IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 5, Ser. 6 (Sept. – Oct. 2025), PP 49-55
www.iosrjournals.org

Cleaning Up IoT Security: Using Real-World Threat Data and Internet Measurements

Vishnu Dutt
Department of Computer Science
Hindu College of Pharmacy, Sonipat

Arvind Singh
Department of Computer Science
I K Gujral Punjab Technical University, Jalandhar

Abstract
The rapid spread of Internet of Things (IoT) devices has turned into this huge, kinda messy and largely insecure attack surface, and it feels like adversaries are now using it at scale, pretty openly. By the end of 2023 there were more than 16.6 billion connected IoT devices logged worldwide, and that number is moving past 18.5 billion by 2024, so yeah, the stakes for getting IoT security right, have never been bigger. Still, a lot of the devices that are already deployed keep a really weak security posture—stuck with default credentials, old firmware that never gets updated, and networks that aren't properly segmented. This piece looks at how real world threat evidence, pulled from internet measurement tools like Shodan and Censys, darknet traffic review, honeypot setups, and public vulnerability repositories, can be used to sort of understand, chart, and then improve IoT security in a more systematic way. It follows how the threat picture evolved, from the more famous Mirai botnet incidents back in 2016, toward the more capable botnets we're seeing in 2024, and it digs into what big internet scanning actually shows about exposure rhythms across nations and device types. It also evaluates the newer regulatory efforts, including NIST SP 800-213 and the EU Cyber Resilience Act, meant to force security-by-design, not just "best efforts."Overall, the article makes a strong point that anchoring IoT security changes in empirical measurement isn't optional anymore; it's the only believable way forward.

Keywords: *internet measurements, botnet, Shodan, Cyber Resilience Act, IoT security, threat intelligence, vulnerability scanning*

I. Introduction

Picture this: you drop in a new IP camera in your living room. You plug it in , connect it to Wi-Fi, and then you move on. What you probably dont know is that within minutes, after that camera comes online, it already gets its first connection probe from some automated scanner, sitting somewhere on the internet. If it's still using default credentials and it has an unpatched firmware build, then it can get compromised before the end of the day.

This isn't paranoia. AV-TEST's honeypot systems, which mimic fragile IoT devices, logged more than 70 million attacks in 2023 by itself — and the early weeks of 2024 basically showed no easing at all, with around 8 million attacks reported in just the first four weeks of January (AV-TEST, as cited in Dotmagazine, 2024). The things being targeted are not exotic. They're routers, cameras, smart plugs, and digital video recorders, you know, the usual bricks of connected homes and workspaces.

What makes IoT security weirdly hard isn't only the device count. It's also that these gadgets often run for years without updates, they ship with factory default passwords surprisingly often, and they live right on the boundary between physical routines and digital control. That position means a compromise can become physically risky, not just "someone hacked my account." The 2021 incident at a water treatment plant in Oldsmar, Florida — where an attacker remotely tweaked chemical levels through insecure remote access software — proved the danger isn't theoretical.

But heres the deal: the security community has got increasingly powerful tools, to figure out where the weak spots actually live. Stuff like internet wide scanning platforms, darknet traffic analysis, global honeypot networks, and public vulnerability databases are generating a huge amount of real world data. That data shows what devices are out there in the open, how attackers are moving around, and which threat actors are really going after which weaknesses. So the big question is, whether the research community, device manufacturers, and policymakers are making use of that information enough, to close the gap.

II. The IoT Threat Landscape: Scale, Scope, and Severity

2.1 Growth of the Connected Device Ecosystem

The whole scale of the IoT ecosystem is genuinely staggering and it really comes with important security implications. As IoT Analytics notes, connected IoT devices sat at 16.6 billion at the end of 2023, that's up 15% compared with the year before, and by the end of 2024 the count climbed to 18.5 billion. That works out to a 12% year-over-year increase (IoT Analytics, 2024). If you follow the growth curve it points toward around 39 billion connected devices by 2030.

Now, each of those devices can act as an entry point, and it's not the same situation as with laptops or smartphones. Most IoT devices can't really run conventional security software, and they usually don't get automatic patches either, plus they rarely show security warnings to a person. A lot of them run in a "set it and forget it" style for years and, so the flaws that were there at deployment time, tend to stay there. That means vulnerabilities can remain present and exploitable for a very long time.

