



Is Defense Winning?

Measuring if Cyberspace Is Becoming
More Defensible and Resilient

Columbia University
School of International and Public Affairs

Jason Healey
With Tarang Jain and Sam Dab

2024

Cybercrime costs to hit \$10.5 trn by 2025 1.39 million cyberattacks handled in 2022, phishing

High-Severity Flaws Uncovered in Bosch Thermostats at attacks rise: Cert-In

Nutrainers **exploited in the wild jumped**

Zero-day vulnerabilities becoming major source of 3, fueled by spyware vendors
cyberattacks: Verizon

exploits hard in 2023 **Check Point Research Reports Highest Increase of Global**
Internet disclos Cyber Attacks Seen in Last Two Years

Report: Cyber-attacks Soar 30% severity vulner
Globally in Q2 2024 **Rapid7 warns of alarming zero-day vulnerability**

CERT-In issues alert for trends

Ads for Zero-Day Exploit Sales Surge 70% Annually **attacks rise in volume as**
attackers revolutionise their attack


Zero-Day Attack Alert: Check Point **Windows users targeted with zero-day attacks**
Warns About Emerging Cyber Threats ; **via Internet Explorer**

Nearly 10 billion stolen passwords were **ty report unve** **Google Confirms 97**
leaked on a hacker forum **tors** **Zero-Day Attacks And**

Industrial sector ransomware attacks increased by 50% in **Points Finger At China**
Softwa **2023** **For 12**

Agenda: Let's Win

- Why “Is Defense Winning,” and What Is “Winning” Anyway
- Propositions—What Winning Looks for: Threat, Vulnerability, and Impact
- Next Steps and Conclusions



WAIT, WHAT DOES “WINNING” MEAN?

Defensive Struggles

- **“Contemporary technology cannot provide a secure system in an open environment, which includes uncleared users working at physically unprotected consoles connected to the system by unprotected communications.”**
- **“None of the known [red] team efforts has failed to date.”**
- **“Few, if any, contemporary computer security controls have prevented a [red team] from easily accessing any information sought.”**

Defensive Struggles (continued)

- **“Contemporary technology cannot provide a secure system in an open environment, which includes uncleared users working at physically unprotected consoles connected to the system by unprotected communications.”** 1970
- **“None of the known [red] team efforts has failed to date.”** 1972
- **“Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.”** 1979

Defensive Struggles (continued)

- “Contemporary technology cannot provide a secure system in an *open environment*, which includes uncleared users working at physically unprotected consoles connected to the system by unprotected communications.” 1970

O > D

- “None of the known [red] team efforts has failed to date.” 1972
- “Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.” 1979

Defensive Struggles (continued)

Defenders Have *Supremacy*

Adversaries have tremendous difficulty achieving even simple goals against poorly resourced organizations

Attackers Have *Supremacy*

Even advanced defenders struggle to prevent basic attacks and threat attackers from achieving substantial impact

Defenders Have More *Advantages*

Adversaries can succeed but somewhat unpredictably and, generally, at high cost

Attackers Have More *Advantages*

Defense can succeed but somewhat unpredictably and, generally, at high cost



Defenders Are Winning

Adversaries Are Winning

$D \gg O$

$D > O$

$D = O$

$D < O$

$D \ll O$

Defensive Struggles (continued)

Before ~1970, we were around here

- Computers were in locked rooms, tended to by (mostly) trusted staff, and malicious acts were harder and could not cascade
- Remote-access terminals multiplied attack surface
- Internetworking multiplied attack surface and added system-wide risks

Attackers have *supremacy*:
Even advanced defenders struggle preventing basic attacks and threat attackers from achieving substantial impact



Defensive Struggles (continued)

A System-Wide Offense Advantage Is Far More Than Just Simplicities Like
“The Attacker Only Has to Be Right Once...”

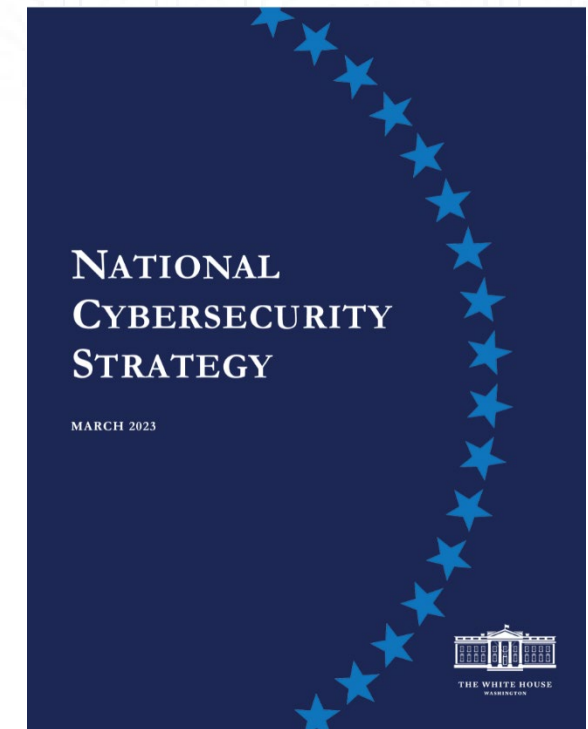
1. Internet was never designed for security
2. Internetworking both increased attack surface and allowed global access
3. Software is shipped insecurely by design and default
4. Countless single points of failure and common mode vulnerabilities exist
5. Cyberspace is tightly connected and highly interdependent; many failure modes are only obvious in retrospect; and it is prone to unpredictable, cascading failures



more recently, we have been in this range

Defensibility and Resilience: A New National Goal

- “We must make fundamental changes to the underlying dynamics of the digital ecosystem, **shifting the advantage to its defenders and perpetually frustrating the forces that would threaten it.**”
- “Maintaining an open, free, global, interoperable, reliable, and secure Internet and building a **more defensible and resilient digital ecosystem** will require generational investments by the federal government, allies and partners, and by the private sector.”



(Source: The White House. “National Cybersecurity Strategy.” Washington, DC, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>, 1 March 2023.)

