SaaSy detection

Purple Teaming Software-as-a-Service Platforms

Nick Jones and Chris Philipov

WITH secure

How many SaaS products do you use at work on a daily basis?

TL;DR

SaaS is a Huge Attack Surface in Most Organisations

Critical attack surface, too – lots of critical data in most organisations' SaaS applications

Early Days, but Some Problems Already Obvious

Log format heterogeneity
Even harder to separate good from bad than cloud infra

Where to start:

Business critical apps – CRM and similar, HR apps, SCM/CICD in dev houses etc
Well known platforms – most likely to get hit by attackers first

Who Are We?

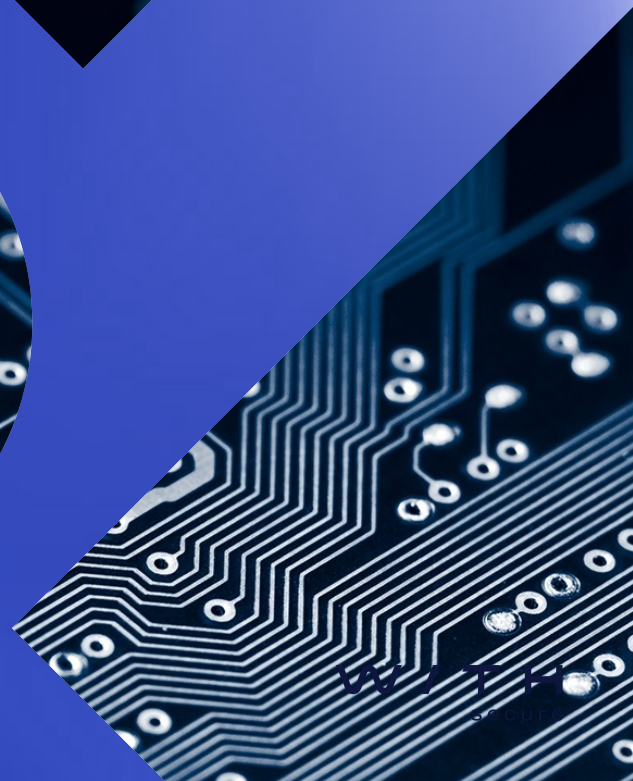
Chris Philipov

Senior Security Consultant

Nick Jones

Principal Security Consultant
Cloud Security Lead

The SaaS Security Landscape



What's the deal with SaaS

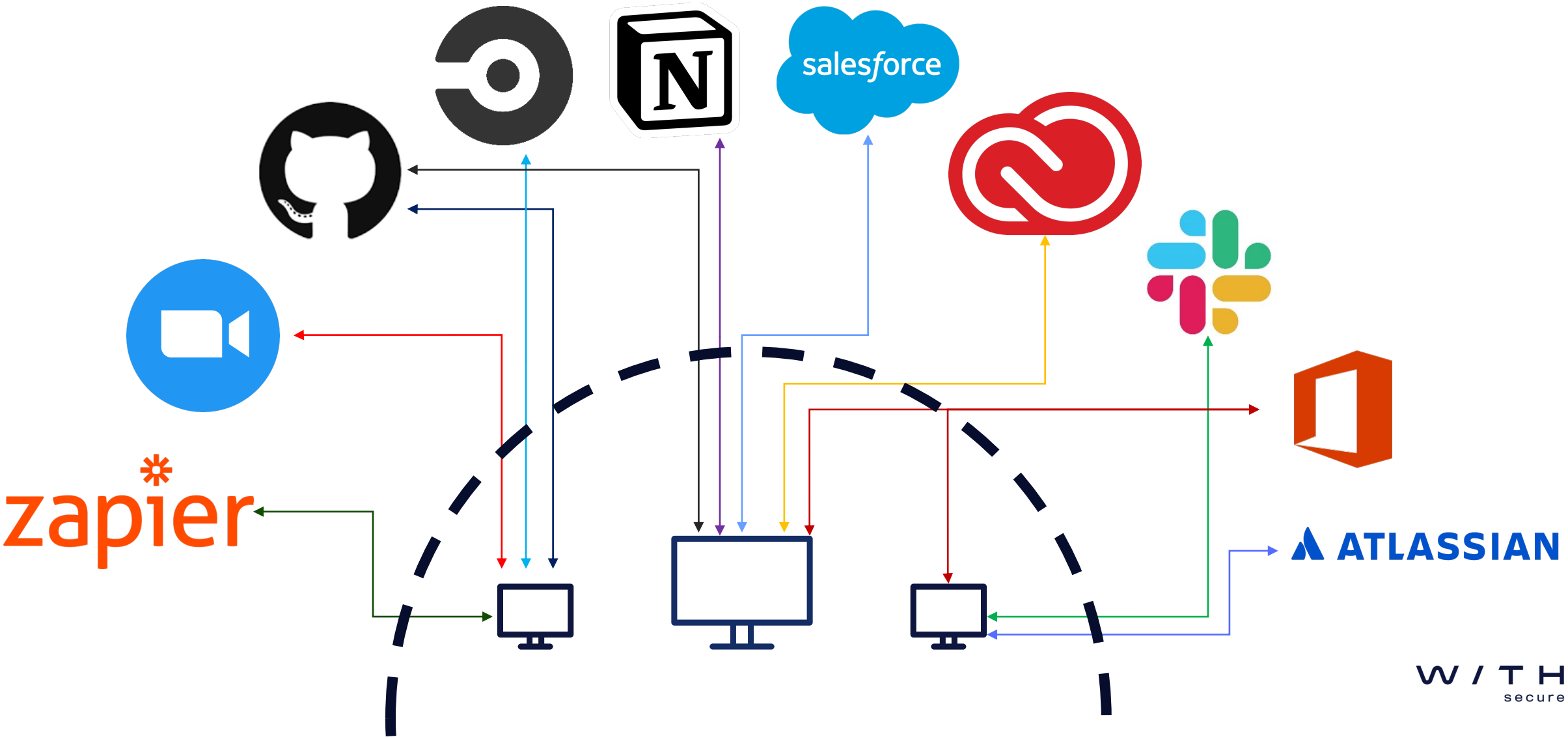
$54 B

$251 M

$689 M

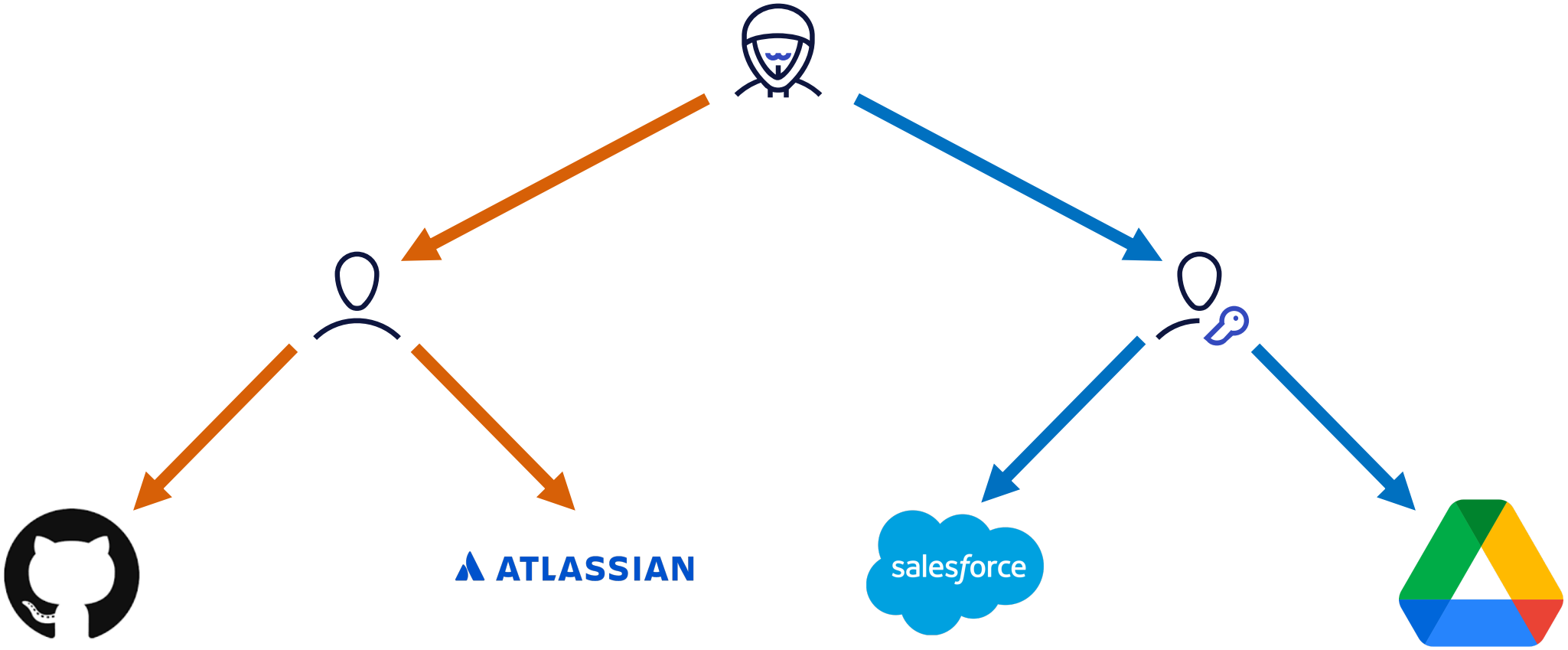
$18 B*

SaaS Map of an Average Organization...



W / T H
secure

SaaS Map Attack Vectors



SaaS involved Breaches

SaaS solutions stand as a key part in major breaches

Attackers aim to use any access as much as they can

Difficult to prevent, so how do we spot it?

How Hackers Used Slack to Break into EA Games

A representative for the hackers explained to Motherboard how the group stole a wealth of data from the game publishing giant.

