Evolution of risk management in software

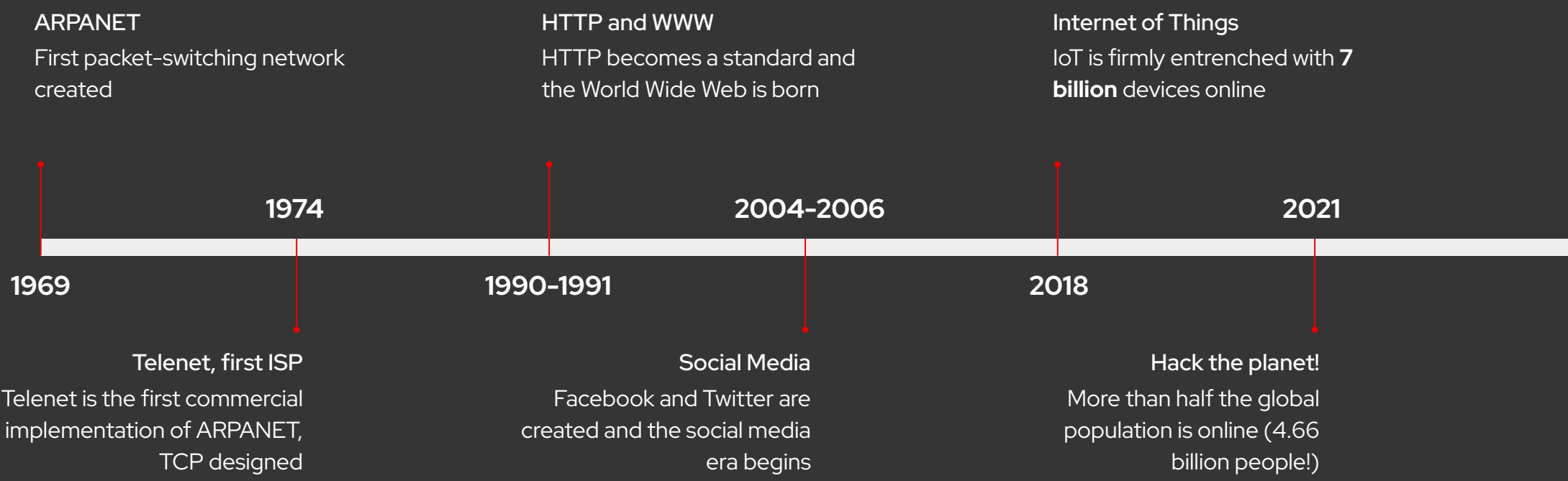
Vincent Danen
Vice President, Product Security

Red Hat
Product Security

Security is top of mind.

Across all industries, from financial to government, security is being discussed, especially as it relates to open source.

Evolution of the internet



Source: Live Science, Internet history timeline: ARPANET to the World Wide Web
https://www.livescience.com/20727-internet-history.html