Bitdefender's 2024 IoT Security Landscape Report also paints a pretty direct picture. It says home network devices see an average of 10 attacks within each 24 hour period, and Bitdefender's smart home security systems block about 2.5 million threats per day. Which is roughly 1,736 threats each minute (Bitdefender/NETGEAR, 2024). And when you look at where the biggest vulnerability concentrations were in 2023, TV sets showed 34%, smart plugs 18%, digital video recorders 13%, and routers 12%.

2.2 Attack Volume and Trends

The attack trend isn't just going up ,itskinda accelerating. SonicWall's 2025 Cyber Threat Report says IoT malware attacks jumped 124% in 2024, and they blocked more than 17 million attacks aimed at IP cameras alone (SonicWall, 2025). Meanwhile, Verizon's 2024 Data Breach Investigations Report basically concluded that one out of every three breaches now involves an IoT device (Verizon, 2024).

So what's really pushing this surge forward? Mostly it's the ongoing abuse of basic authentication problems. In most situations, attackers aren't using fancy zero-day payloads on IoT systems — they're just scanning around for devices still stuck with default usernames and passwords, and they find plenty. And as IoT botnet research keeps showing, you don't always need high cleverness when everyday carelessness is everywhere.

As shown in Figure 1, the evolution of IoT attack volume from 2016 through 2024 reveals a sharp and accelerating upward trend, with pivotal milestones tied to major botnet emergence events.

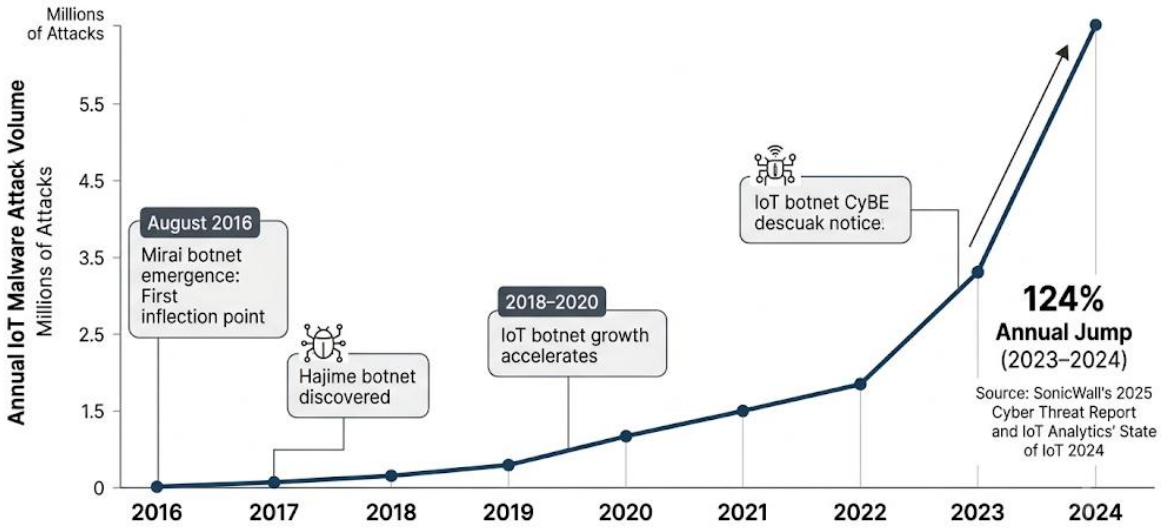

Figure 1: Growth in IoT Malware Attack Volume and Key Botnet Milestones (2016–2024)

This timeline chart show annual IoT malware attack volumes, from 2016 through 2024, using a vertical axis, and on a horizontal time axis it marks a few big botnet milestones. The Mirai botnet's emergence in August 2016 is shown as the first inflection point—after that you see what looks like a steady climb across 2019–2022, and then it gets sharply higher from 2023 to 2024. In that later period, the chart notes a 124% annual jump in IoT malware attacks, pulled from SonicWall's 2025 Cyber Threat Report, plus data tied to IoT Analytics' State of IoT 2024.

The main takeaway is kinda simple: the escalation of attacks seems to line up with device proliferation, like closely. That suggests the expansion of the attack surface is not just happening in the background, but rather it's directly rewarding attacker investment into IoT targeting.

