Continuous Security Testing

claranet | Make modern happen®

Cybersecurity is shifting towards a dynamic, always-on approach to testing

Today, we use more applications than ever before, and we develop and deploy new software faster than ever. When new vulnerabilities arise, within large, complex, and frequently-changing application estates, they can go undiscovered for months, or even years.

Devices, apps, and infrastructure all change constantly. The environment is dynamic, and this expanding attack surface must be monitored.

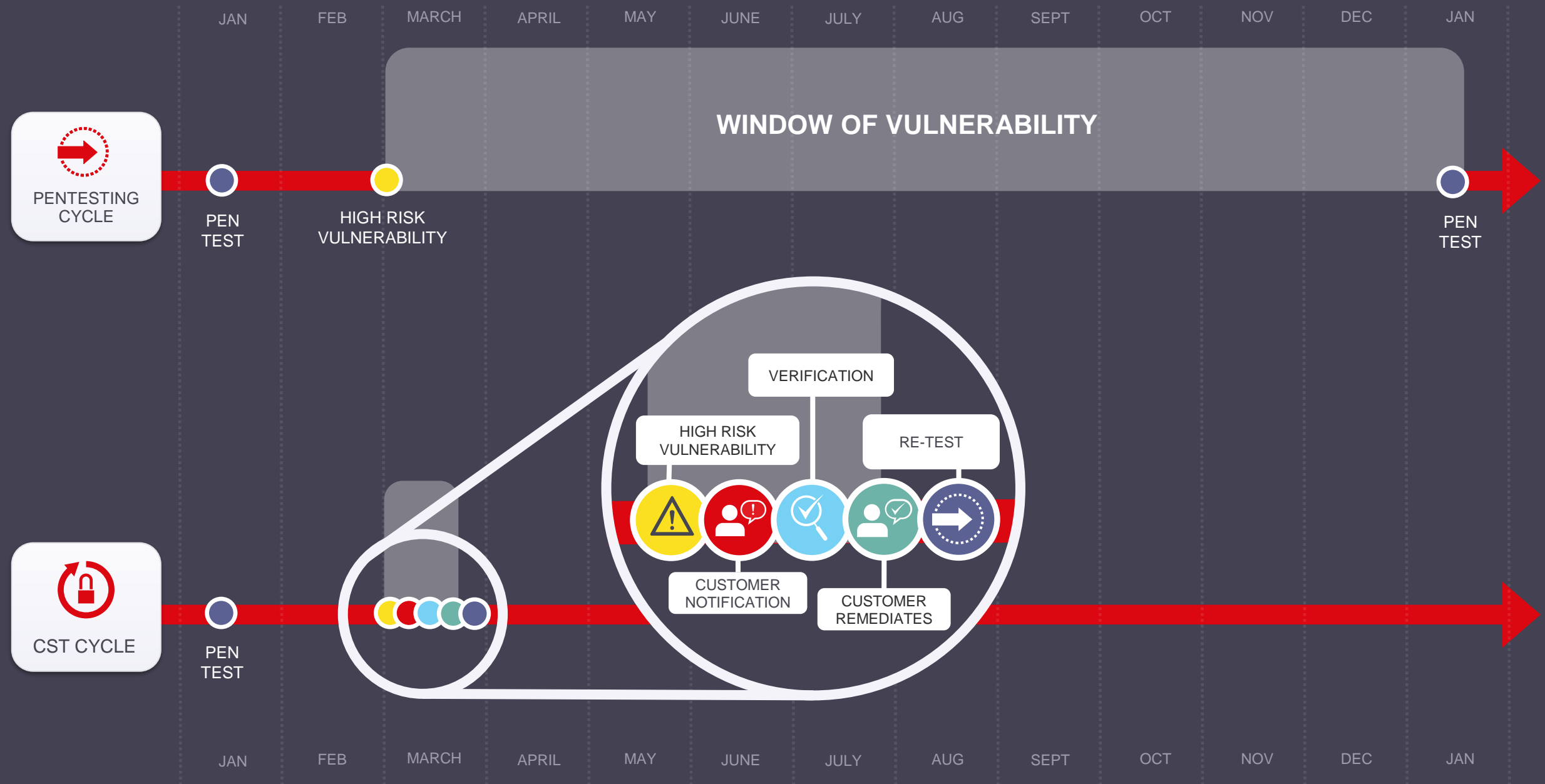Traditional penetration testing uncovers only the vulnerabilities present at a