Evolution of the internet

1969

ARPANET

First packet-switching network created

1974

Telenet, first ISP

Telenet is the first commercial implementation of ARPANET, TCP designed

1990–1991

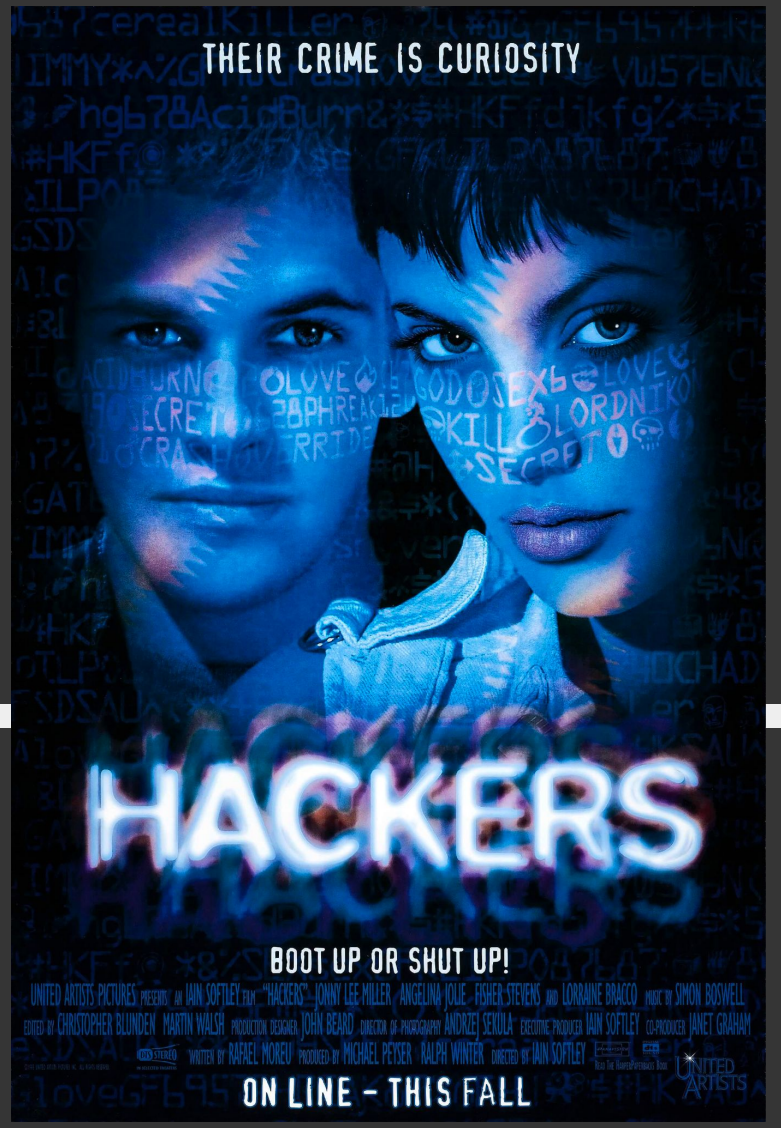
HTTP and WWW

HTTP becomes a standard and the World Wide Web is born

