Hey, Blue Teams:

Stop Waiting for Pen Tests to Find Gaps.

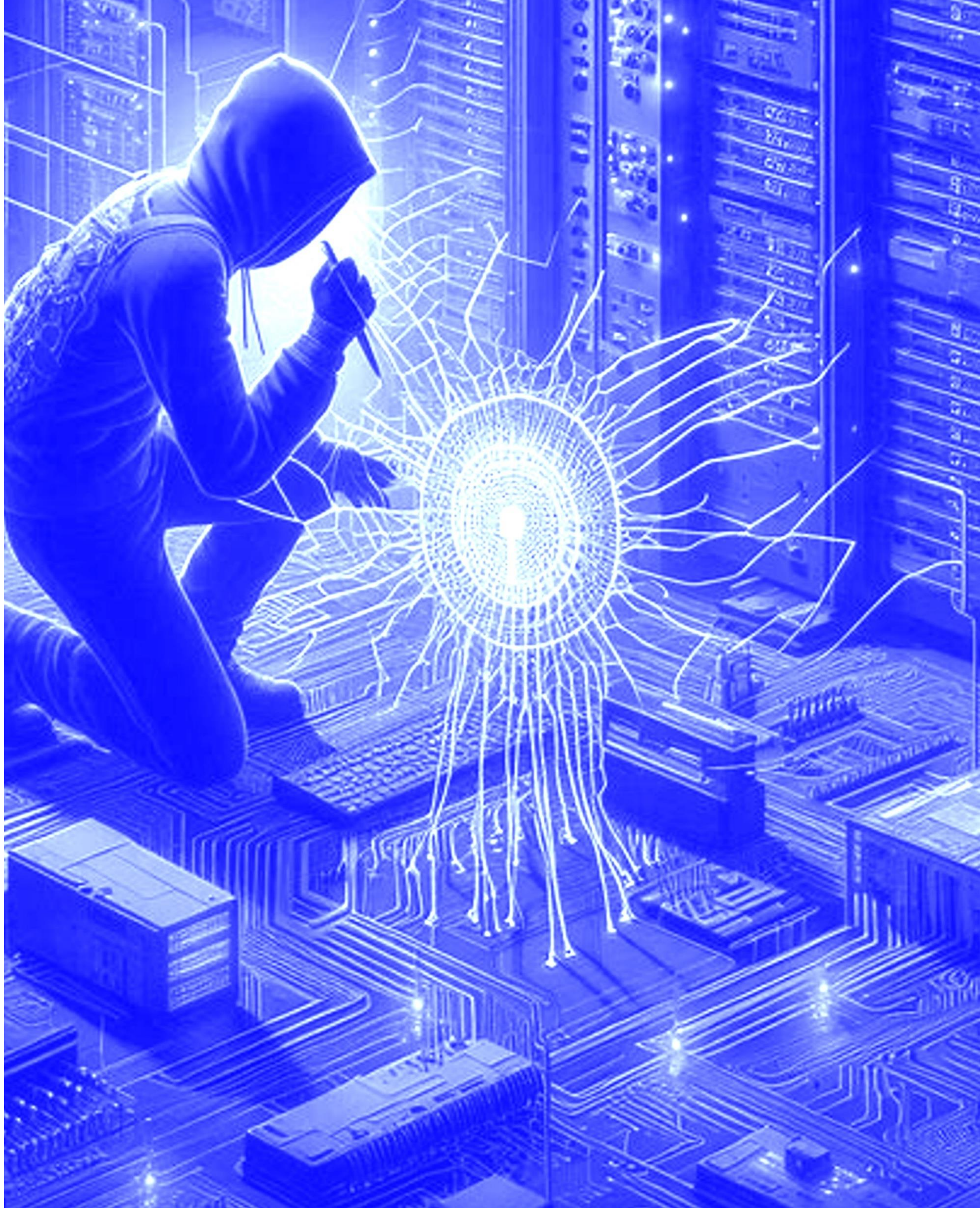
Take Control of Your Offensive Testing.

