGEGNEN

- Nicht davon ausgehen, dass **“schon nichts passieren wird”**
- **Stabile, geprüfte Softwarepakete** nutzen (z.B. aus dem Red Hat Container Catalog)
- Kritische Software unbedingt und immer über **professionelle Supportverträge** absichern
- **Support-Angebot von Red Hat nutzen** (**Security Guides, Hardening Guides, Consulting** etc.) um gezielt Maßnahmen einzuleiten
- **Patch Management** konsequent als Teil eines umfassenden Sicherheits- und Compliance-Managements umsetzen
- Stets auf **unerwartet auftretende Schwachstellen** vorbereitet sein
- Organisationen mit **kontinuierlich funktionierenden Softwareentwicklungs- und -installationsprozessen** und **hohem Automatisierungsgrad** sind in der Regel besser aufgestellt

FAZIT

- Security ist eines der **Top-Themen** unserer Kunden, auch in Bezug auf Investitionen
- Security ist einer der **Hauptgründe**, sich für Red Hat zu entscheiden
- Red Hat - obwohl keine reine Security Company - verfügt über einen **sehr guten Ruf als Anbieter von Produkten und Leistungen zum Erreichen eines hohen Sicherheitsniveaus**
- Einer der wichtigsten Vorteile liegt für unsere Kunden in der Kombination von einem **tiefen Verständnis der Prozesse und Anforderungen unserer Kunden** mit der **Expertise und aktiven Rolle von Red Hat über den gesamten Stack**
- Security ist letztendlich stets eine Kombination von **organisatorischen und technischen Maßnahmen**, und immer ein Kompromiss bzw. eine Balance von **Security**, **Wirtschaftlichkeit** and **Convenience**
- Security ist niemals nur die Absicherung einer einzelnen Komponente, sondern vielmehr die **Kombination von Mindset, Techniken und Best Practices** zum Aufbau eines **vollständig abgesicherten Systems**

IHRE FRAGEN

redhat

Product Security

THANK YOU

https://access.redhat.com/security/