2004–2006

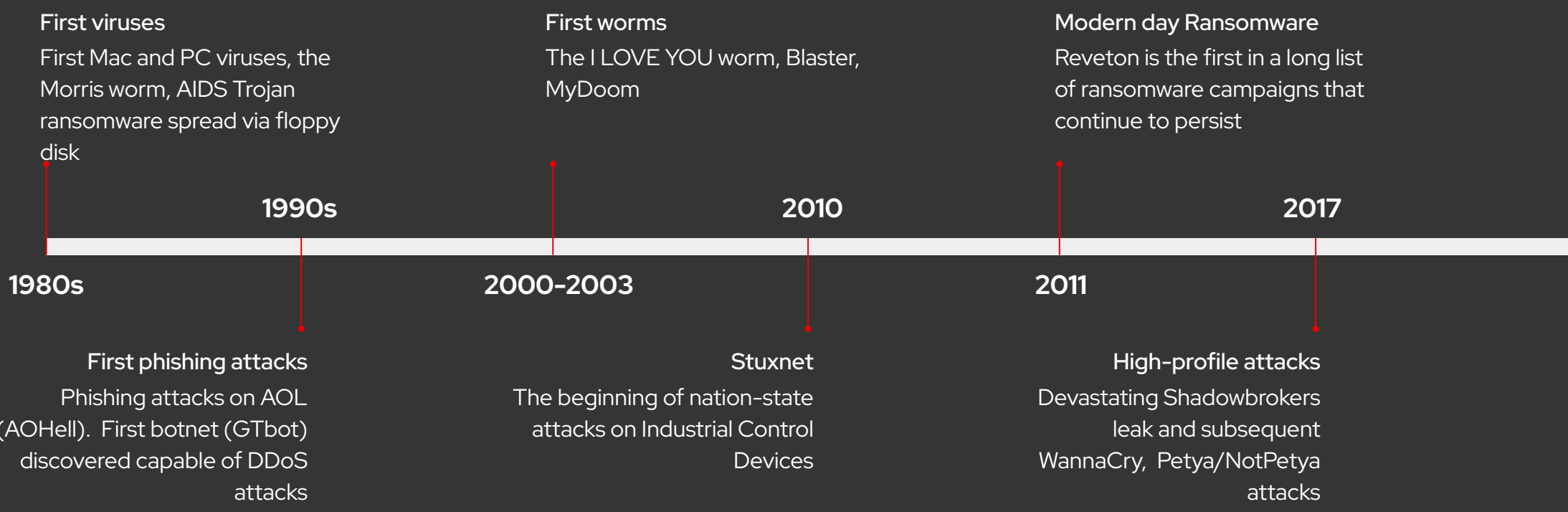
Social Media

Facebook and Twitter are created and the social media era begins



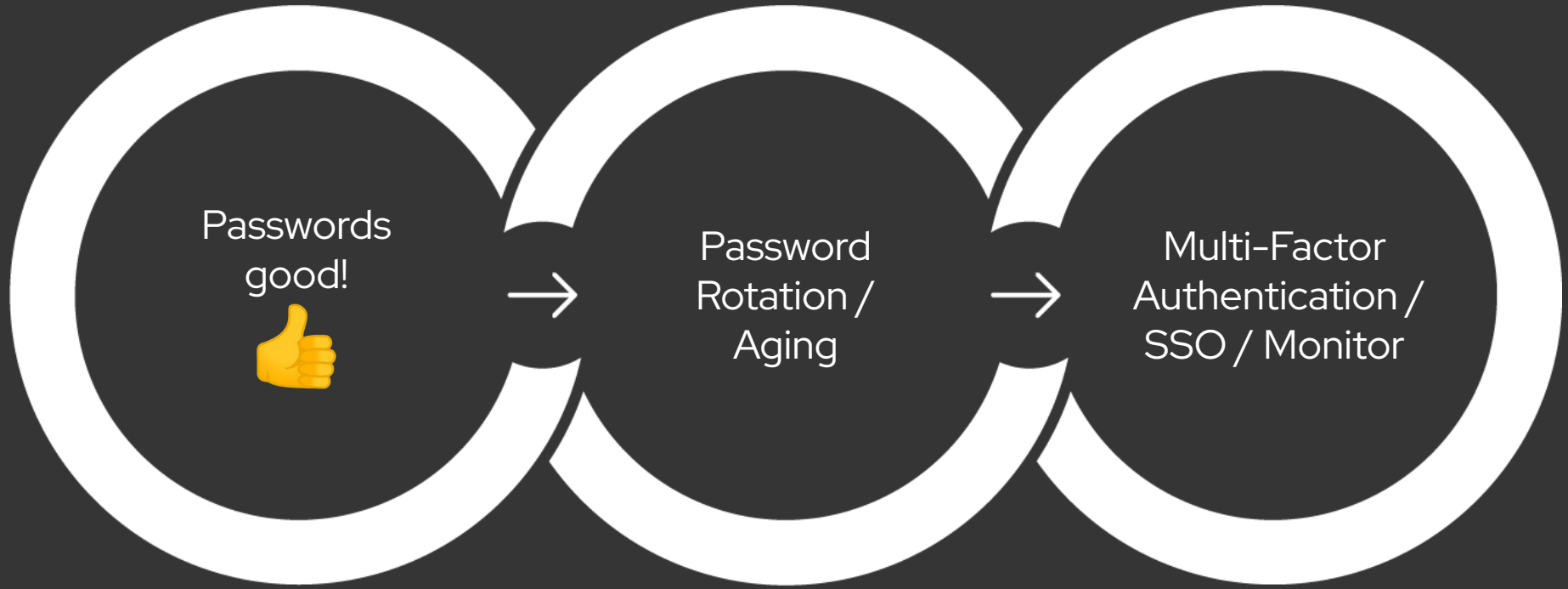
Source: Live Science, Internet history timeline: ARPANET to the World Wide Web
https://www.livescience.com/20727-internet-history.html