Brian Moran,
Senior Director of Product Marketing

The Need for Security Validation

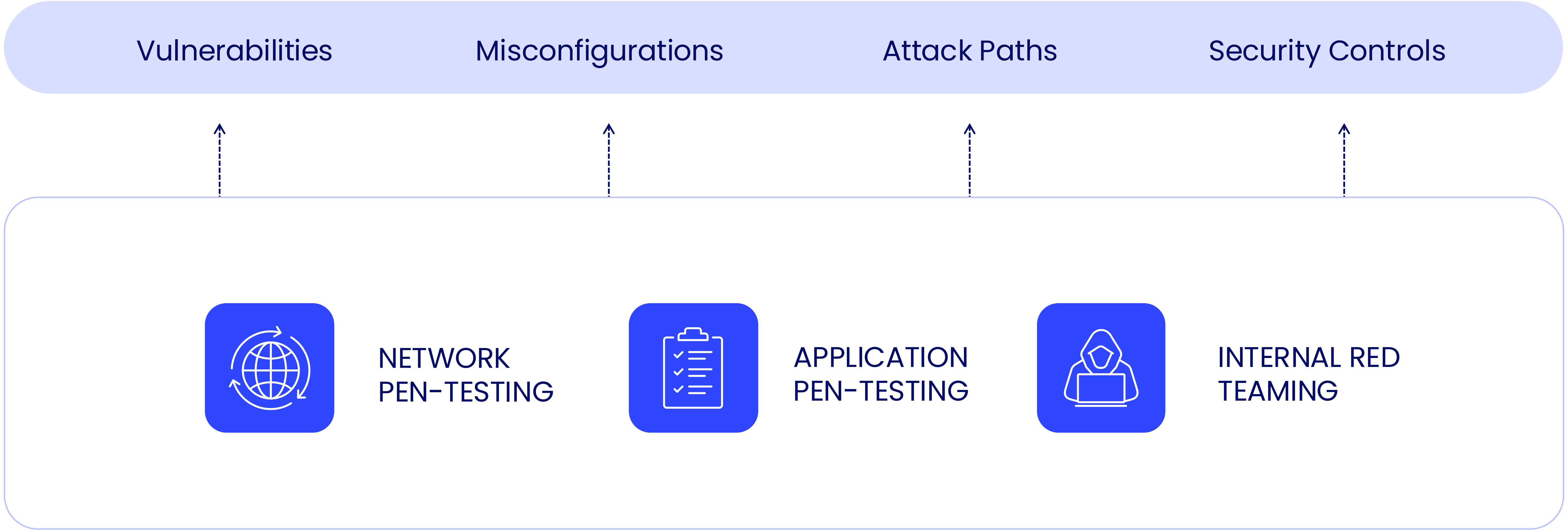
You know you have gaps.

Think like an attacker to find & fix those gaps to prevent the breach.



Cymulate

Breaking Down Manual Penetration Testing



Vulnerabilities

Misconfigurations

Attack Paths

Security Controls

NETWORK PEN-TESTING

APPLICATION PEN-TESTING

INTERNAL RED TEAMING

x Not Continuous

x Not Scalable (Scope + Cost)