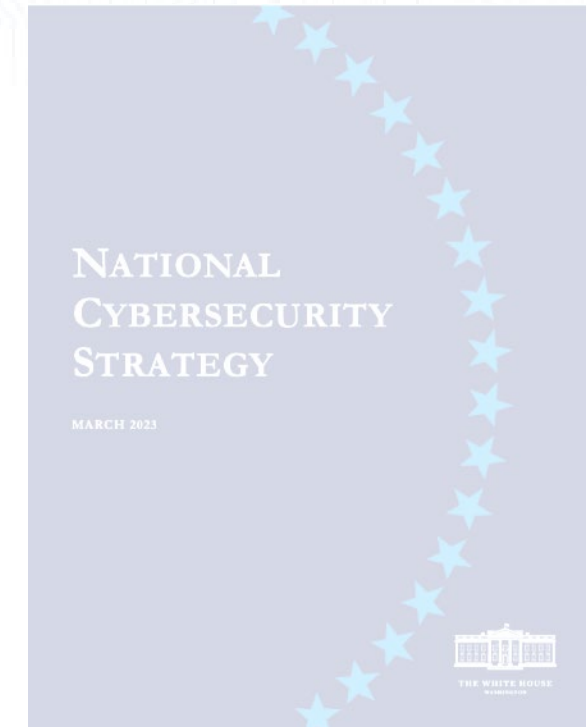
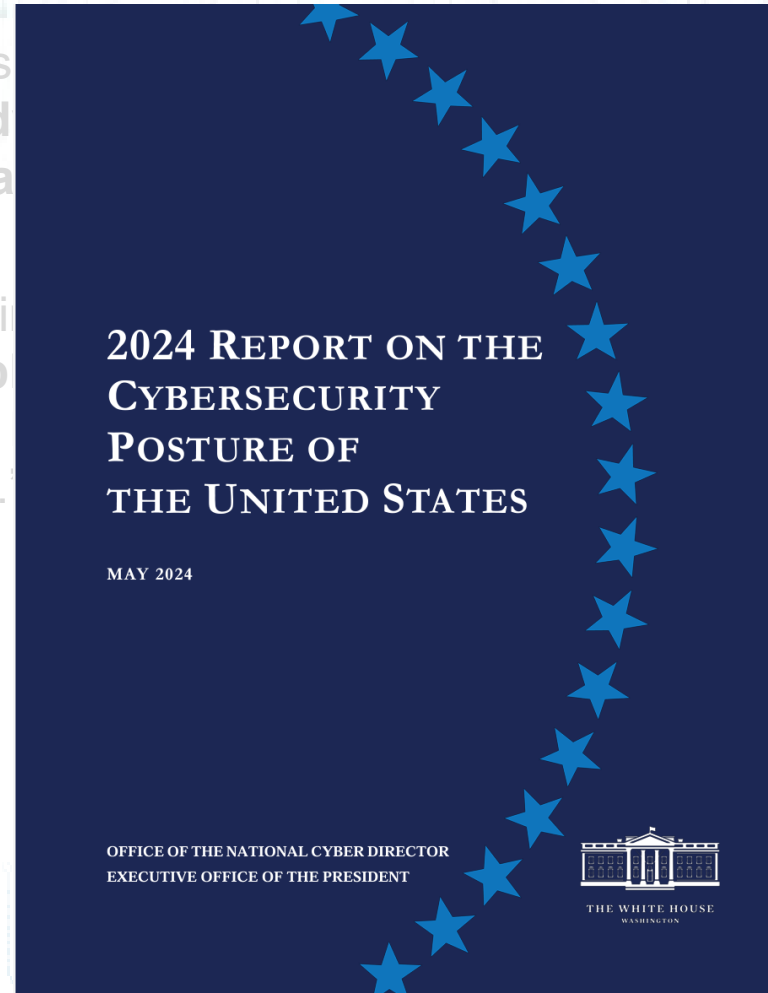
Goal D>O

02/2023

Defensibility and Resilience: A New National Goal

(continued)

- “We must make fundamental changes digital ecosystem, **shifting the ad** perpetually frustrating the forces tha
- “Maintaining an open, free, global, i Internet and building a **more defensible** will require generational investments and partners, and by the private sector.”



Goal D>O

(Source: Office of the National Cyber Director. 2024 Report on the Cybersecurity Posture of the United States. <https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf>, Washington, DC, May 2024.)

Defensibility and Resilience: A New National Goal (continued)

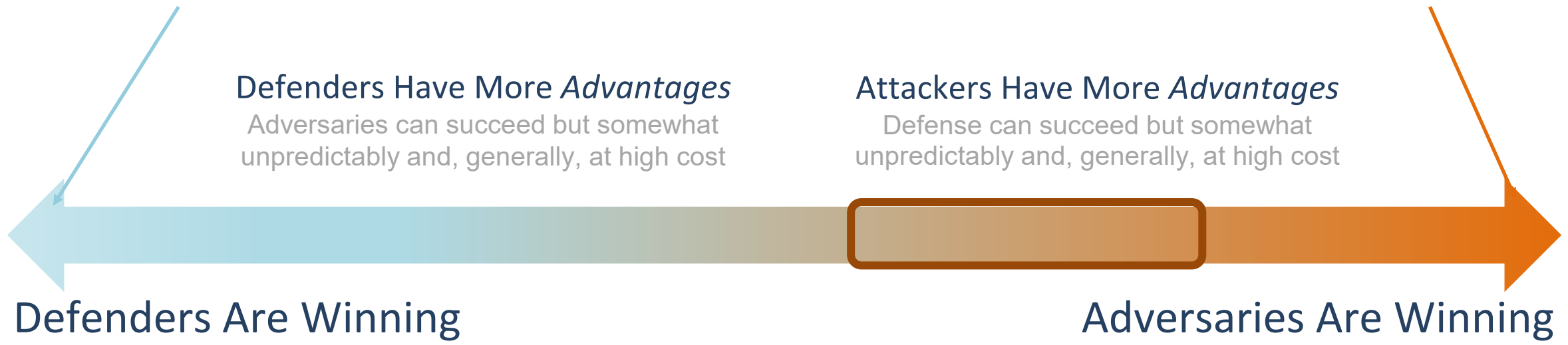


Defenders Have *Supremacy*
Adversaries have tremendous difficulty achieving even simple goals against poorly resourced organizations

Attackers Have *Supremacy*
Even advanced defenders struggle to prevent basic attacks and threat attackers from achieving substantial impact

Defenders Have More *Advantages*
Adversaries can succeed but somewhat unpredictably and, generally, at high cost

Attackers Have More *Advantages*
Defense can succeed but somewhat unpredictably and, generally, at high cost



“Winning” means sliding left, every week, month, year



HOW ARE WE MEASURING?

So Many Metrics...But Little System-Wide Insight

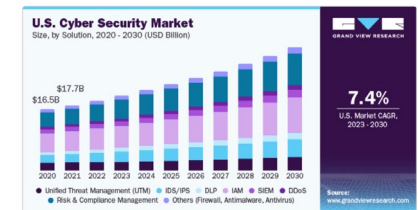
- Many metrics are fairly useless
- Others track inputs or outputs, not results
- Most are optimized for those with purchase authority
- A few are perfect for understanding system-wide dynamics
- Others are close but not quite...
 - Often not presented in time series, so no context if we are improving or not!
 - No common framework how they interact to understand the full story

Number of
Blocked Scans

So Many Metrics...But Little System-Wide Insight (continued)

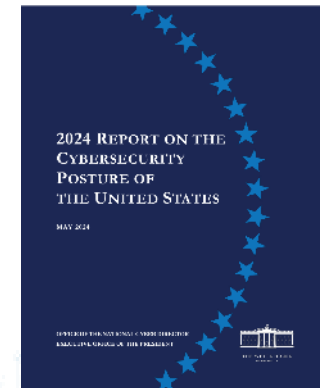
- Many metrics are fairly useless
- **Others track inputs or outputs, not results**
- Most are optimized for those with purchase authority
- A few are perfect for understanding system-wide dynamics
- Others are close but not quite...
 - Often not presented in time series, so no context if we are improving or not!
 - No common framework how they interact to understand the full story

“The global cyber security market size was estimated at [\$]222.66 billion in 2023 and is projected to grow... 12.3% from 2023 to 2030.”



(Source: Grandview Research. “Cyber Security Market Size & Trends.” GVR, <https://www.grandviewresearch.com/industry-analysis/cyber-security-market#>, 2024.)

“Skilled Cybersecurity Team Hiring: Agencies continued to strengthen skilled cybersecurity team hiring, achieving an average position fill rate of 91%.”



(Source: Office of the National Cyber Director. “2024 Report on the Cybersecurity Posture of the United States.” <https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf>, Washington, DC, May 2024.)

So Many Metrics...But Little System-Wide Insight (continued)

- Many metrics are fairly useless
- Others track inputs or outputs, not results
- **Most are optimized for those with purchase authority**
- A few are perfect for understanding system-wide dynamics
- Others are close but not quite...
 - Often not presented in time series, so no context if we are improving or not!
 - No common framework how they interact to understand the full story

“The general feeling among defenders was that an anti-Phishing ‘win’ was a 10- to 20-percent click rate”



(Source: Ragan, S. "How Do You Measure Success When It Comes to Stopping Phishing Attacks?" CSO, <https://www.csoonline.com/article/557583/how-do-you-measure-success-when-it-comes-to-stopping-phishing-attacks.html>, 23 August 2016.)