Evolution of Cybercrime

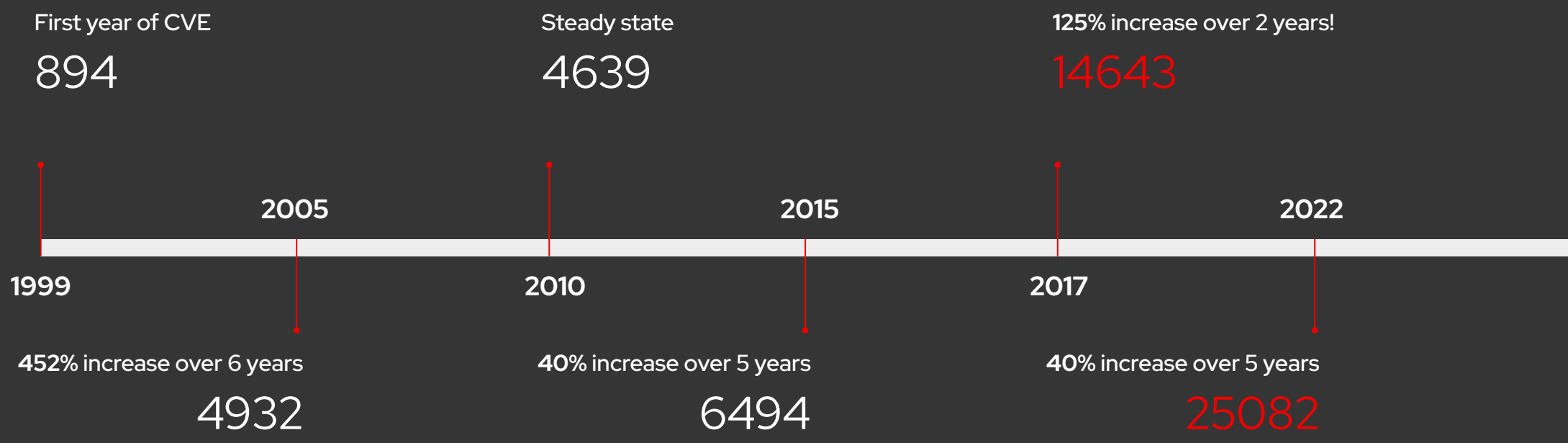


Source: Fortinet, A Brief History of The Evolution of Malware
https://www.fortinet.com/blog/threat-research/evolution-of-malware