x Limited Defense Efficacy

Penetration Testing: Limitations

- Manual
- Costly
- Limited scope
- Point in time

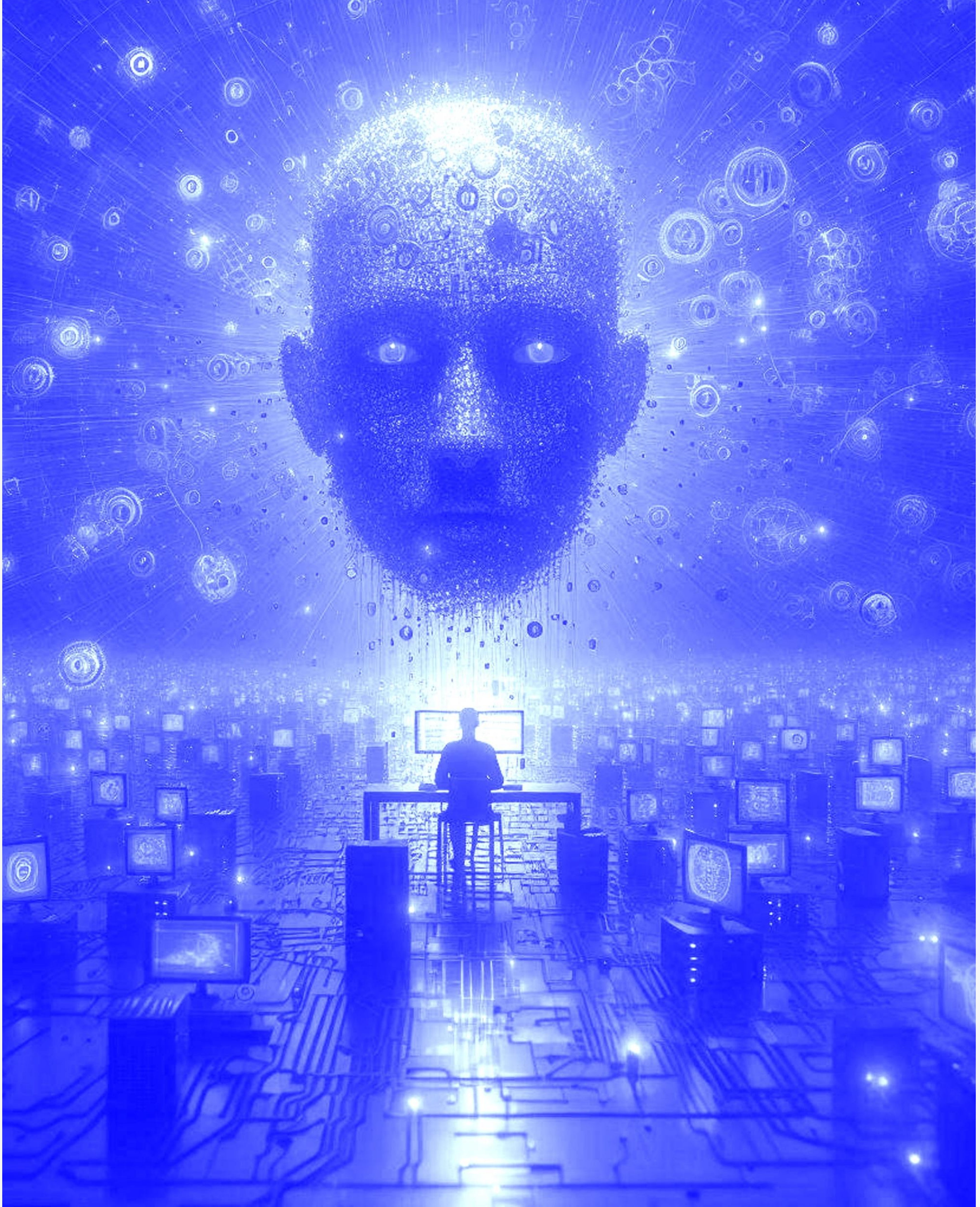
In Search of Continuous Automated Testing

Vulnerability Assessment

Attack Surface Management

Automated Penetration Testing

Security Controls Validation



Vulnerability Assessment

- Identify outdated software
- Compliance mandated

Limits

- Prioritization
- Cannot discern exploitable vs. unreachable vulnerabilities
- Remediation often relies on other teams