So Many Metrics...But Little System-Wide Insight (continued)

- Many metrics are fairly useless
- Others track inputs or outputs, not results
- Most are optimized for those with purchase authority
- **A few are perfect for understanding system-wide dynamics**
- Others are close but not quite...
 - Often not presented in time series, so no context if we are improving or not!
 - No common framework how they interact to understand the full story

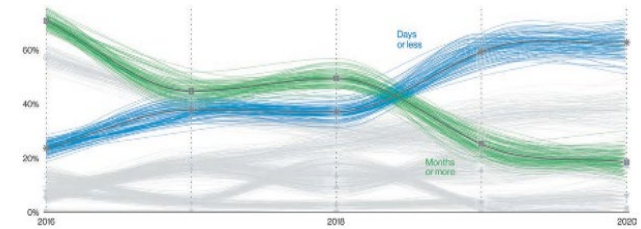


Figure 39. Discovery over time in breaches

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
All	416	243	229	205	146	99	101	78	56	24	21	16	10
External	—	—	—	—	320	107	186	184	141	73	28	19	13
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9



(Sources: Widup, S., A. Pinto, D. Hylender, G. Bassett, and P. Langlois. "2021 Data Breach Investigations Report." Verizon Business, <https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report>, May 2021 [top]; Mandiant. "Mandiant M-Trends: 2024 Special Report." Google Cloud Services, <https://services.google.com/fh/files/misc/m-trends-2024.pdf>, 2024 [bottom].)

So Many Metrics...But Little System-Wide Insight (continued)

- Many metrics are fairly useless
- Others track inputs or outputs, not results
- Most are optimized for those with purchase authority
- A tiny few are perfect for understanding system-wide dynamics
- Others are close but not quite...
 - Often not presented in time series, so no context if we are improving or not!
 - No common framework how they interact to understand the full story

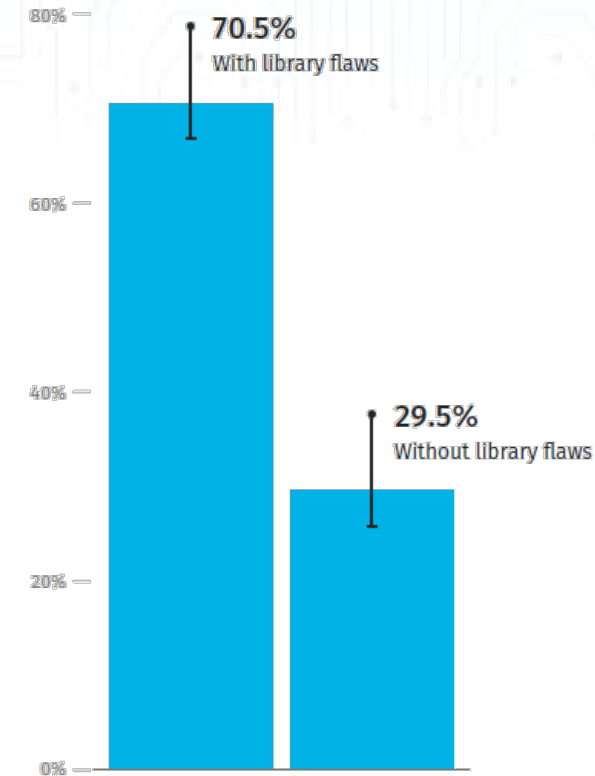


Figure 11
Applications with flaws in an open source library on first scan



(Source: Veracode, Inc. "State of Software Security 2023: Annual Report on the State of Application Security." Veracode, https://info.veracode.com/rs/790-ZKW-291/images/Veracode_State_of_Software_Security_2023.pdf, 2023.)

So Many Metrics...But Little System-Wide Insight (continued)

- Many metrics are fairly useless
- Others track inputs or outputs, not results
- Most are optimized for those with purchase authority
- A tiny few are perfect for understanding system-wide dynamics
- Others are close but not quite...
 - Often not presented in time series, so no context if we are improving or not!
 - No common framework how they interact to understand the full story

Zero-Days Exploited In-The-Wild by Year

ENTERPRISE vs. END USER

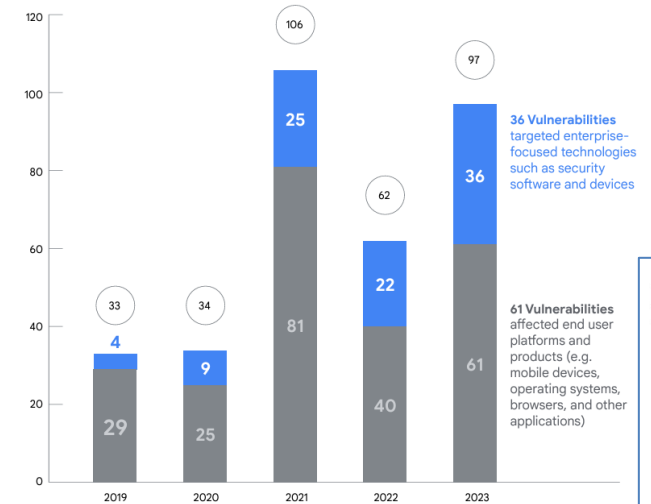
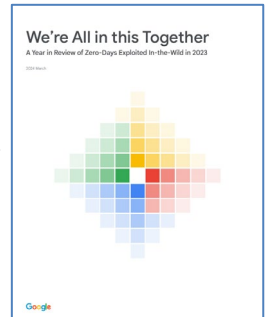


Figure 1. Zero-days exploited in-the-wild by year

36 Vulnerabilities targeted enterprise-focused technologies such as security software and devices

61 Vulnerabilities affected end user platforms and products (e.g. mobile devices, operating systems, browsers, and other applications)



(Source: Mandiant and Threat Analysis Group. "We're All in This Together: A Year in Review of Zero-Days Exploited in-the-Wild in 2023." Google, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf, March 2024.)

Similar Efforts to *Measure Defensibility*

Many Related Efforts

- National cybersecurity performance metrics (Office of the National Cyber Director)
- Cyber as public health (Cyber Green Initiative)
- Leading cyberindicators (President's Council of Advisors on Science and Technology)
- Cybervital statistics (World Economic Forum Global Cybersecurity Outlook)

Yes, We Have a Data Problem

- Cannot do rigor yet (or ever)
- But...we can use discipline: developing logical propositions of what we would expect to see if we were winning or losing
- Then, see if the trends for the same proposition, reported from different sources, are directionally consistent

This is about “good enough for now” public policy indicators, not the rigorous scientific methodologies we will eventually need

One Way to Tackle This...