Evolution of security practices



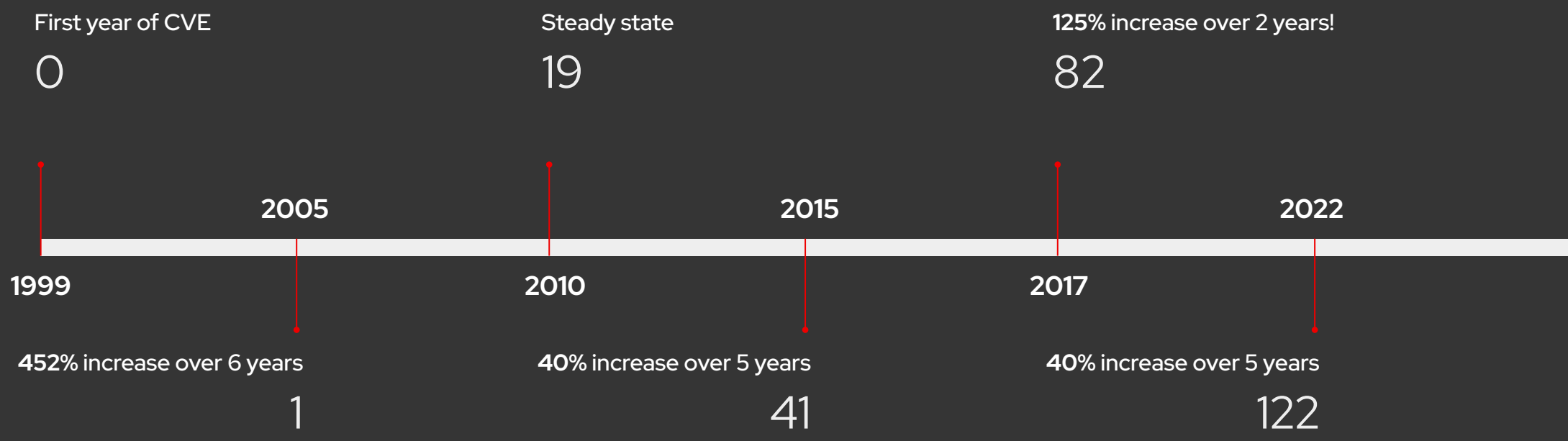
Vulnerabilities continue to increase



Source: CVE Details
https://www.cvedetails.com/

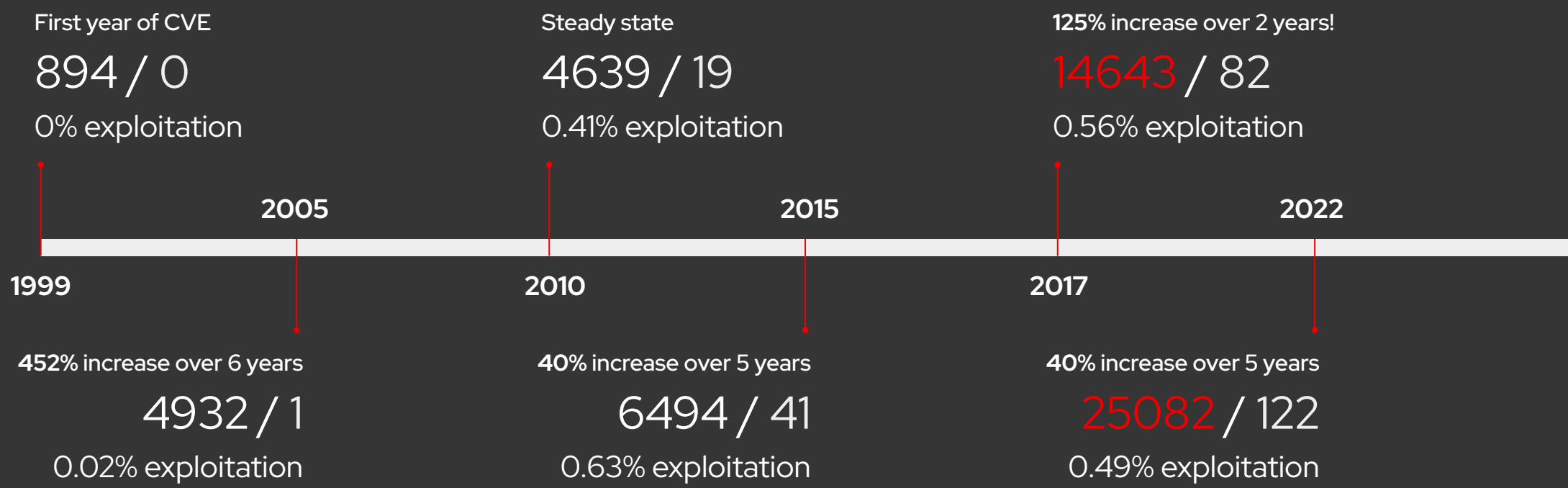
Exploitation continues to increase

Sourced from CISA Known Exploited Vulnerabilities database



Source: CVE Details
https://www.cvedetails.com/

Vulnerabilities vs Exploitation



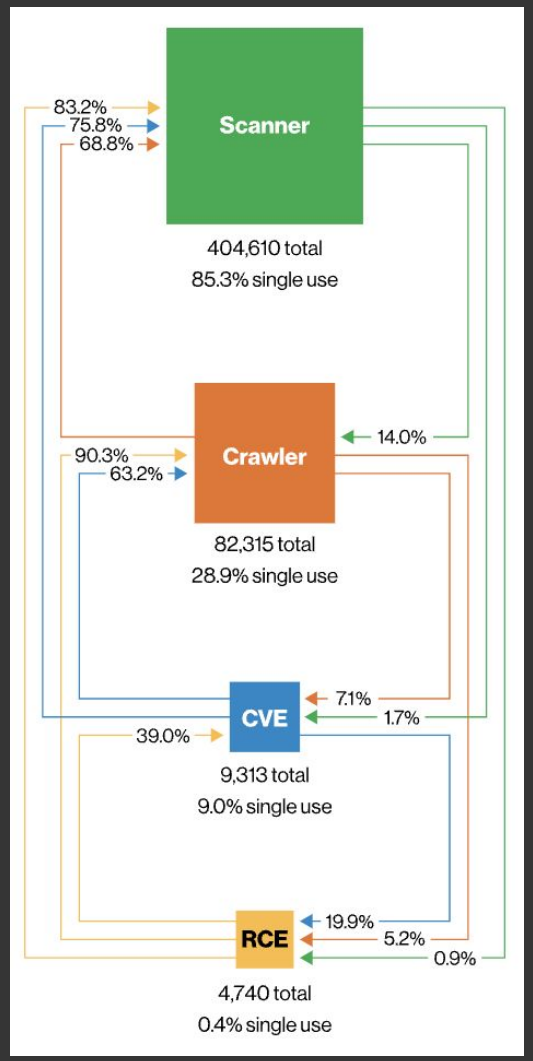
Source: CVE Details
https://www.cvedetails.com/