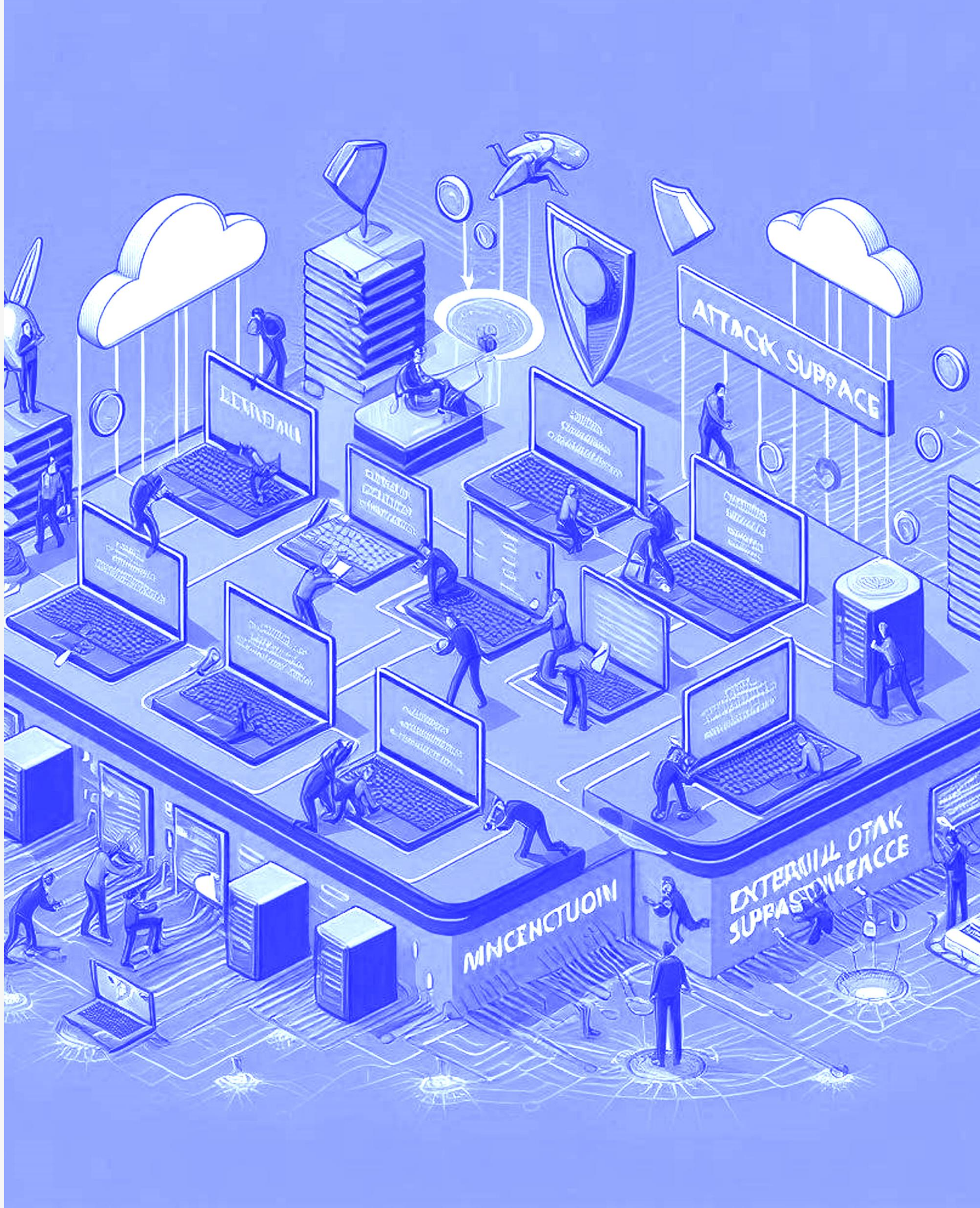
Attack Surface Management

- External attacker view of assets – including unmanaged assets
- Risky configurations
- Some vulnerabilities

Limits

- Theoretical (unproven) attack paths
- Lack context of security controls
- False positives or just noisy with low-severity findings