specific point in time and can't monitor an expanding attack surface.
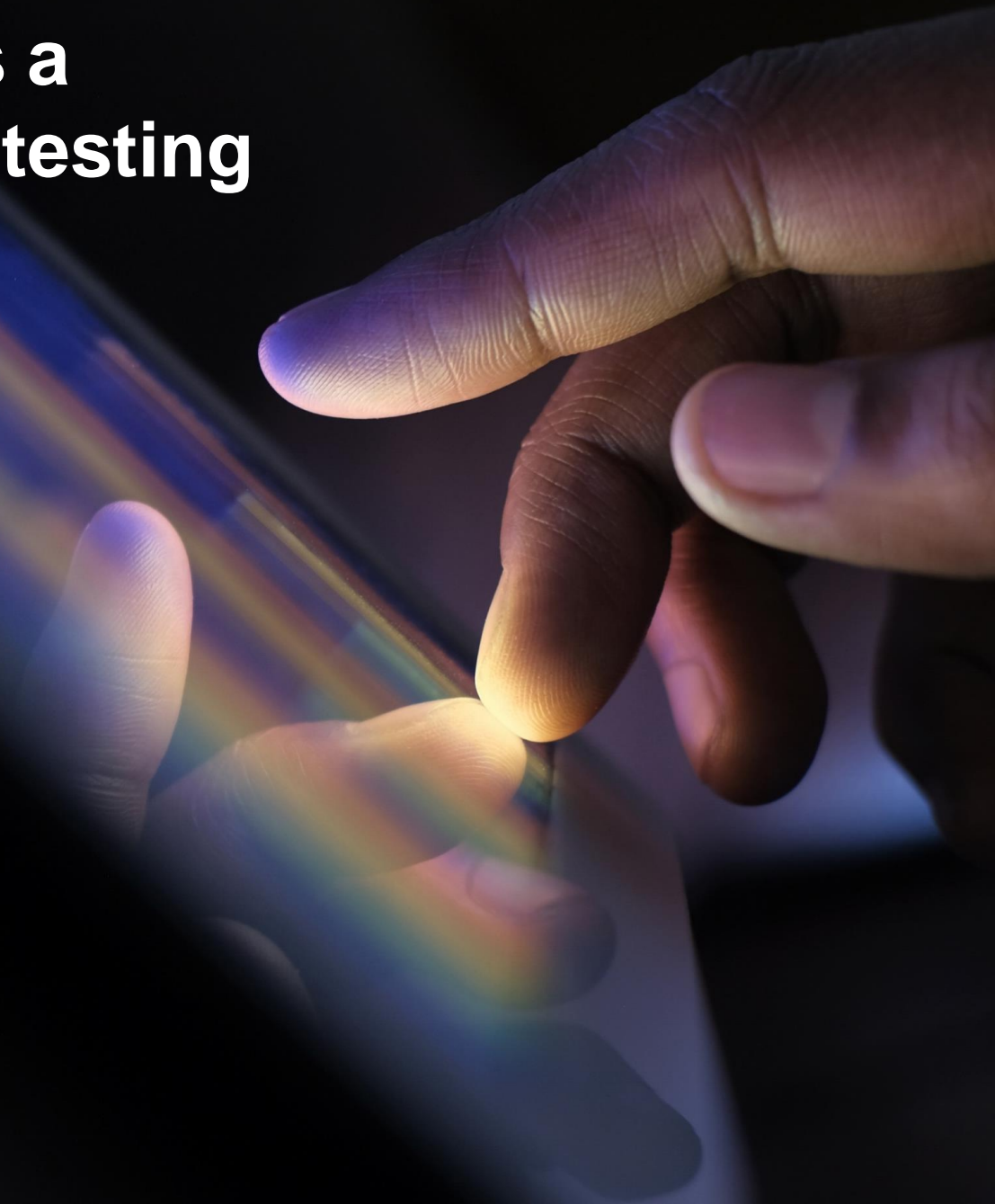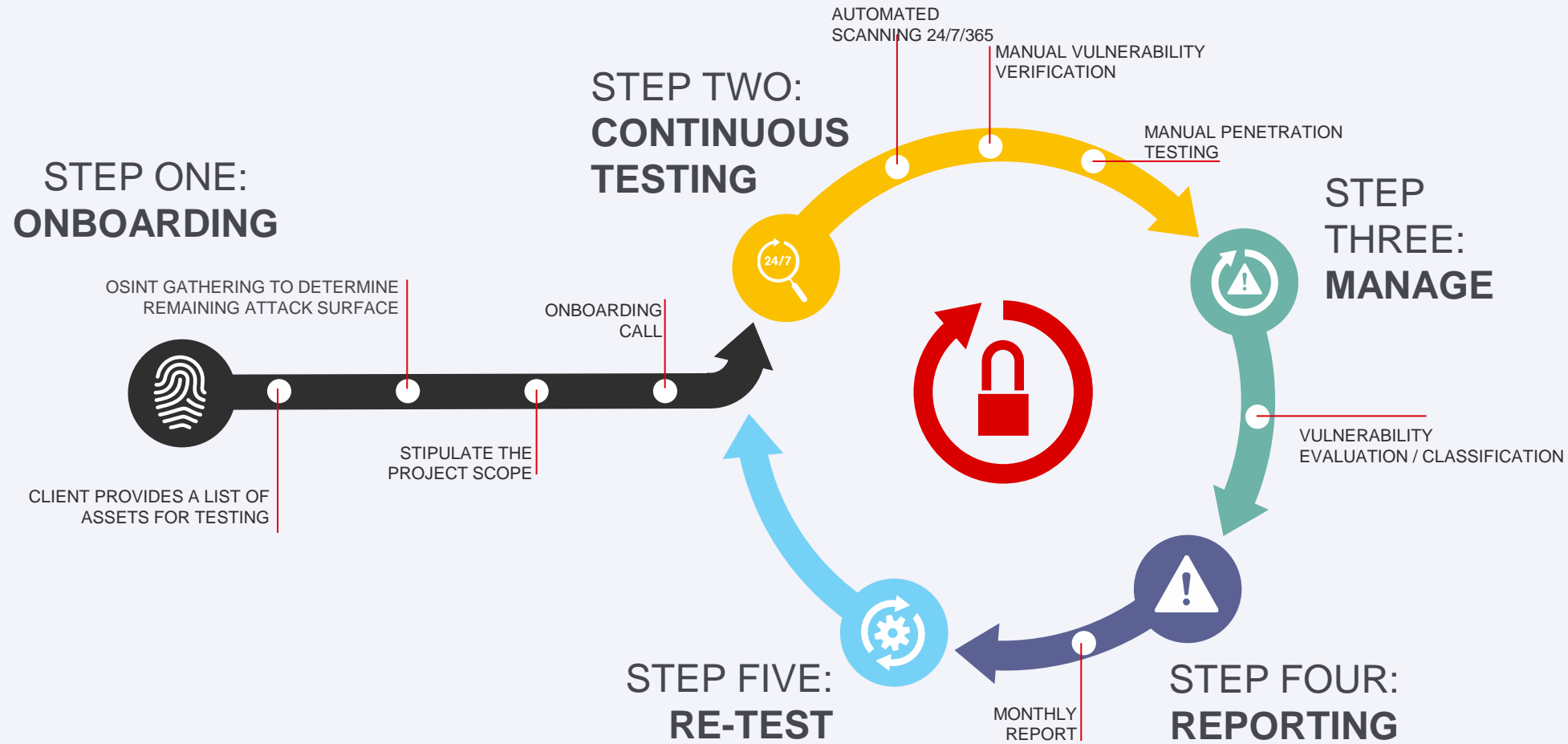
Continuous Security Testing helps you to identify vulnerabilities as they surface so you can patch them quickly and mitigate cyber risks to your organisation on an ongoing basis.

