ELTON

CONTINUOUS TESTING · POINT OF VIEW

Continuous cybersecurity testing and vulnerability contextualization

The future of medical device testing. A product that changes every sprint cannot be secured by an engagement that happens once a year. Continuous testing keeps a model of the product, carries test evidence forward, and classifies what is actually reachable. **Hundreds of findings become a few that matter.**

FROM HUNDREDS OF FINDINGS TO A FEW THAT MATTER

Hundreds raw findings from scanners, SBOM feeds and test tools → **Dozens** conditional, gated behind another root cause → **A few** directly exploitable, and these carry the exposure

Direct

Exploitable on its own from a known entry vector. This is the number under regulatory exposure, and it should be a handful at most.

Conditional

Real, but reachable only while another root cause keeps producing the condition it requires. Fix the root and the condition closes.

Weakness

No path on this device today. Ships dismissed with its reasoning attached, and is re-evaluated as the product changes.

> Point-in-time tests call everything a vulnerability because two weeks with a device is not enough time to know what is reachable. That is why third-party vulnerability reports land so hard.

FREQUENT TESTING IS WHAT FDA ASKS FOR

> *"FDA recommends that cybersecurity testing should occur throughout the SPDF. Security testing early in development can ensure that security issues are addressed prior to impacting release timelines... After release, cybersecurity testing should be performed at regular intervals commensurate with the risk (e.g., annually)."*
>
> Section V.C, Cybersecurity Testing

> *"An SPDF encompasses all aspects of a product's lifecycle, including design, development, release, support, and decommission."*
>
> Section V, Secure Product Development Framework
>
> *"Security risk management should be an integrated part of a manufacturer's entire quality management system, addressed throughout the TPLC."*
>
> Section V.A, Security Risk Management

> *"Cybersecurity risks may continue to be identified throughout the device's TPLC. Manufacturers should ensure they have appropriate resources to identify, assess, and mitigate cybersecurity vulnerabilities as they are identified throughout the supported device lifecycle."*
>
> Section V.A.6, TPLC Security Risk Management

> **FDA also asks you to report the clock.** Section V.A.6 recommends tracking and submitting the "Duration from vulnerability identification to when it is updated or patched." A once-a-year engagement is what makes that number bad.
>
> Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions. FDA final guidance, February 2026. Docket FDA-2021-D-1158.

SEVEN DRIVERS

01
Reduce regulatory risk

Vulnerabilities found ad-hoc during development never enter a formal report or a quality document. They are development artifacts and you control the timeline. Continuous discovery drains the backlog before formal testing, so less reaches FDA.

02
Reduce testing cost

When testing keeps pace, the next test is marginal. Traceable test cases and a digital twin of the software let you diff releases, test the change, and evidence that unchanged components need nothing. Legacy consulting restarts every time, with no carry-forward.

03
Ship faster

Testing that covers only the increment closes a milestone in under two days instead of four to six weeks. With continuous SBOM monitoring the report regenerates on demand, outlasting the roughly six month shelf life of a one-time manual test.

04
Dedicated capacity, no lead time

An annual subscription reserves capacity before you need it. Schedules move and the testing is still there: no lead time, no availability check, no expedite or prioritization fee in the week that matters. Consulting capacity goes to whoever booked first, so a slipped code freeze sends you back into a queue.

05
Greater depth over time

A paid engagement maxes out at two to three weeks and re-covers the same surface each time. Researchers and large hospital systems have no such clock, which is why their reports are so damaging. Continuous coverage compounds instead.

06
Cut V&V time

Posture tracking replaces generic remediation guidance with fixes written against the product itself. It finds the single fix with the broadest impact across open findings and models change impact on the twin, so V&V scope shrinks instead of expanding.

07
AI needs a platform

AI compresses discovery to days but produces more output than a human triage pass absorbs. A platform is what determines exploitability, assigns CVSS, and classifies findings against the real attack surface. Subscription models pass that efficiency back as more testing.

THE REMEDIATION GAP

Consulting guidance

```
F-01  SQL injection in device query
        → "You should sanitize input."
F-02  Weak TLS on management port
        → "Perform better encryption."
```

No file, no line, no patch, no verification. Development guesses, then V&V retests everything the guess touched.

The ELTON fix

```
Weakness: TLS negotiation on mgmt port
- ctx = ssl.PROTOCOL_TLS
+ ctx.minimum_version = ssl.TLSVersion.TLSv1_3
```

Verified against the digital twin at runtime, then delivered into Jira or Azure DevOps. V&V scopes to the line that moved.

What to require of a testing partner

- Test case traceability that carries across engagements, not a fresh scope each time
- Fixes written to a file and a line, verified before they reach a developer
- Reserved capacity with no lead time, no queue and no short-notice fee
- A model of the product that shows what changed since the last test
- Reports that regenerate against today's CVE set without a new engagement
- Findings classified as directly exploitable, conditional or weakness, with reasoning
- Transparency on where AI is used and how that efficiency reaches your price

Continuous testing is not a faster version of the old engagement. It is the only model where evidence accumulates instead of being rebuilt every year.

Jason Sinchak, CEO & Co-founder · jsinchak@eltoncyber.com