Cymulate



Automated
Pen Testing

- Validate attack paths
- Discover vulnerabilities & misconfigurations

Limits

- Results overlap with vulnerability assessments
- Limited testing of controls

WEB GATEWAY

SOC

VULNERABILITY MANAGEMENT

SIEM

IT INFRASTRUCTURE

EMAIL GATEWAY

Security Control Validation

ENDPOINT SEC

ACTIVE DIRECTORY

CLOUD SECURITY

XDR

Test and optimize cyber defenses

NETWORK SECURITY

Cymulate

KUBERNETES

Security Control Validation

- Automatically identify gaps in security controls
- Monitor security control drift
- Test for new threats

- Prioritize initiatives based on gaps
- Know the state of cyber resilience
- Detection engineering & control tuning

Limits

- Exposure assessments
- Attack paths

Technologies & Outcomes

Multiple approaches to Automated Security Validation

	Vulnerabilities	Misconfigurations	Attack Paths	Control Effectiveness
Vulnerability Assessment	●	◑		
Attack Surface Management	◑	●	◑	
Automated Pen Testing	◑	◑	●	◔
Security Controls Validation				●

Cymulate

The results our customers are seeing

1-2 hours

average time to validate new threats, from 2-3 days

INVESTMENT FIRM

70%

reduction vulnerabilities detected in next pen test

IT SOLUTIONS

91%

improvement in malicious file detection post mitigation

SPORTS MEDIA

60%

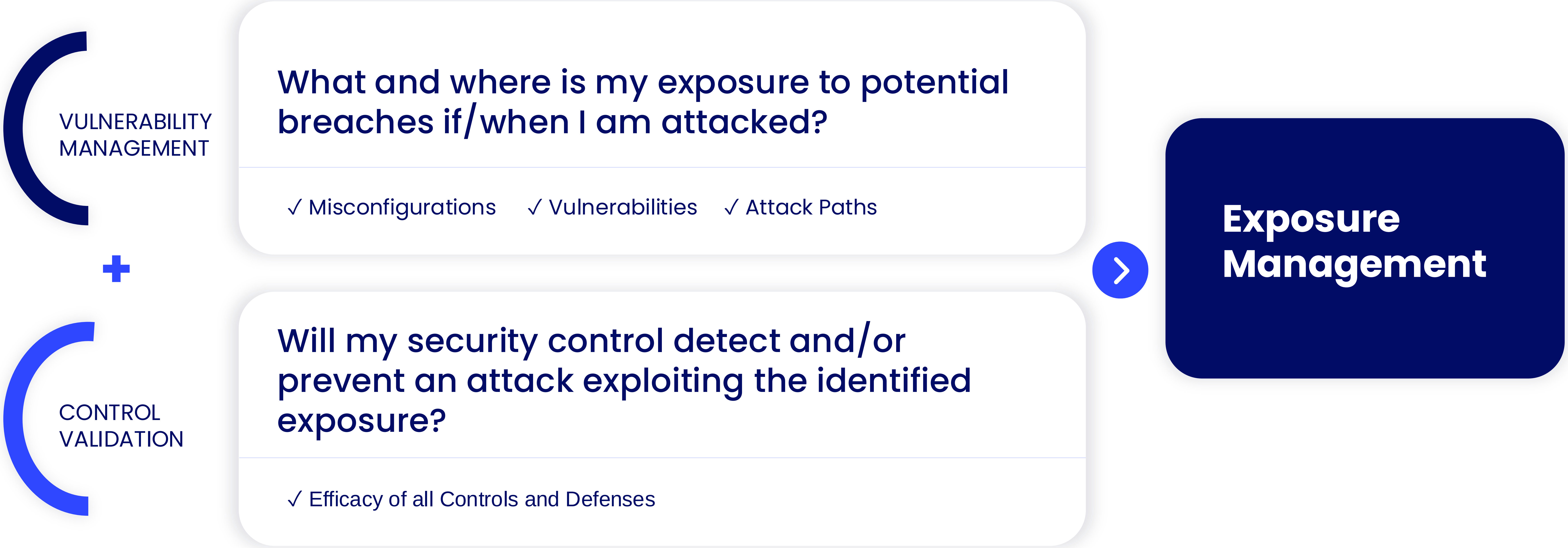
increase in team efficiency addressing vulnerabilities

FINANCE COMPANY

> When testing our endpoint with Cymulate, we noticed large discrepancies between our workstations and servers. Because we can immediately see the impact of our mitigation efforts by re-running the Cymulate assessments, we went from 98% of malicious files not being detected to only 7%!”

