Outsourcing Third-Party Risk: Managing the expanding attack surface

From Chaos to control with Defensive & Offensive Outsourcing

Agenda

- Introduction
- Expanding Attack Surface
- Offensive SOC
- Changed Perspective
- Recommendations
- Q&A

- Robin Bruynseels
- SOC Team Coördinator @ easi
- Interest in everything defensive, tech and people
- Co-Chair of Cyber Security Coalition Belgium Focus Group *CIDR*

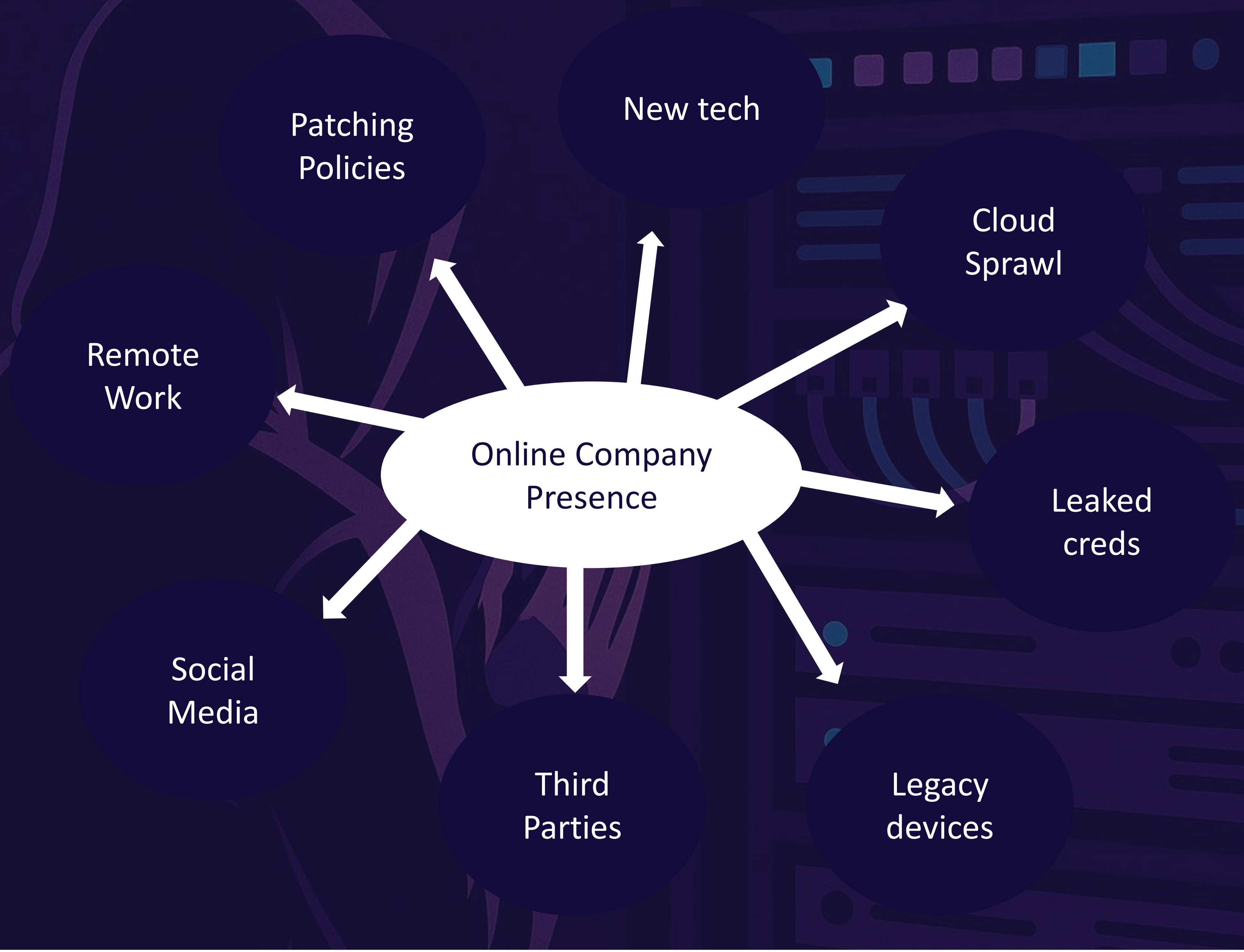
%username%

- △ Joris Ignoul
- △ Penetration Tester @ easi
- △ Interest in everything offensive & defensive
- △ HackTheBox Ambassador

%username%

disclaimer

Expanding Attack Surface



Online Company Presence
Patching Policies
New tech
Cloud Sprawl
Remote Work
Leaked creds
Social Media
Third Parties
Legacy devices

Security Teams' Challenges

We need to review everything before it gets into production.