Threat

Vulnerability

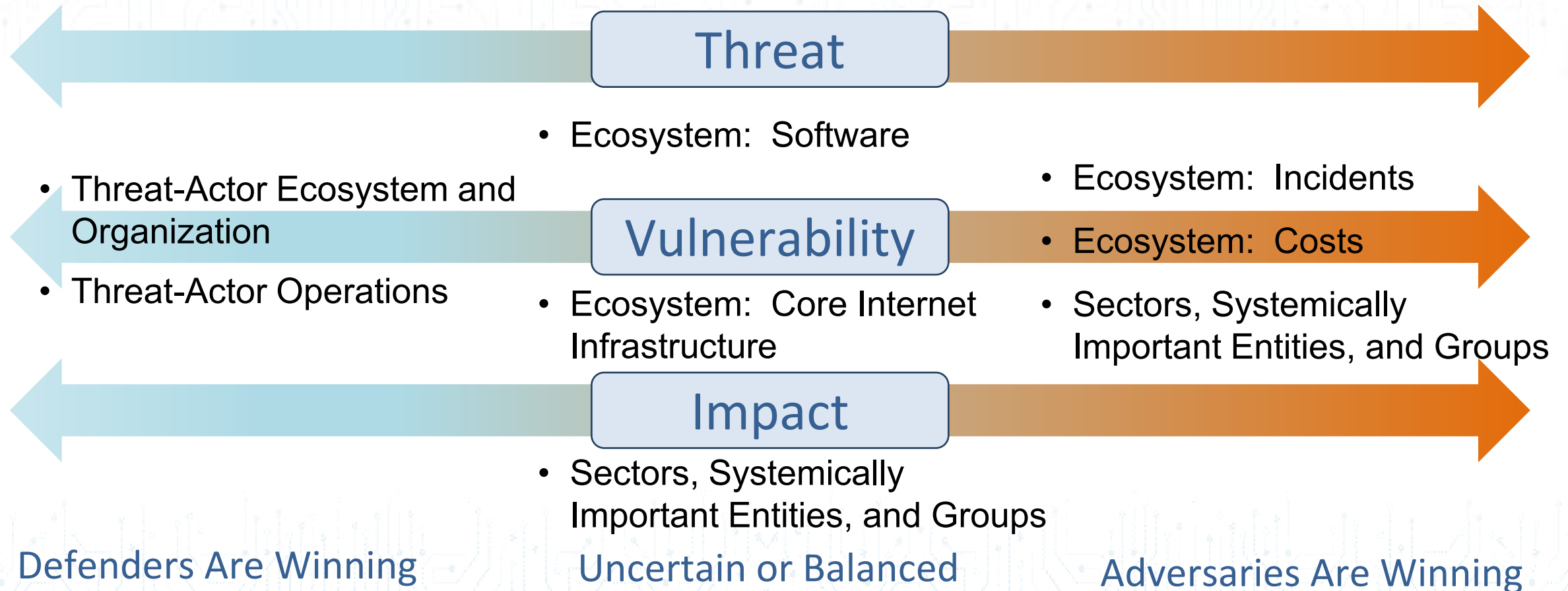
Impact

Defenders Are Winning

Uncertain or Balanced

Adversaries Are Winning

One Way to Tackle This... (continued)





PROPOSITIONS: THREAT

Threat Indicators

What might we expect to see if defenders were successfully disrupting adversaries and their operations over the long term?

Threat Indicators: Operations

What might we expect to see if defenders were successfully disrupting adversaries and their operations over the long term?

Threat-Actor Operations

- Rapid change in tactics, techniques, and procedures (TTPs)
- Shift from easier to harder TTPs
- Frequent retooling of infrastructure
- Rapid turnover of vulnerabilities
- Increase in number, price of zero-days
- Longer attack chains
- Detected, ejected from systems faster
- Attributed relatively easily and quickly

Threat Indicators: Ecosystem and Operations

What might we expect to see if defenders were successfully disrupting adversaries and their operations over the long term?

Threat-Actor Operations

- Rapid change in TTPs
- Shift from easier to harder TTPs
- Frequent retooling of infrastructure
- Rapid turnover of vulnerabilities
- Increase in number, price of zero-days
- Longer attack chains
- Detected, ejected from systems faster
- Attributed relatively easily and quickly

Threat-Actor Ecosystem and Organizations

- Lower profits
- Smaller groups driven out of business
- Consolidation into larger, more capable groups
- Degraded trust between groups
- Struggles to find new talent

These Are *Propositions*: Logical Expressions of Expectations
Many Ambiguous on Their Own—But Have Meaning When Grouped Together

Threat Indicators

Some might be really hard to measure routinely and accurately...

Threat-Actor Operations

- Rapid change in TTPs
- Shift from easier to harder TTPs
- Frequent retooling of infrastructure
- Rapid turnover of vulnerabilities
- Increase in number, price of zero-days
- Longer attack chains
- Detected, ejected from systems faster
- **Attributed relatively easily and quickly**

Threat-Actor Ecosystem and Organizations

- **Lower profits**
- Smaller groups driven out of business
- Consolidation into larger, more capable groups
- **Degraded trust between groups**
- Struggles to find new talent

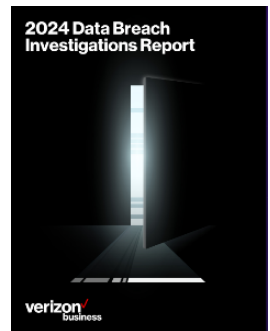
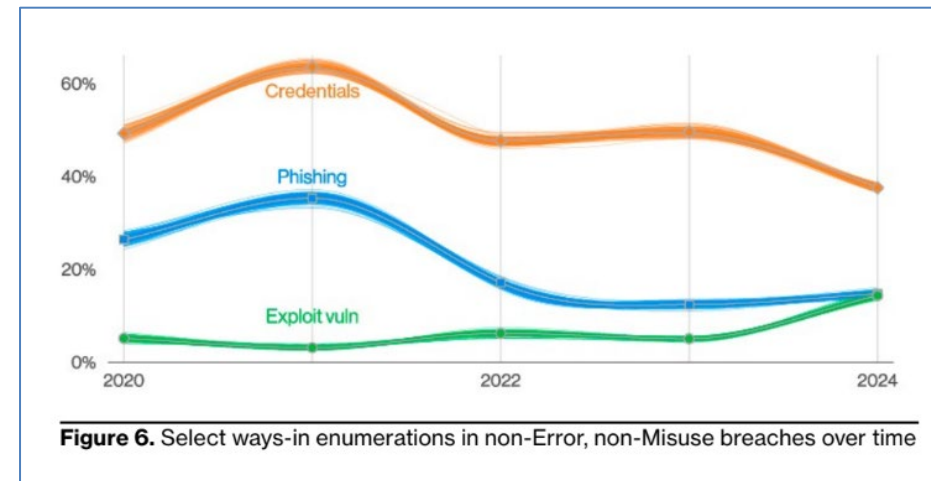
These Are *Propositions*: Logical Expressions of Expectations
 Many Ambiguous on Their Own—But Have Meaning When Grouped Together

Threat Indicators (continued)

Some might be really hard to measure, routinely and accurately...
Some already are, in time series.

Threat-Actor Operations

- Rapid change in TTPs
- **Shift from easier to harder TTPs**
- Frequent retooling of infrastructure
- Rapid turnover of vulnerabilities
- Increase in number, price of zero-days
- Longer attack chains
- Detected, ejected from systems faster
- Attributed relatively easily and quickly



(Source: Hylender, C. D., P. Langlois, A. Pinto, and S. Widup. "2024 Data Breach Investigation Report." Verizon Business, <https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf>, 2024.)

These Are *Propositions*: Logical Expressions of Expectations
Many Ambiguous on Their Own—But Have Meaning When Grouped Together

Threat Indicators (continued)

Some might be really hard to measure, routinely and accurately...
 some already are, in time series.