VISION: THE PATH FORWARD

The transition to Exposure Validation



VULNERABILITY MANAGEMENT

What and where is my exposure to potential breaches if/when I am attacked?

✓ Misconfigurations ✓ Vulnerabilities ✓ Attack Paths

+

CONTROL VALIDATION

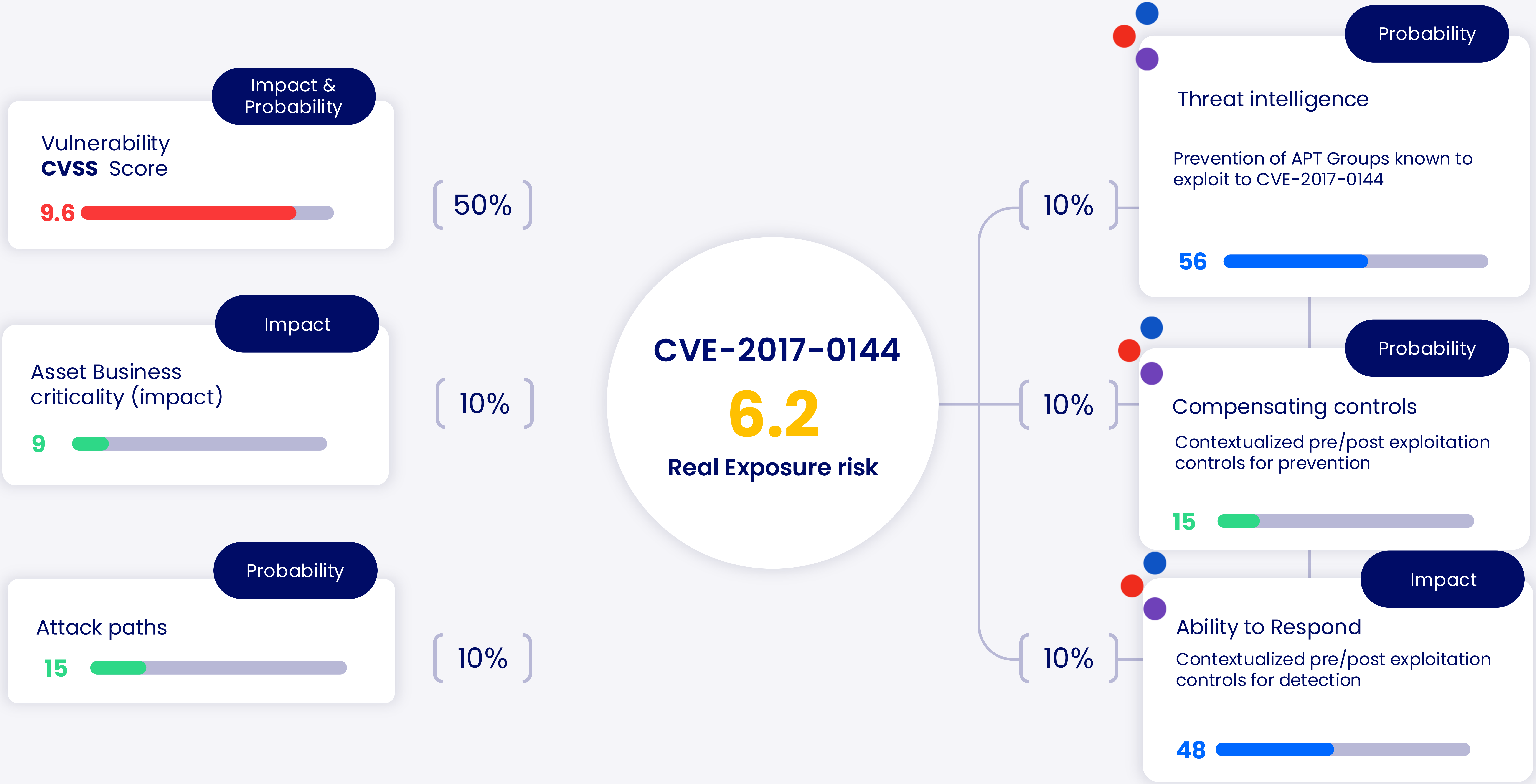
Will my security control detect and/or prevent an attack exploiting the identified exposure?