Why? We trust X.

How come this server is not updated?

Which server?

One of our users got breached through LinkedIn.

Why are we not protected against this?

BLEEPINGCOMPUTER

“Ransomware attack cost IKEA operator in Eastern Europe $23 million”

techradar pro

“IKEA black Friday ransomware attack cost franchise firm millions”

Fourlis
ΟΜΙΛΟΣ ΕΤΑΙΡΙΩΝ

IKEA®

INTERSPORT

Foot Locker®

Holland & Barrett

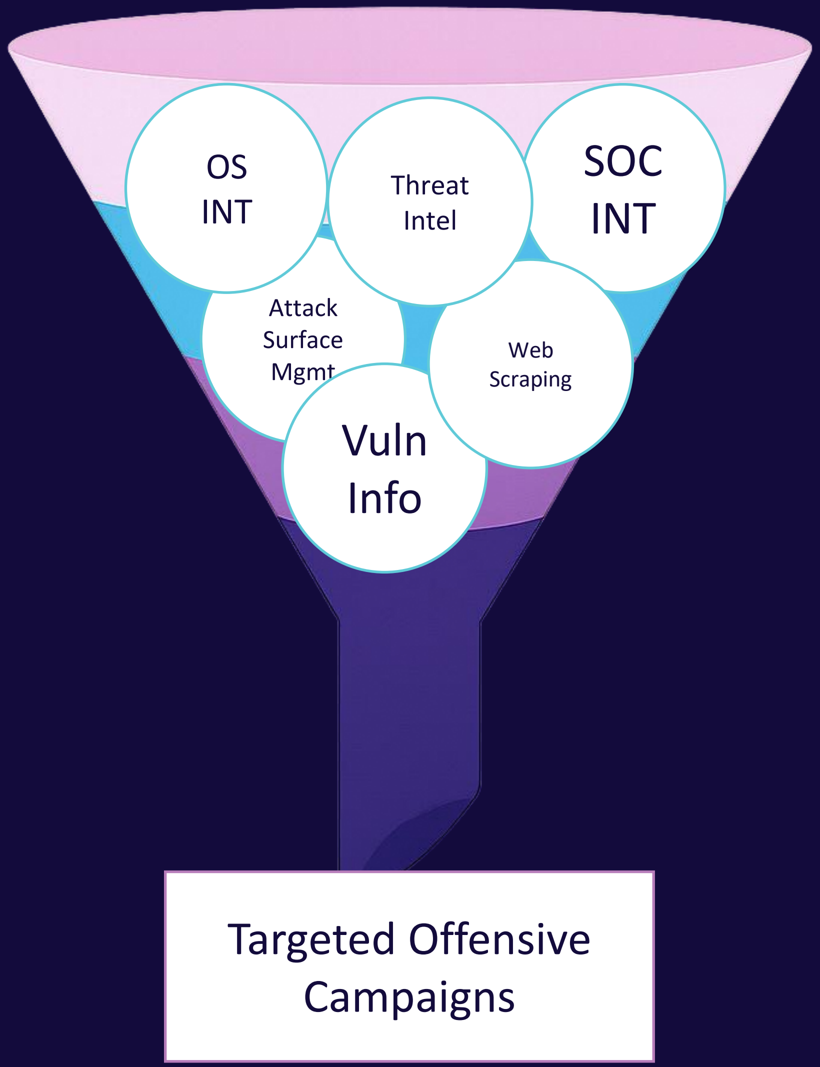
The Blame Game

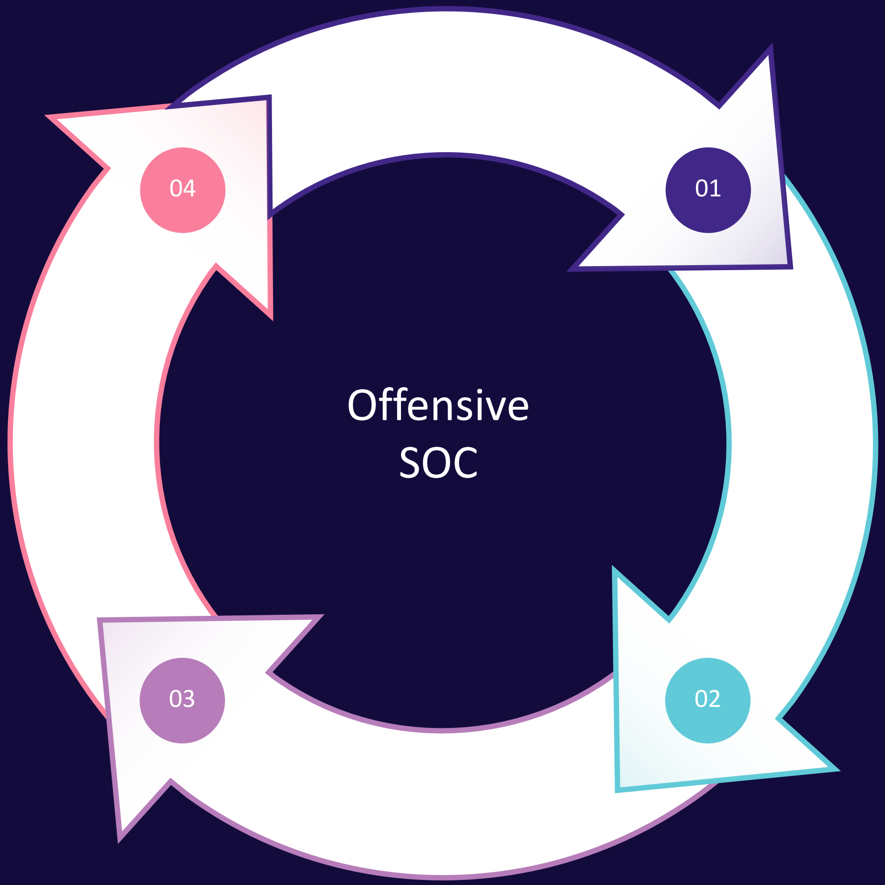
- △ *“How did **the** penetration testers not find this?”*
- △ *“How did a single compromise lead to a domain takeover?”*
- △ *“Is our user awareness even worth it?”*
- △ *“Blame our EDR, NDR, MDR, ...!”*
- △ *“Blame not having an EDR, NDR, MDR, ...!”*
- △ *“There is nothing we could have done...”*

Offensive SOC?

“offensive SOC”

- △ Alerts => triggers to react
- △ Tailored Phishing Campaigns
- △ Targeted Web App Attacks
- △ Emulate Opportunistic Attackers
- △ Proper Setup for a Red Teaming Exercise





THREAT ANALYSIS

Identify and assess potential threats to your systems and infrastructure.

Focus on understanding the evolving tactics, techniques, and procedures (TTPs) used by attackers.

RECON

Perform deep reconnaissance to gather information on systems, networks, and users.

Use insights to simulate real-world attack scenarios.

INTRUSION

Test vulnerabilities through simulated breaches to assess system resilience.

Emulate advanced attacker techniques for deeper insights.

REPORTING

Deliver real-time updates and detailed findings.

Provide actionable recommendations to improve security posture.

Ivanti Vulnerabilities

Last year there was breach in Ivanti endpoints. An unauthenticated attacker could execute remote code through the web portal.

CVE’s tracked:

- CVE-2023-46805
- CVE-2024-21887

Ivanti Unauthenticated Remote Code Execution

- What do we know about the vulnerability?
- Are there POCs available?