Threat-Actor Operations

- Rapid change in TTPs
- Shift from easier to harder TTPs
- Frequent retooling of infrastructure
- Rapid turnover of vulnerabilities
- Increase in number, price of zero-days
- Longer attack chains
- **Detected, ejected from systems faster**
- Attributed relatively easily and quickly

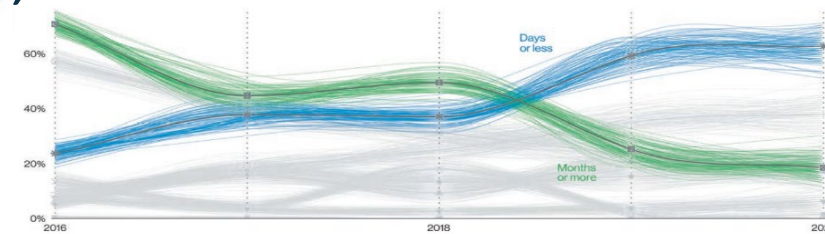
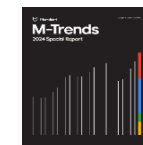
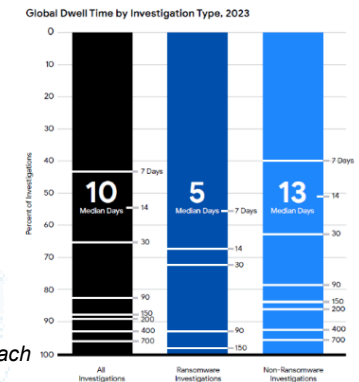


Figure 39. Discovery over time in breaches

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
All	416	243	229	205	146	99	101	78	56	24	21	16	10
External	—	—	—	—	320	107	186	184	141	73	28	19	13
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9



“Nearly two thirds of all intrusions in 2023 were detected within 30 days. This **likely indicates that detection capabilities continue to improve across organizations**, allowing defenders to be notified of threats during the initial infection or reconnaissance phases of the targeted attack lifecycle.”



(Sources: Widup, S., A. Pinto, C. D. Hylender, G. Bassett, and P. Langlois. “2021 Data Breach Investigations Report.” Verizon Business, <https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf>, May 2021 [top]; Mandiant. “Mandiant M-Trends: 2024 Special Report.” Google Cloud Services, <https://services.google.com/fh/files/misc/m-trends-2024.pdf>, 2024 [bottom].)



PROPOSITIONS: VULNERABILITY

Vulnerability Indicators

Ecosystem: Software

- Increased diversity of vulnerabilities
- Reduced stubbornness of vulnerabilities
- Secure, repeatable software development life cycle (SDLC)
- More secure open source and supply chain
- Reduced tail of abandoned critical code

Ecosystem: Core Internet Infrastructure

- Fewer single points of failure
- Increased resilience
- Secure and resilient routing and protocols

Sectors, Systemically Important Entities, and Groups

- Fewer single points of failure and increased resilience
- More companies above the cyberpoverty line?
- Reduced vulnerability of most at-risk populations

Vulnerability Indicators: Internet Infrastructure

Ecosystem: Core Internet Infrastructure

- Domain Name Systems (DNS) Instances, as of 24 December 2024 (Source: root-servers.org. "FAQ." <https://root-servers.org>, accessed December 2024.)
- Root Server Map (Source: <https://espace-mondial-atlas.sciencespo.fr/en/topic-contrasts-and-inequalities/map-1C19-EN-location-of-domain-name-root-servers-2018andnbsp.html>.)
- Internet Exchange Points, Number and Map, as of 24 December 2024 (Source: Packet Clearing House. "Internet Exchange Points." PCH, https://www.pch.net/services/internet_exchange_points, accessed December 2024.)

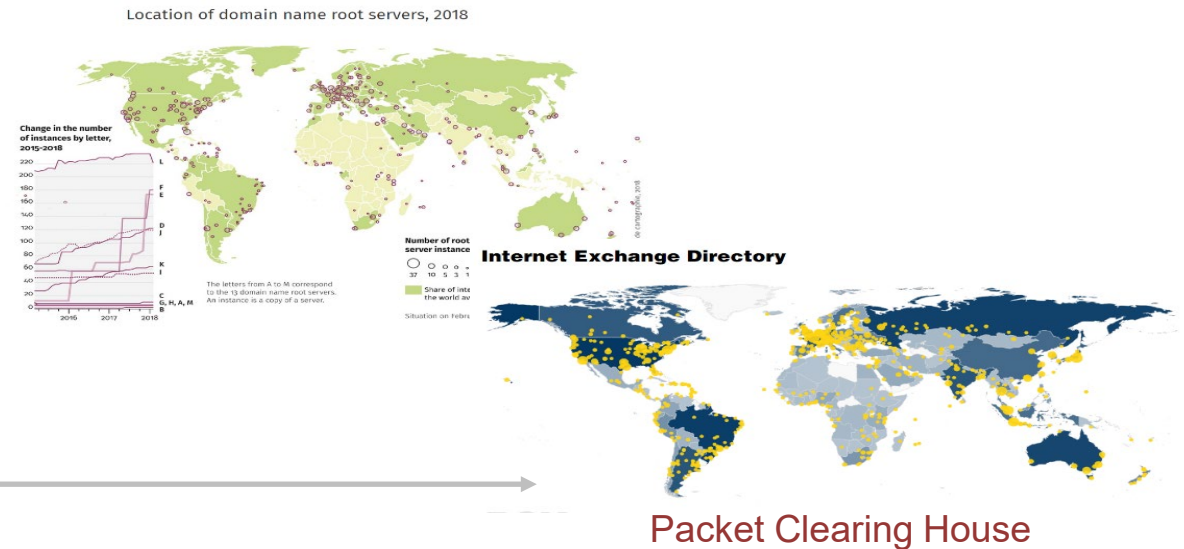
- Fewer single points of failure
- Increased resilience
- Secure and resilient routing and protocols

Number of DNS Root Servers and Instances

- 1984: 1 (University of Southern Carolina)
- 1985: 4
- 1997: 12 (maximum, due to limitations of User Datagram Protocol (UDP))
- 2024: 1,921 (with anycast, added ~2008)

Number of Internet Exchange Points

- 1992: 1 (Metropolitan Area Exchange (MAE)-EAST)
- 1994: 2 (MAE-EAST, MAE-WEST)
- 2024: 1,180



Vulnerability Indicators

Ecosystem: Software

- Increased diversity of vulnerabilities
- Reduced stubbornness of vulnerabilities
- Secure, repeatable SDLC
- More secure open source and supply chain
- Reduced tail of abandoned, critical code

Ecosystem: Core Internet Infrastructure

- Fewer single points of failure
- Increased resilience
- Secure and resilient routing and protocols

Sectors, Systemically Important Entities, and Groups

- Fewer single points of failure and increased resilience
- More companies above the cyberpoverty line?
- Reduced vulnerability of most at-risk populations

These are *propositions*: logical expressions of expectations

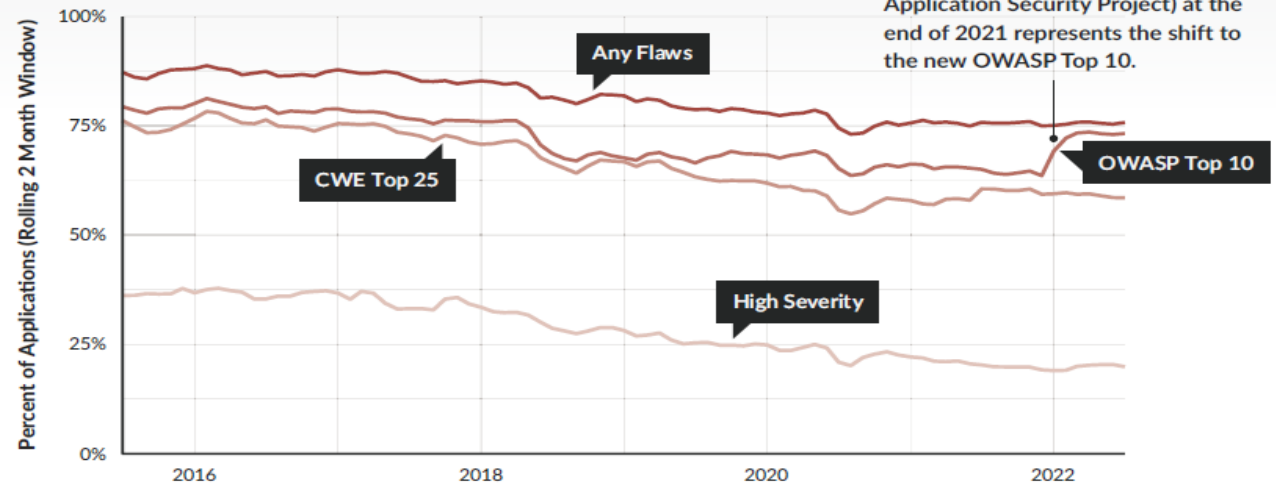
Vulnerability Indicators: Software

Ecosystem: Software

- Increased diversity of vulnerabilities
- Reduced stubbornness of vulnerabilities
- **Secure, repeatable SDLC**
- **More secure open source and supply chain**
- Reduced tail of abandoned, critical code