2022

2023

Verizon

Sources: Verizon, 2022 and 2023 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/dbir/2022/results-and-analysis-not-the-human-element/
https://www.verizon.com/business/resources/reports/dbir/2023/results-and-analysis-intro/



Where we find security risk

"The action variety of Exploit vulnerability is up to 7% of breaches this year, doubling from last year. While it's not on par with the massive numbers we see in Credentials and Phishing, it's worth some thought. The first question one might reasonably ask is "How are attackers finding these vulnerabilities?" As we pointed out last year, attackers have a sort of opportunistic attack sales funnel as seen [here]. They start with scanning for IPs and open ports. Then they move on to testing for specific CVEs. Finally, they try Remote Code Execution (RCE) to gain access to the system."

Verizon DBIR Report 2022

(Data Breach Investigations Report)

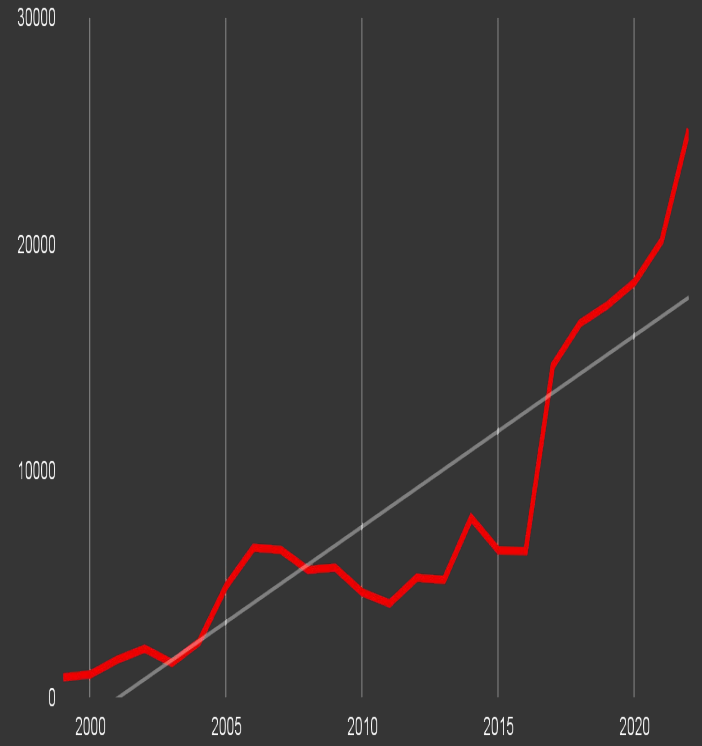
Sources: Verizon, 2022 and 2023 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/dbir/2022/results-and-analysis-not-the-human-element/
https://www.verizon.com/business/resources/reports/dbir/2023/results-and-analysis-intro/