Vulnerability Disclosure
(10 jan 2024)

https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_USx

Ivanti Unauthenticated Remote Code Execution

- IOCs shared
- Testing environment for IOCs & Continuous Help

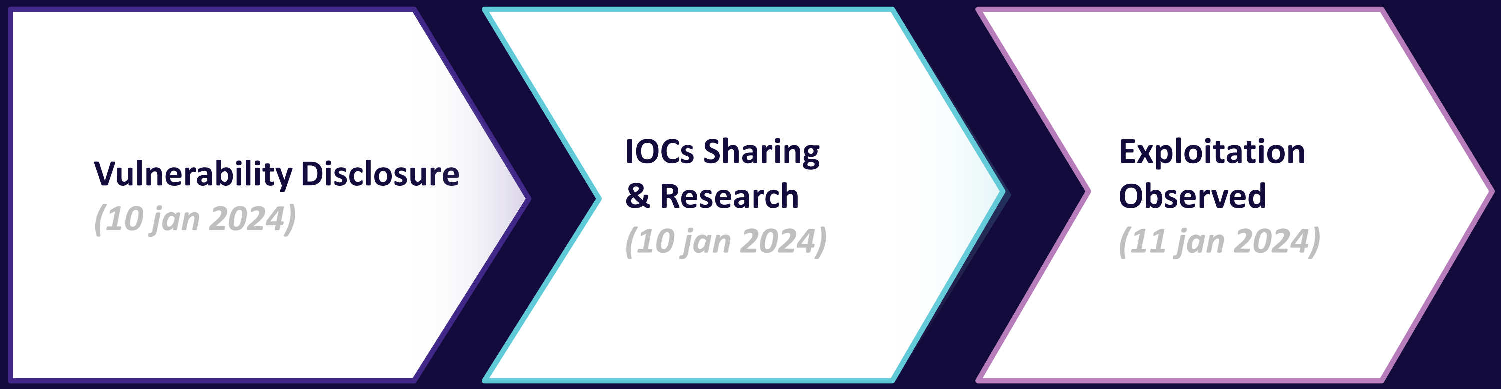
Vulnerability Disclosure
(10 jan 2024)

IOCs Sharing & Research
(10 jan 2024)

Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

Ivanti Unauthenticated Remote Code Execution

- Testing environment for IOCs
- Deeper research into proof of concept



Vulnerability Disclosure
(10 jan 2024)

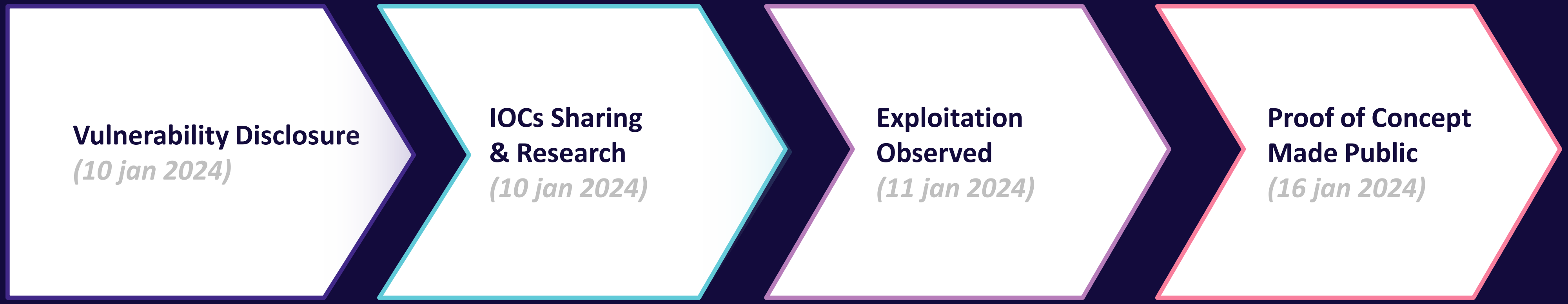
IOCs Sharing & Research
(10 jan 2024)

Exploitation Observed
(11 jan 2024)

Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060bv

Ivanti Unauthenticated Remote Code Execution

- Proof of concept code released on github
- Further exploitation observed



Vulnerability Disclosure
(10 jan 2024)

IOCs Sharing & Research
(10 jan 2024)

Exploitation Observed
(11 jan 2024)

Proof of Concept Made Public
(16 jan 2024)