- Veracode found “every measurement trends downward over the last six years”
- **~30% improvement** in number of applications with high-severity flaws
- **Also ~30% improvement** in software without “flaw in an open-source library when they are first scanned” by Veracode

Figure 4: Existing Flaws in Applications Over Time



(Source: Veracode, Inc.. “State of Software Security: Annual Report on the State of Application Security.” https://info.veracode.com/rs/790-ZKW-291/images/Veracode_State_of_Software_Security_2023.pdf, 2023.)

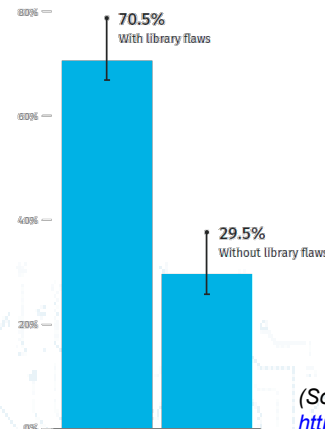


Figure 11
Applications with flaws in an open source library on first scan



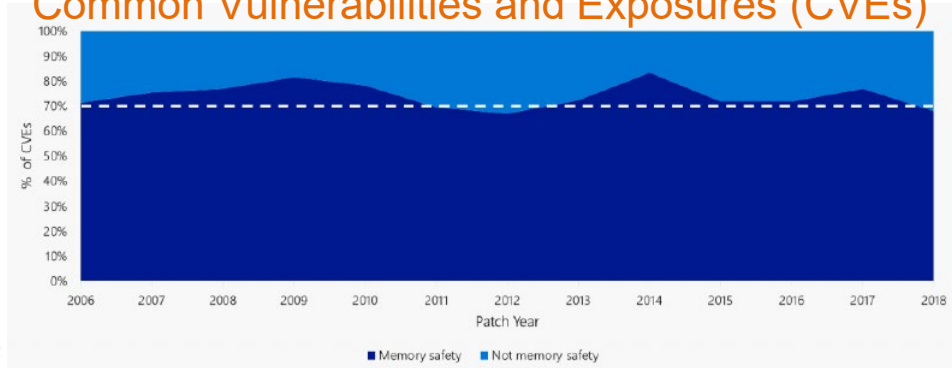
(Source: Veracode, Inc. “State of Software Security: Open Source Edition.” <https://info.veracode.com/report-state-of-software-security-open-source-edition.html>, Veracode, accessed December 2024.)

Vulnerability Indicators: Software (continued)

Ecosystem: Software

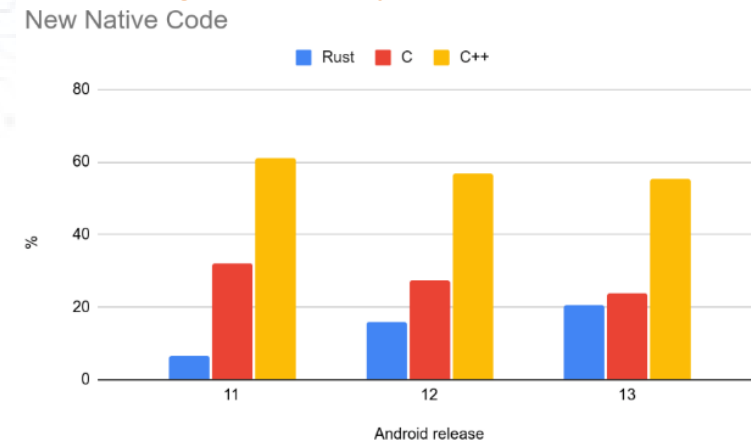
- Increased diversity of vulnerabilities
- Reduced stubbornness of vulnerabilities
- Secure, repeatable SDLC
- More secure open source and supply chain
- Reduced tail of abandoned, critical code

Percent of Microsoft-Assigned Memory-Safety Common Vulnerabilities and Exposures (CVEs)

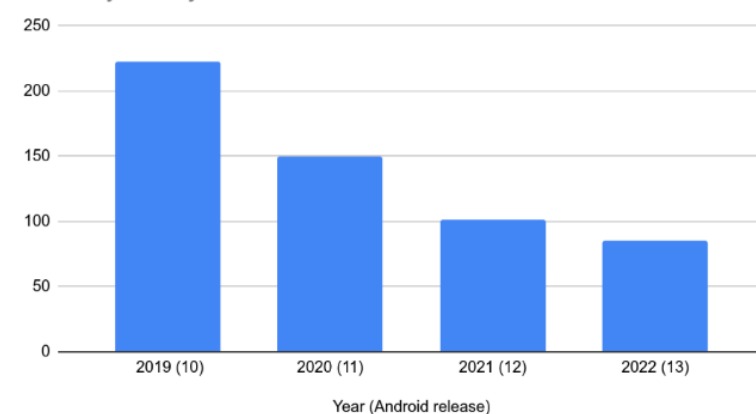


(Source: Microsoft. "We Need a Safer Systems Programming Language." MSRC, <https://msrc.microsoft.com/blog/2019/07/we-need-a-safer-systems-programming-language/>, accessed December 2024.)

Google Memory Safe Use and Vulnerabilities



Memory Safety Vulnerabilities Per Year



(Source: Vander Stoep, J. "Eliminating Memory Safety Vulnerabilities at the Source." Google Security Blog, <https://security.googleblog.com/2024/09/eliminating-memory-safety-vulnerabilities-Android.html>, 25 September 2024.)

Good...but Just Memory Safe Is Too Specific!

Vulnerability Indicators

Ecosystem: Software

- **Increased diversity of vulnerabilities**
- Reduced stubbornness of vulnerabilities
- Secure, repeatable SDLC
- More secure open source and supply chain
- Reduced tail of abandoned, critical code

Increased Diversity of Vulnerabilities

- What are the indicators SDLC is not just killing off a particular category of vulnerability but has a repeatable process to keep doing so?
 - Known Exploited Vulnerabilities (KEV), Open Web Application Security Project (OWASP) 10, and Common Weakness Enumerations (CWE) 25 lists have a decreasing number of new flaws in the same category as classes of vulnerability get eliminated
 - No single category of flaws represents more than a plurality within those lists or in major codebases

Vulnerability Indicators (continued)

Ecosystem: Software

- Increased diversity of vulnerabilities
- Reduced stubbornness of vulnerabilities
- Secure, repeatable SDLC
- More secure open-source and supply chain
- Reduced tail of abandoned, critical code

Increased Diversity of Vulnerabilities

- What are the indicators SDLC is not just killing off a particular category of vulnerability but has a repeatable process to keep doing so?
 - KEV, OWASP 10, and CWE 25 lists have a decreasing number of new flaws in the same category as classes of vulnerability get eliminated
 - No single category of flaws represents more than a plurality within those lists or in major codebases

Reduced Stubbornness of Vulnerabilities

- What are indicators that end users are patching, at scale?
 - Decreasing duration that individual flaws remain on OWASP 10 and CWE 25; lists should have a high turnover as vulnerabilities are quickly remediated
 - Decreasing average age of vulnerabilities used in successful incidents