It combines 24/7 automated scanning to reveal vulnerabilities within your web-facing assets, APIs and external infrastructure, with targeted manual penetration testing to verify and evaluate the risk that they present.

Continuously scanning for new vulnerabilities and flagging them when they are discovered reduces the time and effort required to remediate the risks to your organisation.

The Continuous Security Testing cycle

STEP ONE: **ONBOARDING**

OSINT GATHERING TO DETERMINE REMAINING ATTACK SURFACE

ONBOARDING CALL

STIPULATE THE PROJECT SCOPE

CLIENT PROVIDES A LIST OF ASSETS FOR TESTING

STEP TWO: **CONTINUOUS TESTING**

AUTOMATED SCANNING 24/7/365

MANUAL VULNERABILITY VERIFICATION

MANUAL PENETRATION TESTING

24/7

STEP THREE: **MANAGE**

VULNERABILITY EVALUATION / CLASSIFICATION

STEP FOUR: **REPORTING**

MONTHLY REPORT

STEP FIVE: **RE-TEST**

claranet cyber security®

Best of both worlds

Combine the speed of automation with the expertise of a team of penetration testers.

_____

24/7 automated scanning provides broad coverage across your application estate, and targeted manual penetration testing gives you the depth of insight only provided by experts.

We manually verify all the vulnerabilities which have been uncovered and evaluate their risk to your business according to impact and probability of exploitation.

We understand viable attack paths which attackers might take and we analyse attack chains based on combining present vulnerabilities, so you get the full context of how your applications and infrastructure could be compromised.
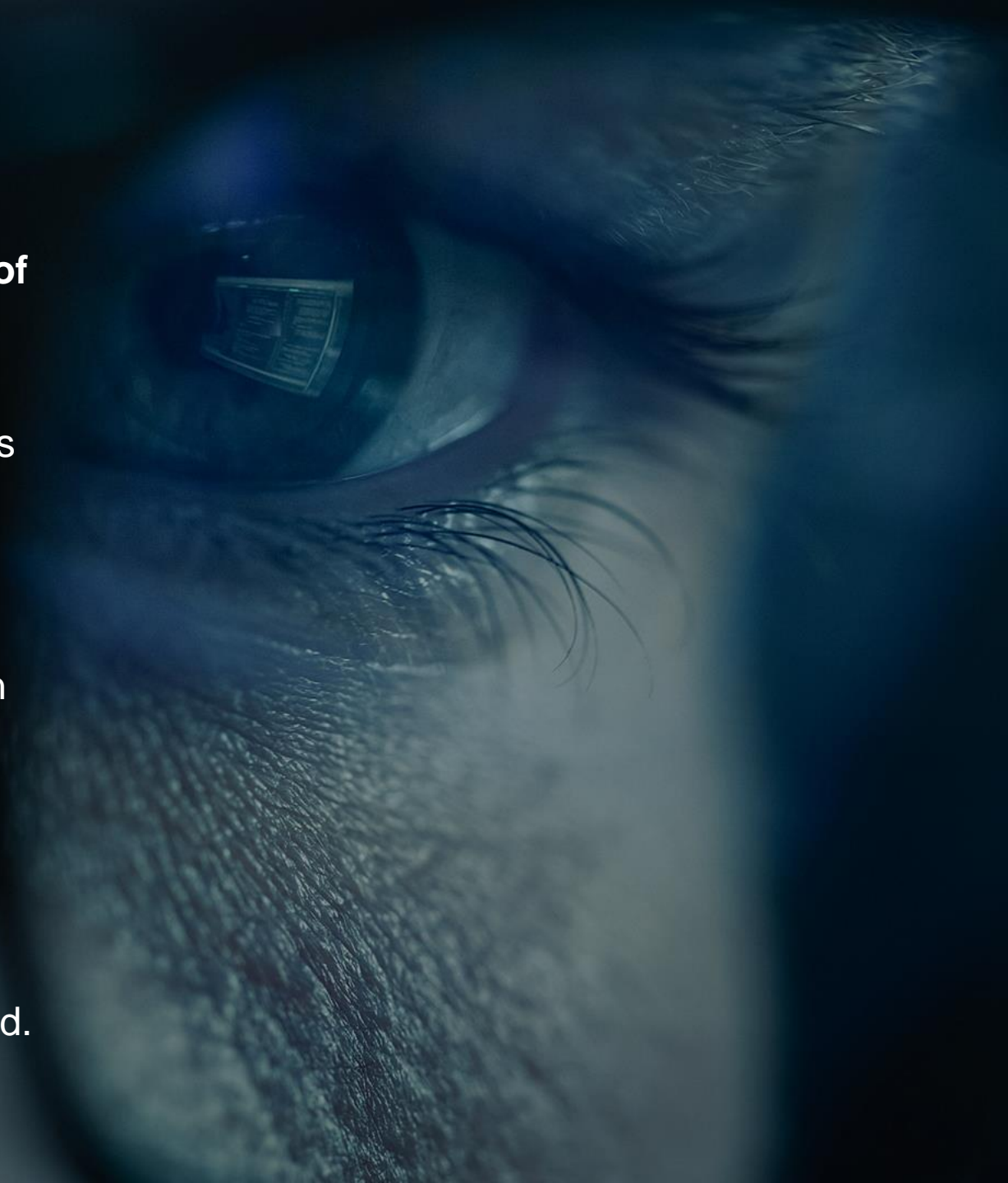
Agile and always-on