By Joseph Cox

Social media boosting service exposed thousands of Instagram passwords

Zack Whittaker @zackwhittaker / 5:19 PM GMT • January 30, 2020 Comment

Okta's Investigation of the January 2022 Compromise

Breaches 2: Electric Boogaloo

SolarWinds Orion: More US government agencies hacked

15 December 2020

$938M

A Devastating Twitch Hack Sends Streamers Reeling

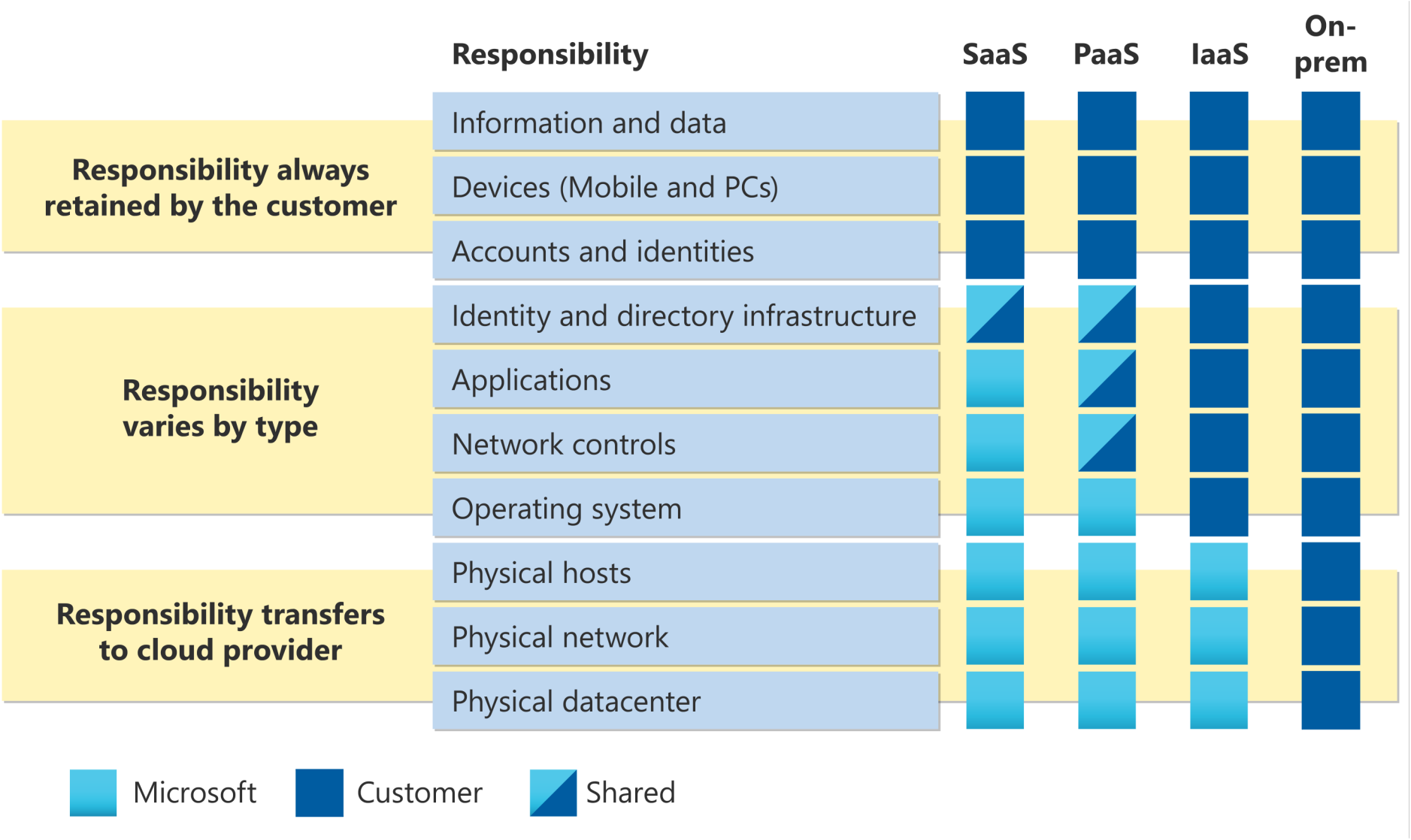
The data breach apparently includes source code, gamer payouts, and more.

$2.3B

W / T H secure

Detection in SaaS apps

What is so different about SaaS?



https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

WITH secure

Less Control

Reliant on provider's controls

- Compensating controls *sometimes* possible
- At mercy of provider for new controls

Purchase process is critical

- Establish baseline control requirements for SaaS products
- Evaluate controls **BEFORE** purchase