PROPOSITIONS: IMPACT

Impact Indicators

Ecosystem: Incidents

- Fewer overall incidents
- Fewer catastrophic incidents and events
- Fewer one-on-multitude and cascading incidents

Ecosystem: Costs

- Reduced monetary losses
- Reduced economic impact
- Fewer direct and indirect deaths
- Fewer national-security-relevant incidents

Sectors, Systemically Important Entities, and Groups

- Reduced downtime of public core of the internet
- Similar categories for global, just at different scope

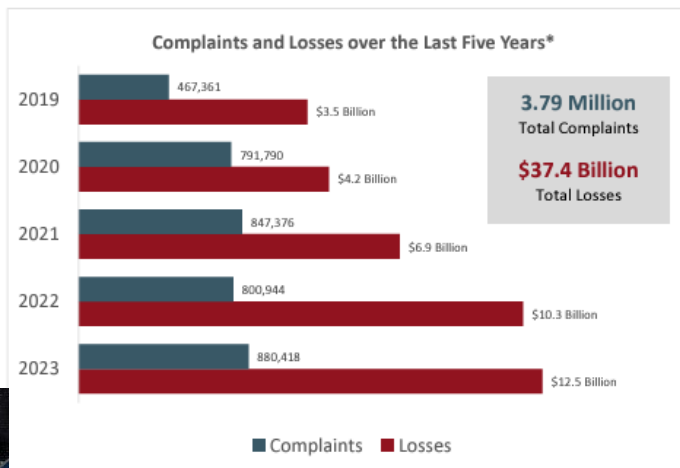
Impact Indicators (continued)

Ecosystem: Incidents

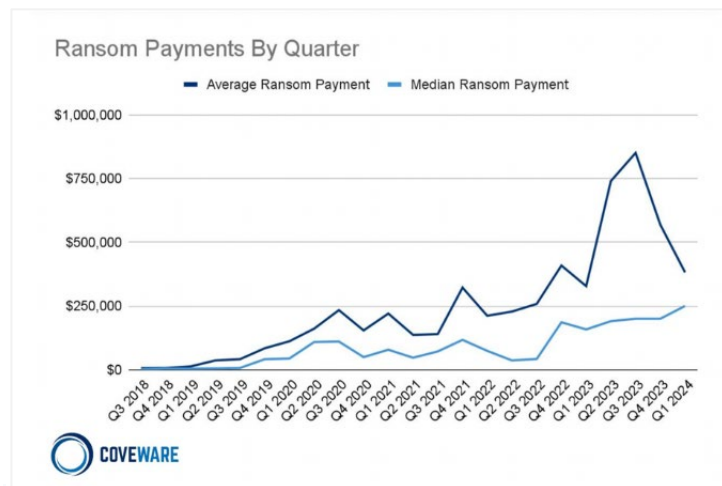
- Fewer overall incidents
- Fewer catastrophic incidents and events
- Fewer one-on-multiple and cascading incidents

Ecosystem: Costs

- Reduced monetary losses
- Reduced economic impact
- Fewer direct and indirect deaths
- Fewer national-security-relevant incidents



(Source: Federal Bureau of Investigation. "Federal Bureau of Investigation Internet Crime Report 2023." https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf, 2023.)



(Source: Coveware, Inc. "RaaS Devs Hurl Their Credibility by Cheating Affiliates in Q1 2024." <https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024>, 17 April 2024.)

Estimated Global Damages From Cybercrime

- 2015: \$3 trillion
- 2021: \$6 trillion
- 2025: \$10.5 trillion

(Source: Morgan, S. "Cybercrime to Cost the World \$10.5 Trillion Annually by 2025." Cybercrime Magazine, <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>, 13 November 2020.)

Impact Indicators (continued)

Ecosystem: Incidents

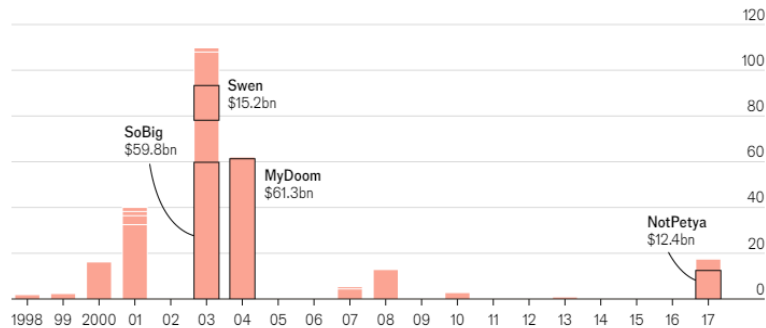
- Fewer overall incidents
- Fewer catastrophic incidents and events
- Fewer one-on-multitude and cascading incidents

Ecosystem: Costs

- Reduced monetary losses
- Reduced economic impact
- Fewer direct and indirect deaths
- Fewer national-security-relevant incidents

NotSoBig

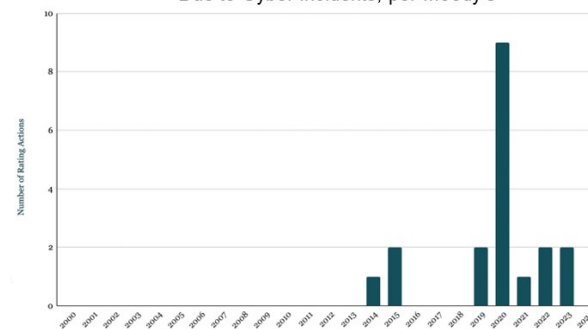
Global economic losses from significant cyber attacks*, \$bn, 2023 prices



Source: Tom Johansmeyer *Includes events with over \$800m in economic losses and a significant number of victims

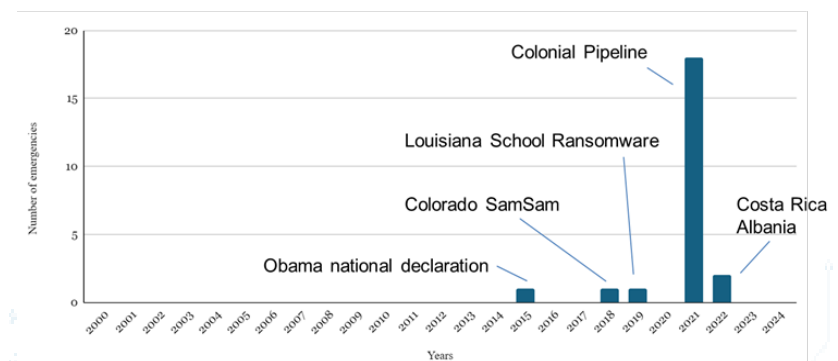
(Source: The Economist Newspaper Limited. "Unexpectedly, the Cost of Big Cyber-Attacks Is Falling." The Economist, <https://www.economist.com/graphic-detail/2024/05/17/unexpectedly-the-cost-of-big-cyber-attacks-is-falling>, 17 May 2024.)

Negative Credit Events per Year Due to Cyber Incidents, per Moody's



(Source: Moody's Investors Service, Inc.)

States of Emergency Declared After Cyber Incidents National or State Level



(Source: Healey, J., T. Jain, and S. Dab.)