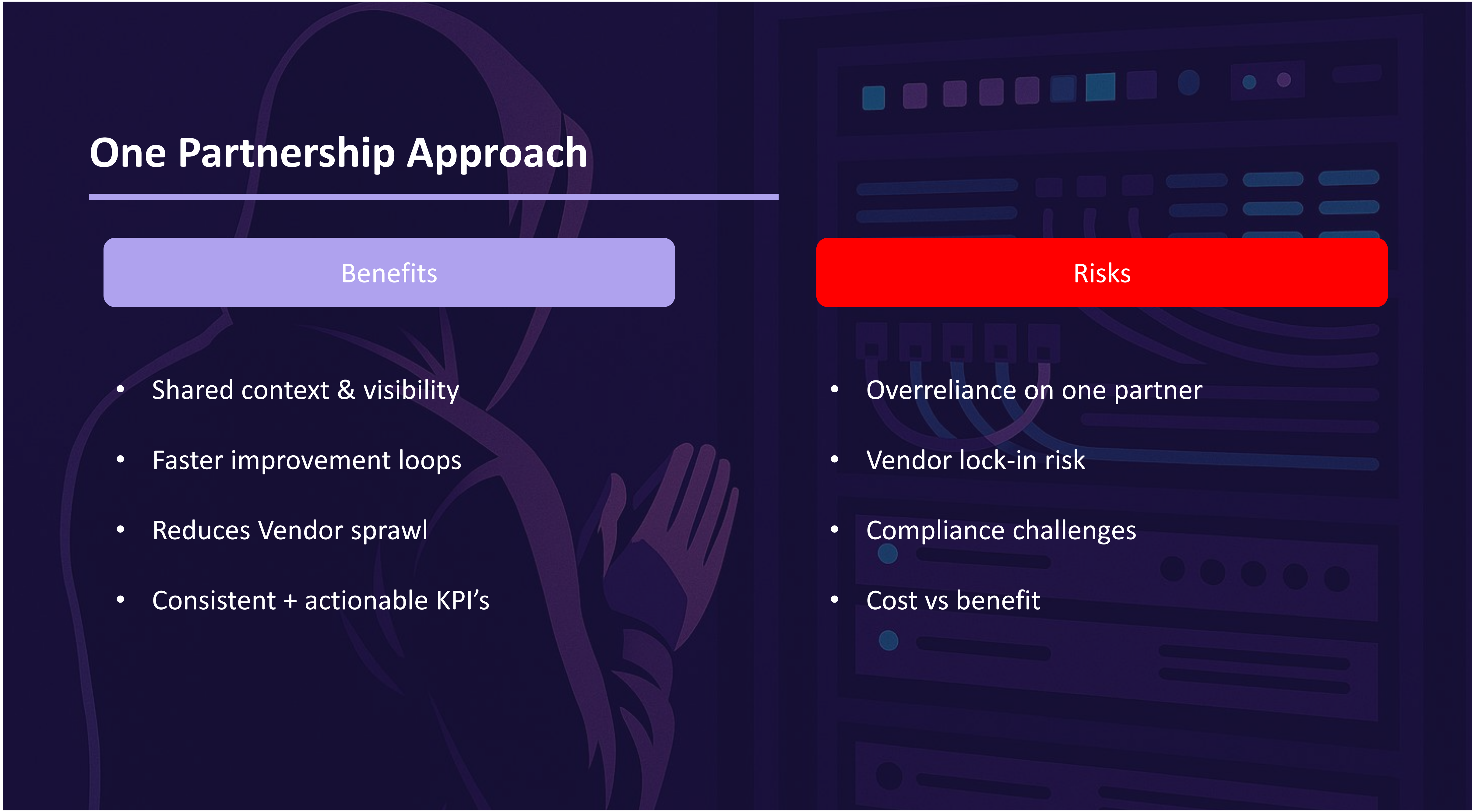
Source: https://github.com/duy-31/CVE-2023-46805_CVE-2024-21887

Both Defense and Offense

The Changed Perspective

- △ Defensive Monitoring
  - △ Attack surface discovery + continuous threat detection
- △ Offensive Testing
  - △ Testing/simulating real-world attacks before attackers do