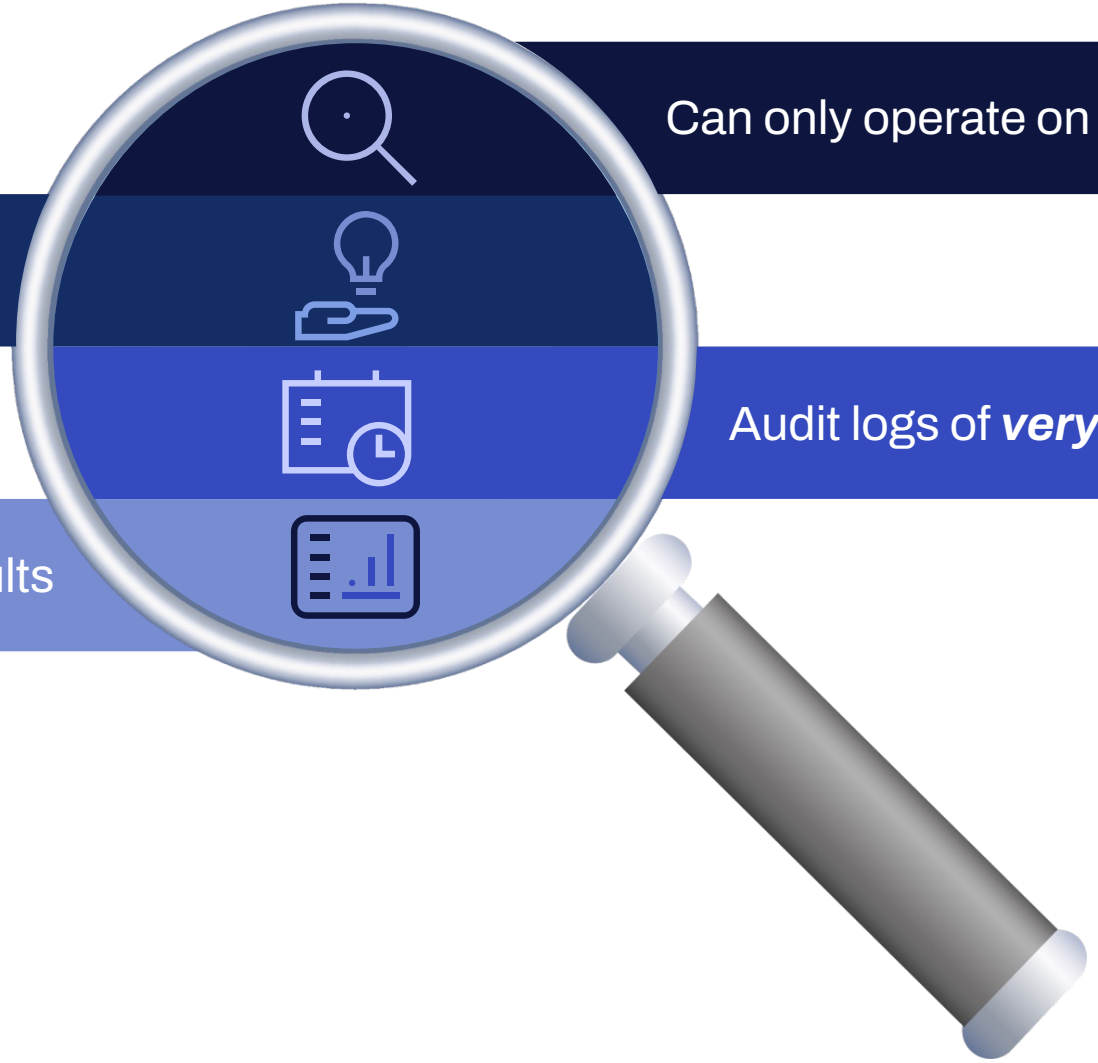
Less Visibility

Can only operate on what you can see

Visibility dictated by the provider

Audit logs of ***very*** varying quality

Combine logs to get effective results



W / T H secure

Telemetry format variation

Totally unstandardized at present

Increases effort requirements to integrate different apps

For now, leverage whatever your SIEM provider offers where possible

If no support for most of your SaaS apps, you need a translation layer

Open Cybersecurity Schema Framework should help!