✓ Efficacy of all Controls and Defenses

Exposure Management

Cymulate

Contextualized exposure prioritization



Impact & Probability

Vulnerability **CVSS** Score

9.6

50%

Impact

Asset Business criticality (impact)

9

10%

Probability

Attack paths

15

10%

CVE-2017-0144

6.2

Real Exposure risk

10%

Probability

Threat intelligence

Prevention of APT Groups known to exploit to CVE-2017-0144

56

10%

Probability

Compensating controls

Contextualized pre/post exploitation controls for prevention

15

10%

Impact

Ability to Respond

Contextualized pre/post exploitation controls for detection

48

Attack paths done right

- 🔴 EDR Prevention
- 🟡 IPS Prevention
- 🟡 EDR Detection
- 🔴 SIEM Alert

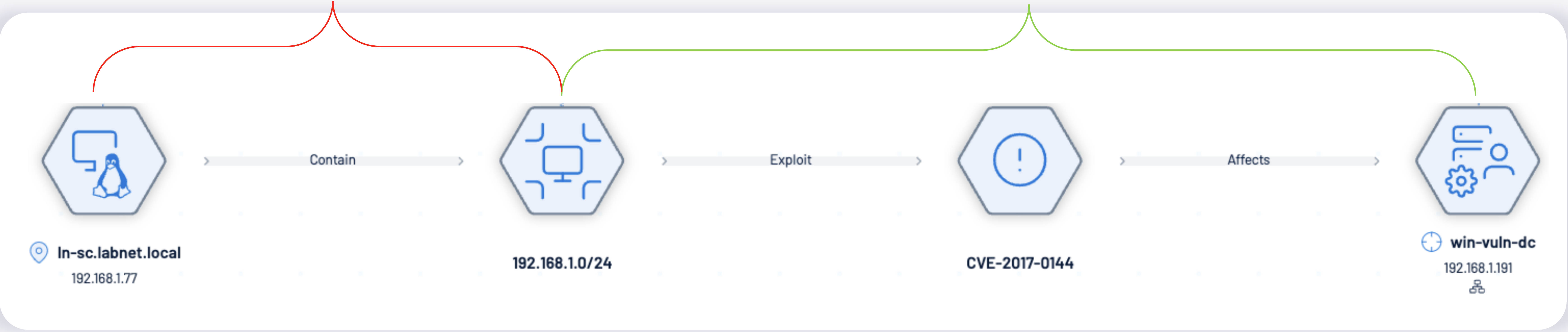
9.4 MITRE ATT&CK T1040

- 🟢 EDR Prevention
- 🟢 IPS Prevention
- 🟢 EDR Detection
- 🟡 SIEM Alert

4.6 CVE 2017-0144

Discovery, Credential Access/Network Sniffing

Lateral Movement / Exploitation of Remote Services



Cymulate

Exposure Management done right.

Blue Teamers, you now have control

Disrupt attack paths

Tune and optimize defenses

Compensate for known gaps

Interested in a deeper discussion?

Joe Heckley
Account Manager

Gio Macias
Solution Engineer

Cymulate