III. Internet Measurements as a Security Tool

3.1 What Internet Scanning Platforms Tell Us

Over the past decade, one of the more significant moves in IoT security research has been the appearance of internet wide scanning platforms. Things like Shodan, Censys, ZoomEye and FOFA keep scanning the public IPv4 space, sort of mapping what services are visible on which ports, what the device banners actually say, what protocols are in play, and sometimes even what firmware or software builds are running. It's really useful intelligence, not only for attackers, but also for defenders, researchers, and people in policy roles that are trying to grasp what the internet looks like in practice.

Censys, for instance, has noted that nearly 7 out of 10 HTTP services sit on non-standard ports, and because HTTP makes up 88% of all internet services, this translates to more than 60% of internet services living on ports that "normal" vulnerability scanners—usually checking only 200 to 300 ports—would never bother to look at (Censys, 2023). It's a pretty uncomfortable structural picture: the attack surface most organizations believe they are surveilling is only a slice of what's genuinely exposed.

Shodan an Censys sort of differ in how they scan in real ways that actually matter. In Greynoise's 2024 benchmarking review they tracked 10 major scanning services across 24 sensor nodes spread across five independent systems and eight geographies, and yeah the results show Censys tends to cover more ports overall, while ShadowServer leans harder toward finding weaknesses, not just open doors. Meanwhile Shodan showed a more periodic, measured scanning style, with clusters of touches rather than a steady flow of packets (Greynoise, 2024). These behavior shifts matter, because security researchers need to pick a tool that matches what they're trying to measure, you know, for their own aims.

3.2 What Scan Data Reveals About IoT Exposure

Mean counts of risky ports per host varied from 0.4 up to 1.0 depending on the country, so it was not flat. Also the results suggested that service-level indicators were more predictive of high risk exposure patterns than simply belonging to a specific geography, in other words what a device is actually running appears to matter more than where it sits.For a moment, it's worth dwelling on TR-069. This protocol is commonly used by internet service providers to manage customer routers at a distance, but it has also shown up as an attack channel in multiple large scale campaigns, mainly because across many ISPs the admin interfaces were not hardened properly. Shodan records keep turning up thousands of devices with this same port open globally, including in places where consumer router security rules are basically absent or not clearly enforced.

There's also a broader line of work on IoT weaknesses using Shodan and Censys that was published in the International Journal of Advanced Research. That paper reported the tools were effective at spotting flaws across "ubiquitous computing" devices, and it offered evidence that weaknesses that are visible at the network layer are systematically findable through passive measurement (IJAR, 2022).

3.3 Darknet Traffic and Honeypot Intelligence

Internet measurement isn't only about sweeping devices or enumerating endpoints, it's also about paying attention to what's already going on. Darknets are basically parts of the routed IP address space where there are no real, sanctioned services; so any traffic that shows up there is, by definition, unsolicited and it is typically malicious, or at the very least it looks anomalous. If you monitor darknet traffic, researchers can kind of see the internet's background radiation— automated scanners, probes coming from compromised machines, and botnet chatter — all this without having to touch real user traffic too much.

In the Journal of Edge Computing's 2024 honeypot framework work, the authors argue that adaptive honeypots, which are decoy systems meant to resemble fragile IoT devices, are getting more and more useful for catching genuine attacker behavior, checking detection models, and keeping tabs on the way the threat landscape keeps shifting (Acnsci, 2024). Put those deployments at scale across multiple places and regions, and the setup can spot new or rising attack campaigns, fresh malware families, and even changes in attacker tactics weeks ahead of when they finally land in incident reports.

Meanwhile, the Annual Computer Security Applications Conference's 2022 paper on hybrid IoT/OT honeypots, built around the RIoTPot framework, put the honeypots onto the public internet for about three months and recorded what attackers did against both IoT and operational technology protocol traffic. They reported sharp swings in attack intensity, with some windows showing wildly higher activity, suggesting coordinated campaign bursts rather than a steady, always-on background sweep (ACSAC, 2022).

IV. The Botnet Problem: From Mirai to the Modern Era

4.1 Mirai and Its Legacy

If there is one moment that kinda crystallized the whole IoT security headache for people beyond the technical bubble, it was the Mirai botnet attacks back in 2016. Mirai— a Japanese word meaning "future" — was malware aimed at Linux-based IoT gear, especially IP cameras and home routers, and it did this by leaning on their default or kinda weak credentials. It ended up infecting something like over 600,000 devices between August 2016 and February 2017, and later it was tied to more than 15,000 DDoS attacks (MDPI Sensors, 2024).