Gain a thorough, up-to-date register of vulnerabilities. All in scope assets are constantly checked for vulnerabilities, when change occurs, you'll know if it introduces risk.

Shorten the window of opportunity for attackers. Detect vulnerabilities sooner so you can remediate them faster.

We issue rapid notifications to you whenever high-risk vulnerabilities are discovered during testing, that detail which technologies are affected, how they might be exploited, and what action you can take to remediate the vulnerability.
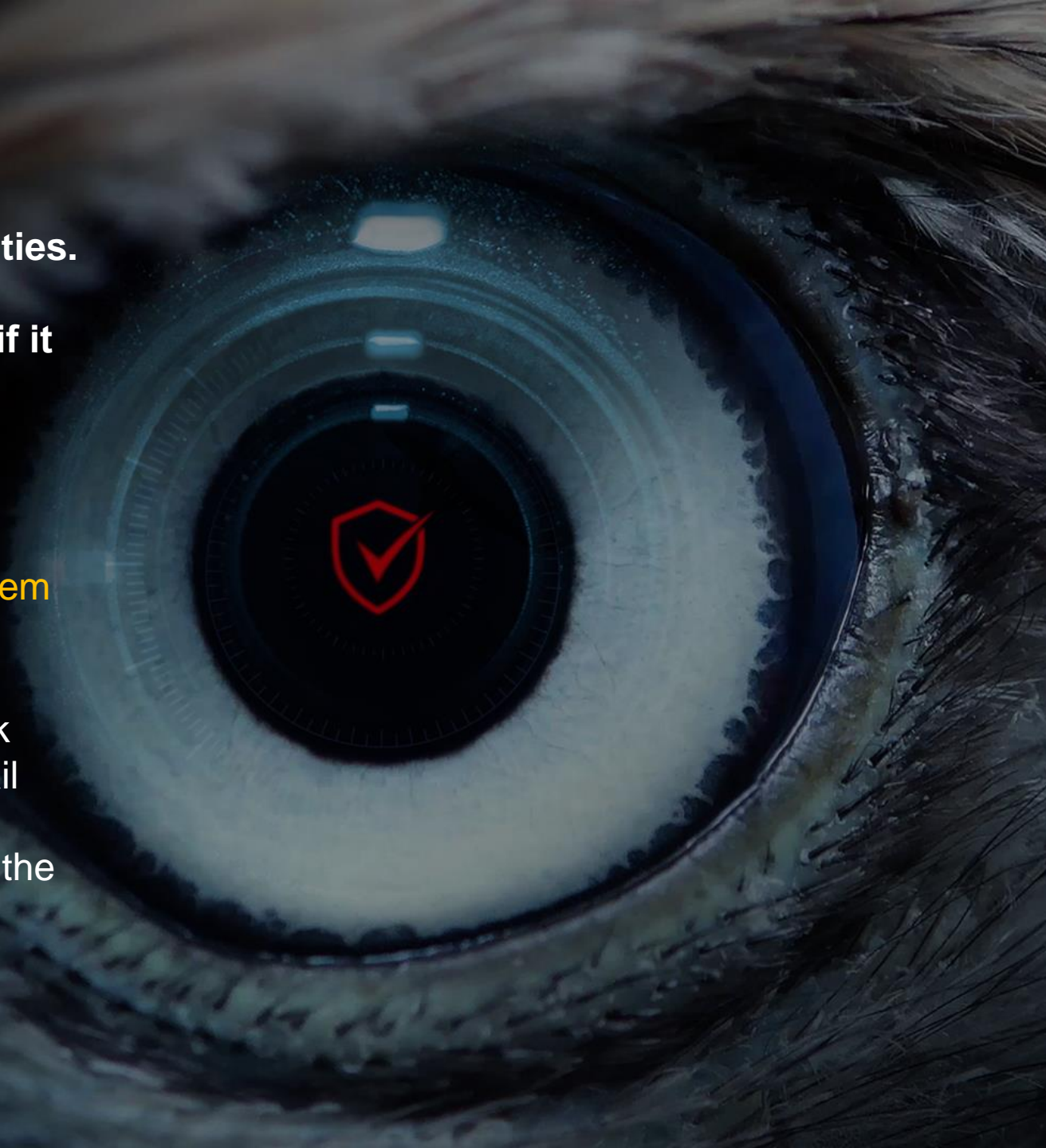
Little and often

Reduce your team's workload with a little and often approach.

- By uncovering and remediating vulnerabilities on an ongoing basis, you make securing your IT estate bitesize and manageable.

- Monthly reports categorise vulnerabilities.

- **Prioritise with clarity and confidence** and ensure your remediation efforts are focused on the most critical risks to your business.

claranet cyber security®

The assurance of experts

Gain a team of trusted security advisers who understand your business and your IT estate.

_____

Work hand-in-hand with our dedicated team of expert penetration testers, as they build their knowledge of your IT estate, your organisation, and the potential risks you face, to provide you with tailored security recommendations.

Continuous support from our team during your normal working hours helps you digest the findings in your report and support your remediation efforts. You'll get direct access to the penetration testers involved.