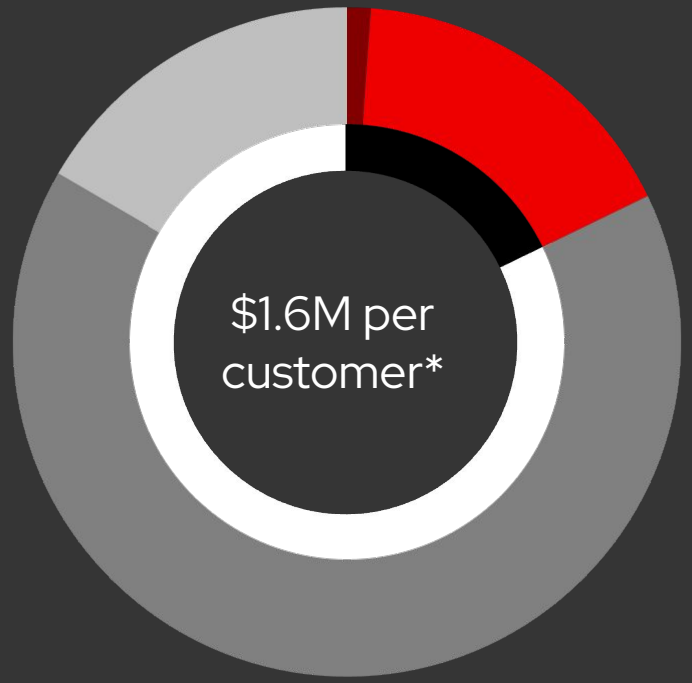
Risk by the numbers

Critical	Important	Moderate	Low	All
19 discovered	**276** discovered	**1,086** discovered	**275** discovered	**1,656*** discovered
2 known exploited	**3** known exploited	**2** known exploited	**0** known exploited	**7** known exploited
10.5%	1.1%	0.2%	0%	0.4%

Source:Red Hat Product Security risk report 2022
https://www.redhat.com/en/resources/product-security-risk-report-2022
* 1656 vulnerabilities in 2022 for the entire Red Hat portfolio of products

Cost to avoid (2022)





$276,000
Fix all Important
(3 exploited,
$92,000 each)

$1,086,000
Fix all Moderate
(2 exploited,
$543,000 each)

$19,000
Fix all Critical
(2 exploited,
$9,500 each)

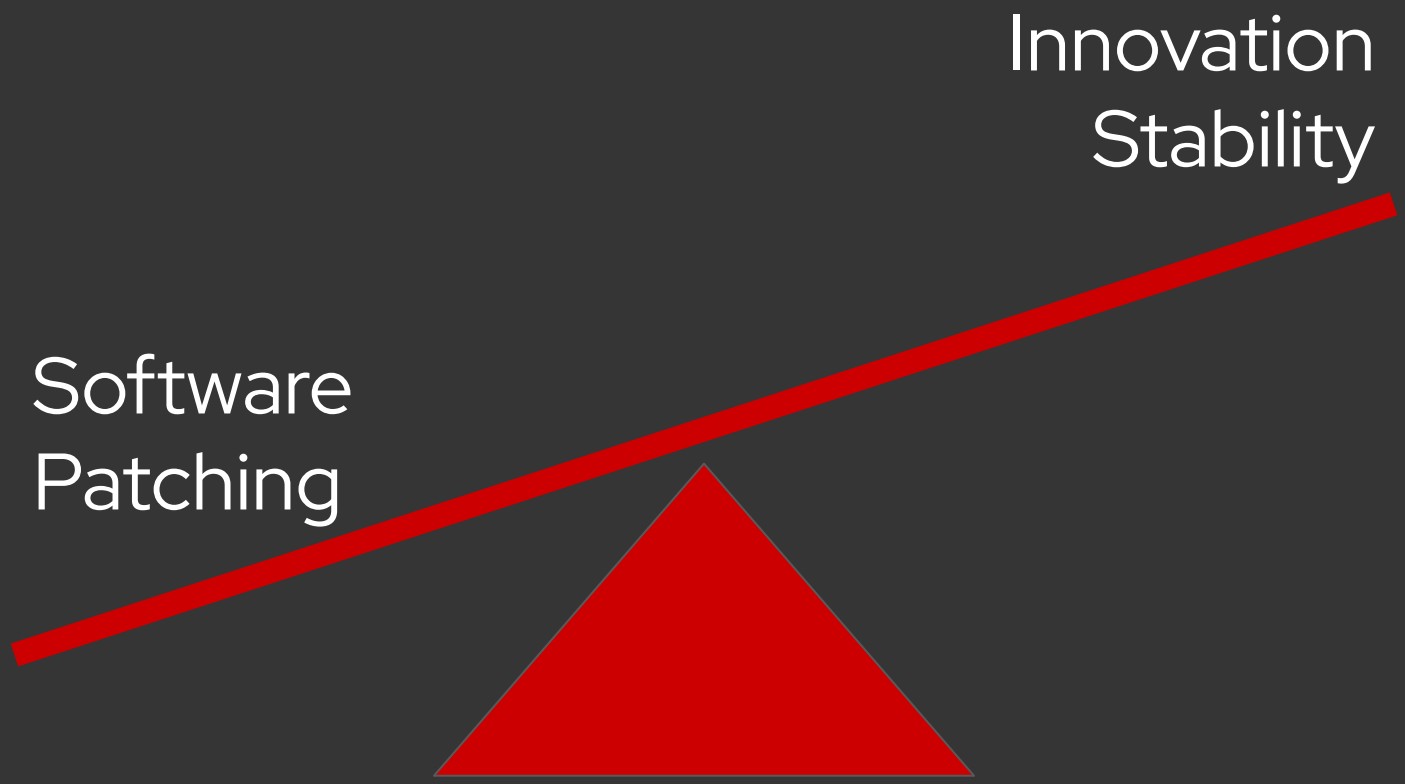
$275,000
Fix all Low
(0 exploited,
$275,000 🔥)