Then there was the assault on security journalist Brian Krebs' website on September 20, 2016. That one reportedly hit a peak of more than 620 Gbps, and at the time it was described as the largest DDoS event on record. (CISA, 2016). Not too long after, OVH, one of Europe's bigger web hosting players, got hit with an attack above 1 Tbps. But the most disruptive episode showed up on October 21, 2016, when Mirai took Dyn offline. Dyn was a key DNS infrastructure provider, so blocking access to over 1,200 websites including Twitter, Netflix, Reddit and GitHub for almost an entire day. (ScienceDirect, 2020)

What really made Mirai feel especially frightening wasnt some advanced, high level technique. It was the opposite, the low sophistication, the kinda blunt approach of it. Mirai basically swept, the internet for devices that still had factory-default login details from a fixed, hardcoded list of username-password combinations. That was it. And once the source code got released publicly in October 2016, it spawned a bunch of variations, and permanently shifted the threat landscape, in a way that people could not ignore.

4.2 The Botnet Ecosystem in 2023–2024

Mirai never really went away. It kinda evolved, in the background. By 2024, fresh variants kept weaponizing the very same foundational weak spots— default passwords, unpatched firmware, open administrative ports— things Mirai was leaning on like eight years earlier. And in 2024, attackers were still very much riding the wave of CVE-2023-1389, a command-injection flaw in TP-Link routers, and it hit more than 21% of small and medium-sized businesses (GAP, 2024).

The "Matrix" campaign in 2024 also followed a similar trail, it leaned on default or even hardcoded credentials, to stitch together a brand new botnet scaffolding. Meanwhile, the MDPI Sensors systematic review (2024) on IoT botnet studies noted that peer-to-peer command-and-control setups have been replacing the older centralized designs. That shift makes today's botnets, more durable— and honestly way harder to knock out using classic takedown playbooks.

And the published honeypot findings basically back up all of that signal. Attackers aren't exactly pouring effort into brand new tricks. They don't really need to. The core attack patterns, first logged about a decade back, still work because the underlying device vulnerabilities are still sitting there, unchanged. Put another way, this is one of the harsher verdicts on how the IoT sector handles security— same weak points, same login details, same neglected firmware, again and again, year after year.

V. Vulnerability Databases and Their Limitations

5.1 The Role of CVEs and the NVD

Figuring out what vulnerabilities show up in IoT devices, and how dangerous they really are, kind of depends on a dependable tracking system. The National Vulnerability Database (NVD) run by NIST, has been like the core global reference point for this whole thing. It logs vulnerabilities through the Common Vulnerabilities and Exposures (CVE) standard, then attaches severity numbers plus product identifiers so security teams can line up known weaknesses with what they actually run in production (NIST, 2021).

The NVD today holds more than 150,000 CVE entries, and they're compiled from over 200 data sources (Fortinet, 2024). In theory, this looks very useful for IoT defense — like, if a manufacturer wants to confirm whether the device's underlying open-source components have already been reported, they can check the NVD and verify it.

But in real life, things don't stay so smooth. The whole workflow is under heavy pressure. CVE submissions jumped 32% in 2024 by itself, and then they shot up 263% between 2020 and 2025. NIST also examined almost 42,000 vulnerabilities in 2025, about 45% higher than the year before, yet it still couldn't catch up with the inflow. Starting in 2024, the NVD started building up a big backlog of unenriched CVEs. Those are entries that are already sitting in the database, but they are missing the severity scores and the product mapping that most security tools need, to act on them.

5.2 Implications for IoT Security

This backlog problem matters especially for IoT, ok. Consumer IoT devices, unlike the software used by the federal government or critical infrastructure, do not get priority enrichment under NIST's new triage criteria. So newly disclosed vulnerabilities in smart home cameras, routers, and connected appliances can end up

sitting in the NVD as unenriched shells for extended periods, and then well… no severity score, no product list, and no clear remediation guidance at all.

For IoT manufacturers attempting to track vulnerabilities in their own devices, and for users who are trying to figure out if updates are actually needed, this really becomes a noticeable gap. Consumer-facing security tools that depend on NVD data can turn out less reliable once that data becomes more incomplete.
The table below summarizes key internet measurement and vulnerability data sources currently used in IoT security research, their primary data types, and their key limitations.