We retest your applications after you have remediated the vulnerabilities, so you get the assurance of experts.
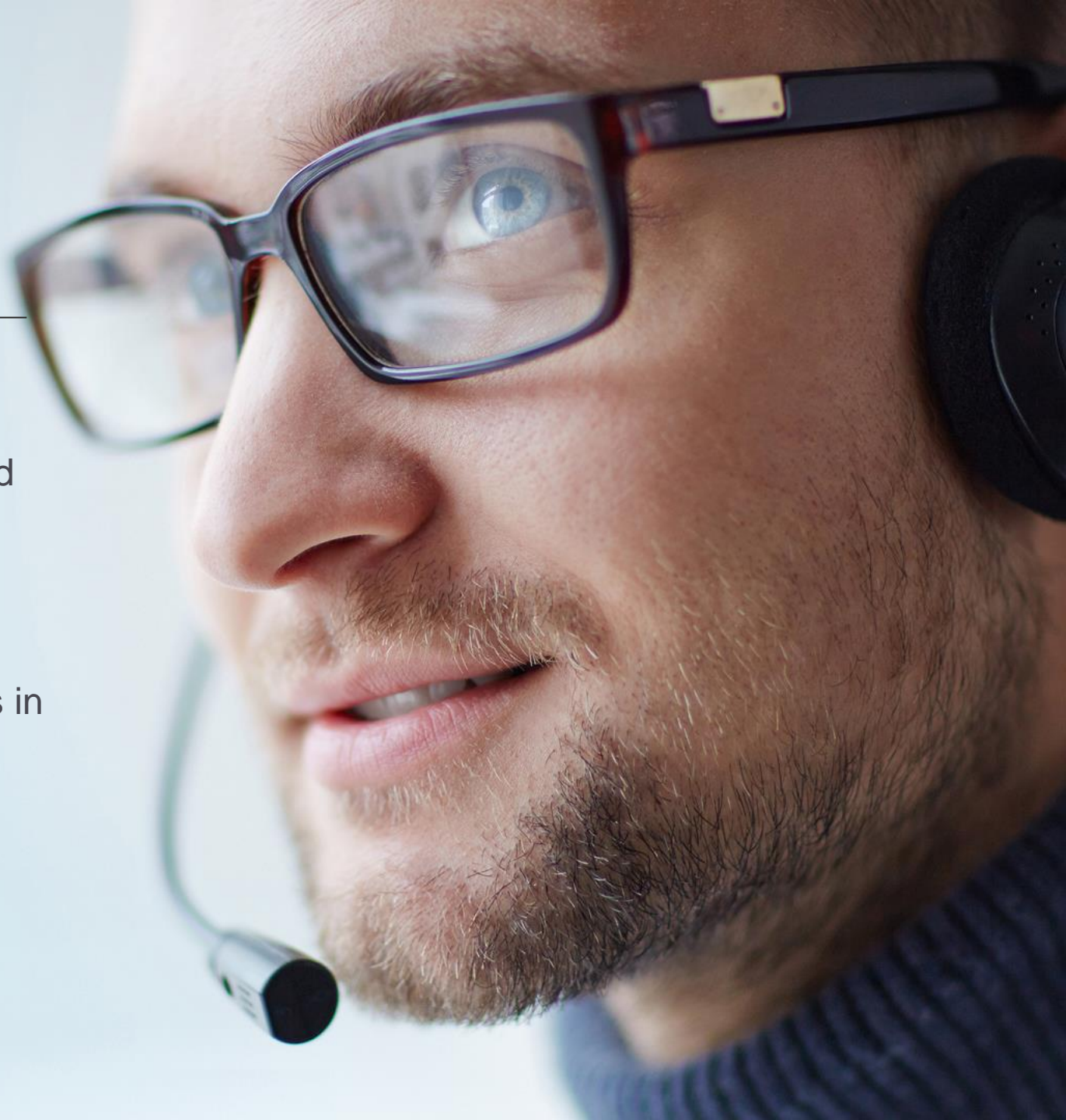
Cyber Portal

The Cyber Portal puts you in control, allowing you to view all discovered vulnerabilities at a glance, and generate custom reports.

Use the Dashboard to:

- Gain an overview of your exposure to vulnerabilities.
- Identify the most frequently occurring vulnerabilities.
- Identify your most vulnerable assets.

claranet cyber security®

Cyber Portal – Features

Inventory (Asset Management)

- Easily manage your assets in one place.
- Request status changes for assets (e.g., transition from active to inactive).

Vulnerabilities

- Access a comprehensive list of vulnerabilities.
- Filter vulnerabilities for custom results.
- Generate and download customised reports based on selected or filtered vulnerabilities.
- Dive into the details of each vulnerability with just one click.

Reports

- Easily access all your reports in one place.
- Quickly view a list of custom-generated reports.
- Stay informed with notifications for high-impact vulnerabilities.

claranet **cyber security**®

Contact us today

(415) 907-7084

teamusa@claranet.com