One Partnership Approach



Benefits

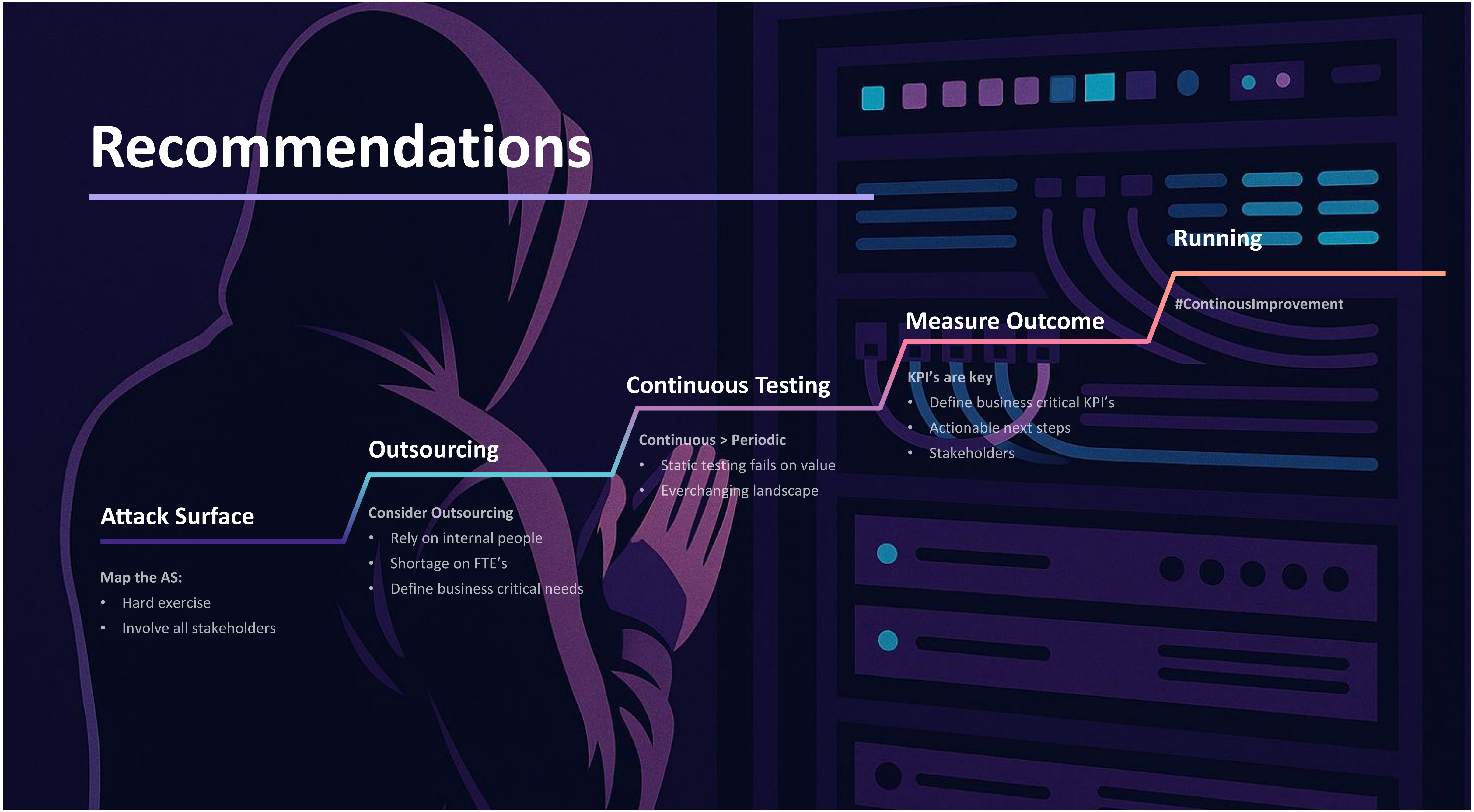
- Shared context & visibility
- Faster improvement loops
- Reduces Vendor sprawl
- Consistent + actionable KPI’s

Risks

- Overreliance on one partner
- Vendor lock-in risk
- Compliance challenges
- Cost vs benefit

Recommendations

Recommendations



Attack Surface

Map the AS:

- Hard exercise
- Involve all stakeholders

Outsourcing

Consider Outsourcing

- Rely on internal people
- Shortage on FTE’s
- Define business critical needs

Continuous Testing

Continuous > Periodic

- Static testing fails on value
- Everchanging landscape

Measure Outcome

KPI’s are key

- Define business critical KPI’s
- Actionable next steps
- Stakeholders

Running

#ContinousImprovement

questions?