Table 1: Comparison of Key Data Sources Used in IoT Security Measurement Research

Data Source	Type of Data Provided	Primary Strength	Key Limitation	Source
Censys	HTTP/HTTPS services, TLS certificates, non-standard ports	Strong port coverage breadth; frequent scans	Commercial costs for full API access; excludes some protocols	Censys, 2023
Darknet / Network Telescope	Unsolicited inbound traffic patterns	Captures background internet noise; reveals attack campaigns	No application-layer content; requires significant infrastructure	ACSAC, 2022
Honeypots	Actual attacker behavior, malware samples, credential attempts	Captures real attack sequences; validates detection models	Limited scale; requires careful deployment to avoid attribution errors	Journal of Edge Computing, 2024
AV-TEST Honeypot Systems	Attack volume against simulated IoT targets	High-volume longitudinal data (70M+ events in 2023)	Simulated devices may not reflect all real-world deployment scenarios	Dotmagazine, 2024

VI. Regulatory and Standards Frameworks

6.1 NIST SP 800-213 and the U.S. Approach

Yeah, so, recognizing that market incentives alone haven't really pushed the IoT industry toward secure practice, regulators in both sides of the Atlantic have started to require minimum security baselines. In the United States, the IoT Cybersecurity Improvement Act of 2020 — which is often described as the first federal law meant to regulate IoT device security — asked NIST to put together guidance so federal agencies can use IoT devices in a more controlled way. That work later turned into NIST SP 800-213, released in November 2021, and it basically offers a framework for how to find, and then set, IoT device cybersecurity requirements within the federal Risk Management Framework (NIST, 2021).

SP 800-213 then gets backed up by SP 800-213A, sort of like a catalog with both technical and non-technical cybersecurity controls. It covers device capabilities and also the supporting actions around them. These documents have had impact outside federal agencies too, because they often end up being used as reference frameworks for procurement decisions, plus they feed into industry standards development. On top of that, NIST published NISTIR 8425 in September 2022, which established the IoT Core Baseline for consumer products. Then NISTIR 8425A came out in September 2024, and it zeroes in on consumer router security, (and yes, it's one of those device categories that gets targeted again and again) (NIST, 2022; NIST, 2024).

In July 2023, the White House launched the U.S. Cyber Trust Mark, which is a voluntary cybersecurity labeling program for smart devices. The whole goal is to help consumers quickly spot products that meet defined security baselines (NIST, 2023). The program, in other words, leans into a market-signal idea: it's not a mandatory requirement, more like a credentialing system. So, security-minded consumers have a clearer way to recognize what counts as safer products.

6.2 The EU Cyber Resilience Act

The European approach is kinda more prescriptive. The EU Cyber Resilience Act (CRA), which was proposed by the European Commission on September 15, 2022, got formally adopted by the EU Council on October 10, 2024, after some political agreement in December 2023 and formal Parliament approval in March 2024. (Wikipedia, 2024; European Cyber Resilience Act, 2024). So the CRA sets compulsory cybersecurity needs for all products that include digital elements, meaning hardware and software, that end up placed on the EU market.

Manufacturers now have a December 2027 deadline to comply or else they risk loosing market access. The regulation also says manufacturers have to own the product security across the whole device lifecycle, not only at the point of sale, which is a pretty big change from the usual practice before. And it further requires incident reporting, clear vulnerability disclosure rules, plus defined security update periods.

This CRA does not come out of nowhere, it is preceded by the NIS2 Directive of 2022 and the Cybersecurity Act of 2019, and it builds on a regulatory stack the EU has been shaping for years. In tandem, these instruments want connected devices sold in Europe to start with fewer vulnerabilities, and stay secure over time, not just when they are shipped,

Meanwhile the UK runs something parallel with its Product Security and Telecommunications Infrastructure (PSTI) Act, which came into effect in 2024. It bans universal default passwords, asks for vulnerability disclosure policies, and also pushes transparency about security update timelines- and these are enforced by a dedicated regulator (M3AAWG, 2025).

As shown in Figure 2, the regulatory timeline from 2020 through 2024 reveals a rapid convergence of national and international IoT security mandates across multiple jurisdictions.