Impact Indicators (continued)

Ecosystem: Incidents

- Fewer overall incidents
- Fewer catastrophic incidents and events
- Fewer one-on-multitude and cascading incidents

Ecosystem: Costs

- Reduced monetary losses
- Reduced economic impact
- Fewer direct and indirect deaths
- Fewer national-security-relevant incidents

Longer “mean time between catastrophes”

(less frequent NotPetya, Shields Up, or log4j...and not every holiday, thanks)

Average number of victims per incident should approach one

(more like Sony, fewer like SolarWinds or NotPetya)

Very Initial Assessment: Vulnerability Illustration Purposes

Not scientific, just
an initial, basic
assessment of
limited information

Fewer Overall Incidents

Fewer Catastrophic
Incidents and Events

Fewer one-on-multiple
and cascading incidents

Fewer Direct and
Indirect Deaths

Fewer National Security
Relevant Events

Reduced Economic
Impact

Reduced Monetary
Losses

Defenders Are Winning

Uncertain or Balanced

Adversaries are Winning



NEXT STEPS AND CONCLUSIONS

Goals of This Project

- **Phase 1**
 - Develop initial framework of “is defense winning” with propositions and examples
- **Phase 2**
 - Create a more complete catalog of indicators across threat, vulnerability, and impact
 - Encourage cybersecurity companies (and others with data) to report defensibility-relevant statistics in time series, mapped to the catalog
 - Drive improved analyses: White House posture reports to Congress, systemic risk analysis, reinsurance
- **Phase 3**
 - Evolve from indicators to actions, with targets (e.g., “reduce global mean time to detect [MTTD]” to a specific goal like “reduce global MTTD from days or weeks to less than 24 hr”)
 - Produce an annual report on progress, based on data from others

Goals of This Project (continued)

- **Phase 1**

- Develop initial framework of “is defense winning” with propositions and examples

- **Phase 2**

- Create a more complete catalog of indicators across threat, vulnerability, and impact
- Encourage cybersecurity companies (and others with data) to report defensibility-relevant statistics in time series, mapped to the catalog
- Drive improved analyses: White House posture reports to Congress, systemic risk analysis, reinsurance

- **Phase 3**

- Evolve MTTD
- Produce

Some Additional Needed Work

- How can we calculate **mean time between catastrophes** (or similar)?
- May need a **“zero-day Index”**
 - Like the U.S. Consumer Price Index to track costs of similar-but-changing basket of goods over time

reduce global

Goals of This Project (continued)

- **Phase 1**

- Develop initial framework of “is defense winning” with propositions and examples

- **Phase 2**

- Create a more complete catalog of indicators across threat, vulnerability, and impact
- Encourage cybersecurity companies (and others with data) to report defensibility-relevant statistics in time-series, mapped to the catalog
- Drive improved analyses: White House posture reports to Congress, systemic risk analysis, reinsurance

- **Phase 3**

- Evolve from indicators to actions, with targets (e.g., “reduce global MTTD” to a specific goal like “reduce global MTTD from days or weeks to less than 24 hr”)
- Produce an annual report on progress, based on data from others



Thank you!

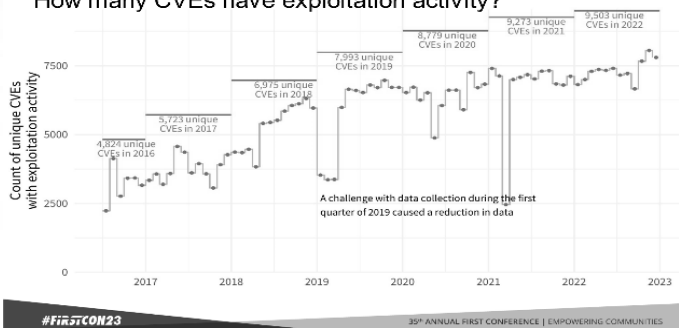




BACKUP SLIDES

Other Indicators for Threat

How many CVEs have exploitation activity?

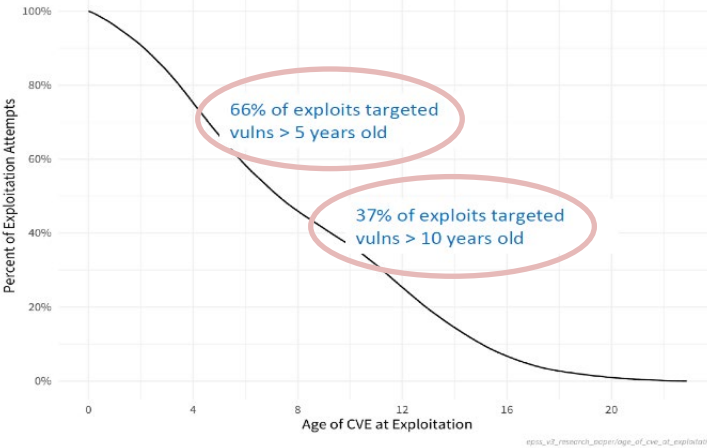


(Source: Romanosky, S. "Presentation." FIRSTCON 23, June 2023.)

Never before seen exploited

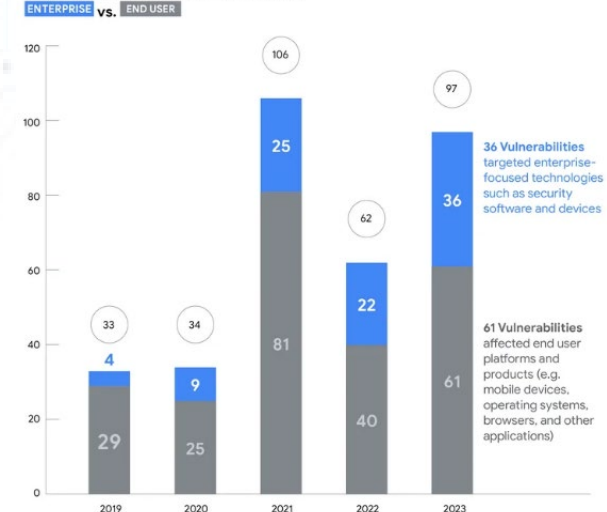


#FIRSTCON23 35th ANNUAL FIRST CONFERENCE | EMPOWERING COMMUNITIES



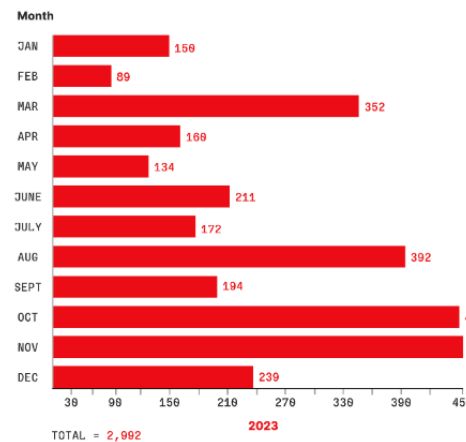
(Source: Romanosky, S. "Exploit Prediction Scoring System." https://www.first.org/epss/data_stats, 7 December 2022.)

Zero-Days Exploited In-The-Wild by Year



(Source: Mandiant and Threat Analysis Group. "We're All in This Together: A Year in Review of Zero-Days Exploited in-the-Wild in 2023." Google, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf, March 2024.)

Access Broker Advertisements by Month



(Source: CrowdStrike. CrowdStrike 2024 Global Threat Report. [CrowdStrike 2024 Global Threat Report | CrowdStrike](https://www.crowdstrike.com/crowdstrike-2024-global-threat-report/), 2024.)



- CrowdStrike: Average breakout time for interactive eCrime intrusion activity decreased from 84 min in 2022 to 62 min in 2023

- Vendors like CrowdStrike indicate steady increases in zero-day prices (e.g. iPhone operating system full-chain, zero click from \$3M in 2019 to \$5M in 2024)
- Need a zero-day price index based on prices for a basket of similar vulnerabilities over time, like the U.S. Consumer Price Index

- A [2020 report](#) found that “91% of the codebases examined contained components that were more than four years out of date or had no development activity in the last two years.” There are still many running versions of ancient operating systems like [Windows NT](#) and [XP](#), including in critical infrastructure.