$295,000
Fix all risky
(5 exploited,
$59,000 each)

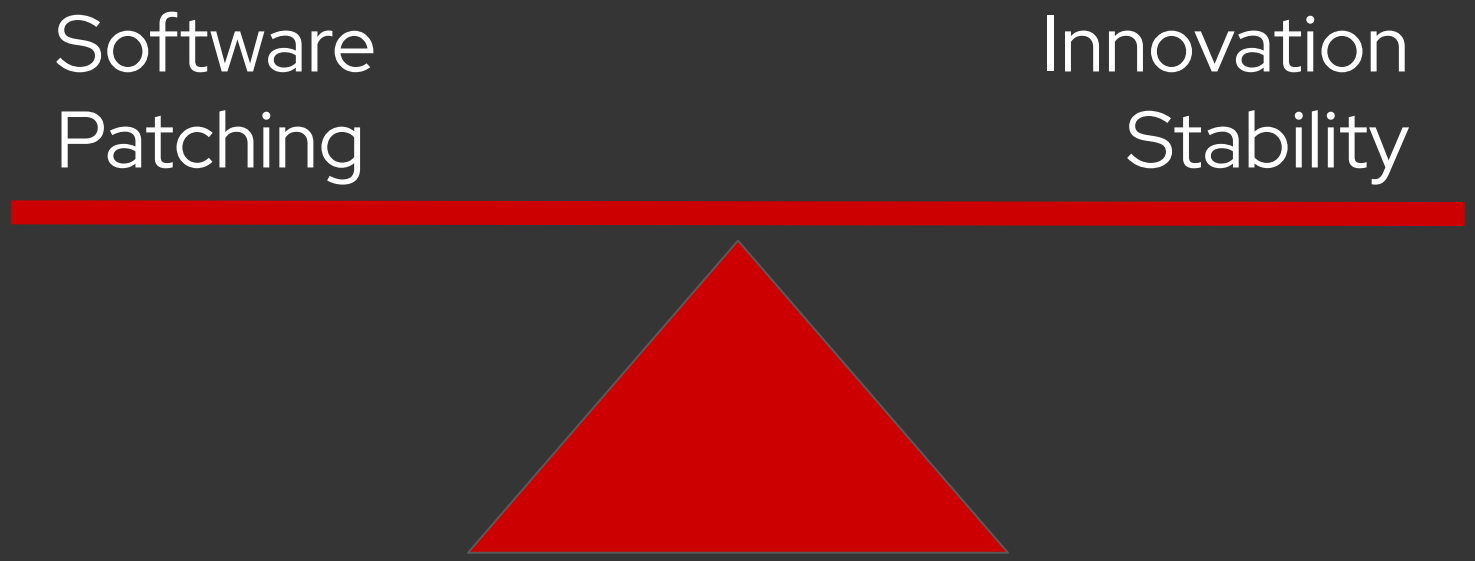
$1,361,000
Fix all not risky
(2 exploited,
$680,500 each)

* Using the assumption that every vulnerability costs a customer $1000 to fix (test and deploy).

A better balance is needed



A better balance is possible



Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat
Product Security