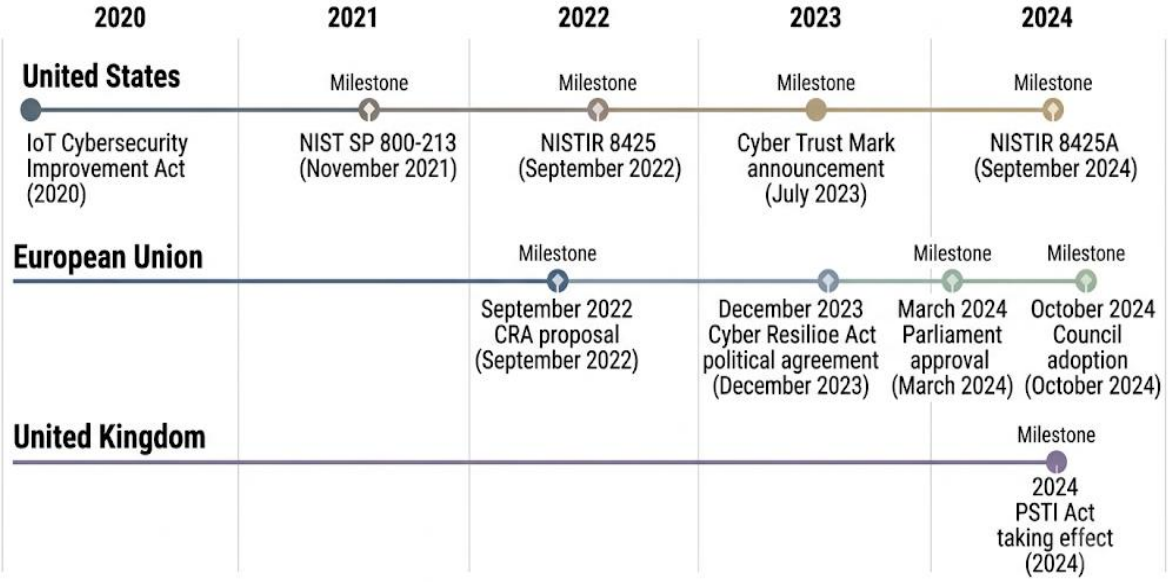

Figure 2: Timeline of Major IoT Security Regulatory Developments (2020–2024)

This horizontal timeline diagram kind of runs from 2020 into 2024, and it basically lays out the big regulatory moments across three different jurisdiction lanes. First lane is the United States (top), second is the European Union (middle), and the third is the United Kingdom (bottom). In the U.S. Lane you can spot the IoT Cybersecurity Improvement Act around 2020, then NIST SP 800-213 in November 2021, NISTIR 8425 in September 2022. After that it mentions the Cyber Trust Mark announcement in July 2023, and later NISTIR 8425A shows up again in September 2024. For the EU lane it lists the CRA proposal in September 2022, then a political agreement in December 2023, then Parliament approval comes in March 2024, and finally the Council adoption lands in October 2024. For the UK lane it just says the PSTI Act takes effect in 2024. The main takeaway, or the key insight really, is that regulatory momentum speeds up from 2022 through 2024, like several frameworks moving at the same time. The background info is taken from NIST, European Parliament, and M3AAWG (2025).

VII. Conclusion

IoT security is not like, an unsolvable thing. The measurement tools exist, or at least they do most of the time. The threat data is getting more rich and more actionable too. Also the regulatory frameworks are being built, slowly but still. What seems to be needed now is just the will to mash all these elements together into some kind of coherent sustained improvement effort.

The most obvious lesson from the Mirai era, is that attackers do not have to be very sophisticated, if the devices are insecure by default. Eight years after Mirai, default credentials and unpatched firmware are still the main attack routes. You can see this in scan data, you can confirm it from honeypot captures, and you can watch it being used daily in real campaigns. The measurement data has been basically saying the same story for years; whats changed is that regulators are finally listening, more or less.

The EU Cyber Resilience Act pushes lifecycle security, the UK PSTI Act bans default passwords, and NIST's evolving guidance for consumer IoT is real progress. But enforcement won't happen just by vibes. It needs ongoing empirical measurement. That means scan based assessments of compliance, honeypot monitoring for how attacks evolve, and keeping vulnerability databases in good shape—robust enough to track IoT specific weaknesses at scale without dropping the ball. The NIST NVD backlog is kind of a cautionary tale here: infrastructure that was "okay" for a world with a few thousand annual CVEs is not enough once you are in a world producing tens of thousands, many of them affecting billions of IoT endpoints.

So the forward path is basically better data, better standards, and better enforcement— in that order, not some other order. The first ingredient is becoming available. The second is already being assembled, at least parts of it. The third is where the real work sits, and it's not glamorous.

References

[1]. AV-TEST Institute, & Clausing, J. (2024). *The Cyber Resilience Act and its impact on security in the IoT*. Dotmagazine. https://www.dotmagazine.online/issues/building-trust-in-the-digital-world/the-cyber-resilience-act-iot-security

[2]. Bitdefender, & NETGEAR. (2024). *The 2024 IoT security landscape report*. NETGEAR. https://www.netgear.com/hub/network/2024-iot-threat-report/

[3]. Censys. (2023). *Raising the bar on internet coverage: Predictive scanning takes the Censys internet map to the next level*. Censys Blog. https://censys.com/blog/raising-the-bar-on-internet-coverage-predictive-scanning-takes-the-censys-internet-map-to-the-next-level/

[4]. Cybersecurity and Infrastructure Security Agency (CISA). (2016, October 14). *Heightened DDoS threat posed by Mirai and other botnets*. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

[5]. European Commission. (2022, September 15). *Proposal for a regulation on cybersecurity requirements for products with digital elements (Cyber Resilience Act)*. European Commission. https://www.european-cyber-resilience-act.com/

[6]. European Parliament. (2024, March 12). *European Parliament legislative resolution on the proposal for the Cyber Resilience Act (TA-9-2024-0130)*. European Parliament. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html

[7]. Fortinet. (2024). *What is the National Vulnerability Database (NVD)?* Fortinet Cyberglossary. https://www.fortinet.com/resources/cyberglossary/national-vulnerability-database-nvd

[8]. Greynoise Intelligence. (2024, December). *Checking it twice: Profiling benign internet scanners — 2024 edition*. Greynoise Blog. https://www.greynoise.io/blog/checking-it-twice-profiling-benign-internet-scanners----2024-edition

[9]. International Journal of Advanced Research (IJAR). (2022). *Study of vulnerabilities in IoT environments using Shodan and Censys tools*. IJAR. https://www.journalijar.com/article/43052/study-of-vulnerabilities-in-iot-environments-using-shodan-and-censys-tools/

[10]. IoT Analytics. (2024). *State of IoT summer 2024: Number of connected IoT devices growing 13% to 18.8 billion globally*. IoT Analytics Research. https://iot-analytics.com/number-connected-iot-devices/

[11]. M3AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group). (2025). *Global momentum builds toward secure IoT ecosystems*. M3AAWG Blog. https://www.m3aawg.org/blog/GlobalMomentumBuildsTowardSecureIoTEcosystems

[12]. Mohanta, A., Reddy, K. H. K., & Bhoi, A. K. (2022). *Interaction matters: A comprehensive analysis and a dataset of hybrid IoT/OT honeypots*. Proceedings of the Annual Computer Security Applications Conference (ACSAC '22). ACM. https://dl.acm.org/doi/fullHtml/10.1145/3564625.3564645

[13]. National Institute of Standards and Technology (NIST). (2021, November). *SP 800-213: IoT device cybersecurity guidance for the federal government*. U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/213/final

[14]. National Institute of Standards and Technology (NIST). (2022, September). *NISTIR 8425: Profile of the IoT core baseline for consumer IoT products*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8425

[15]. Osei-Bonsu, A., Asante, M., & Kusi, G. (2024). *Systematic literature review of IoT botnet DDoS attacks and evaluation of detection techniques*. Sensors, 24(11), 3571. MDPI. https://www.mdpi.com/1424-8220/24/11/3571

[16]. Redwood, O., & Lawrence, J. (2024). *The sweet taste of IoT deception: An adaptive honeypot framework for design and evaluation*. Journal of Edge Computing, 2(1). https://acnsci.org/journal/index.php/jec/article/view/607

[17]. ScienceDirect. (2020). *IoT botnet forensics: A comprehensive digital forensic case study on Mirai botnet servers*. Forensic Science International: Digital Investigation, 33. https://www.sciencedirect.com/science/article/pii/S2666281720300214

[18]. SonicWall. (2025). *2025 cyber threat report*. SonicWall Inc. https://www.sonicwall.com/medialibrary/en/white-paper/2025-sonicwall-cyber-threat-report.pdf

[19]. Verizon. (2024). *2024 data breach investigations report*. Verizon Business. https://www.verizon.com/business/resources/T4e4/reports/2024-dbir-data-breach-investigations-report.pdf