The Tyranny of Product Tiers

Slack

- Enterprise logging only available in top tiers

GitHub

- Audit logs available in app, but logging APIs only exposed to enterprise tier users

Microsoft 365

- Complex licensing makes it hard to work out what you have access to

The Pitfalls of SaaS Detection

W/TH secure

Telemetry Pitfalls

Require data from multiple events

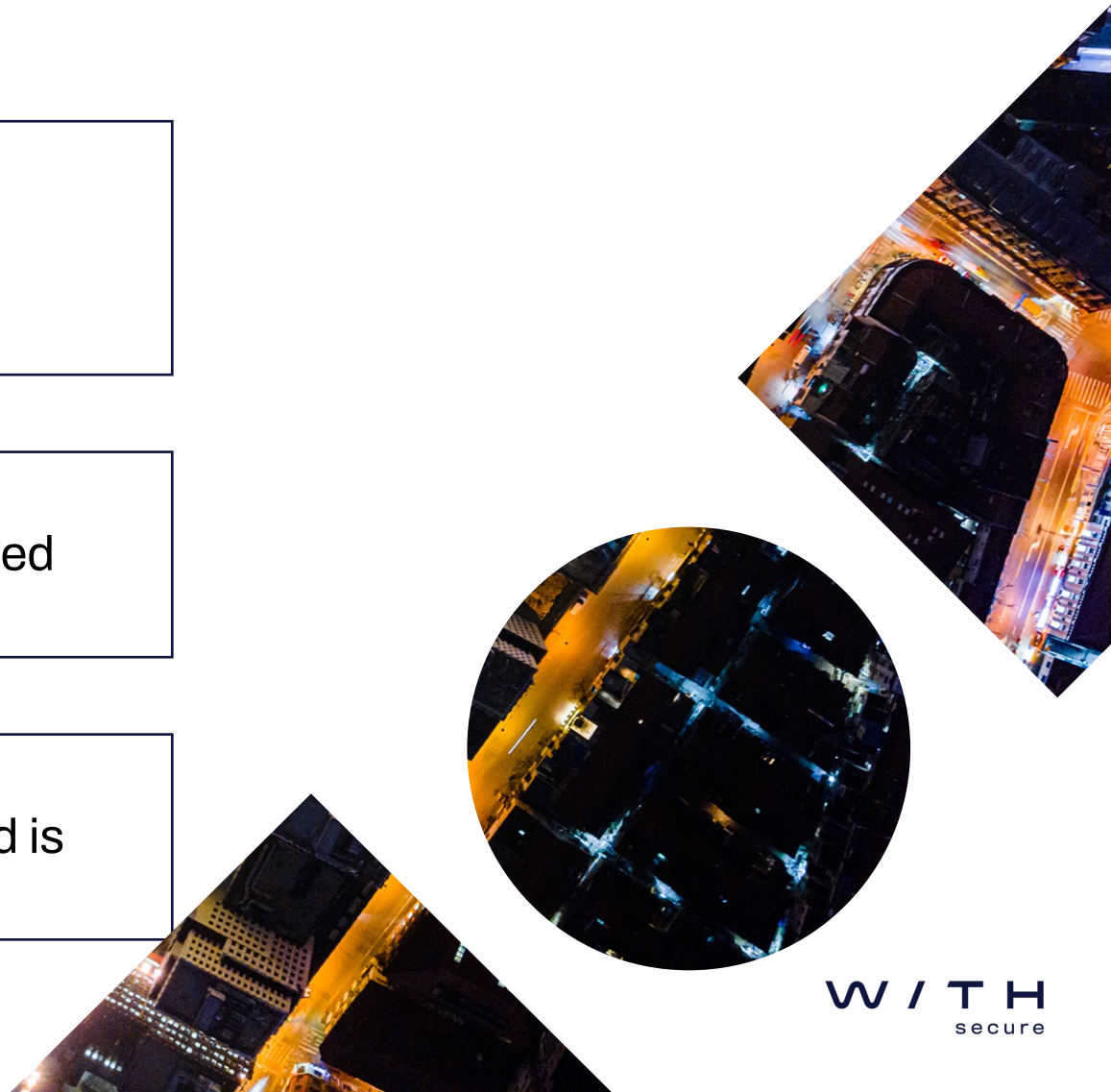
- Disabling branch protection – actions logged are “protected_branch.destroy” and “protected_branch.policy_override”

Require data from different APIs

- Promote user to Organization Owner – action logged is “org.update_member”

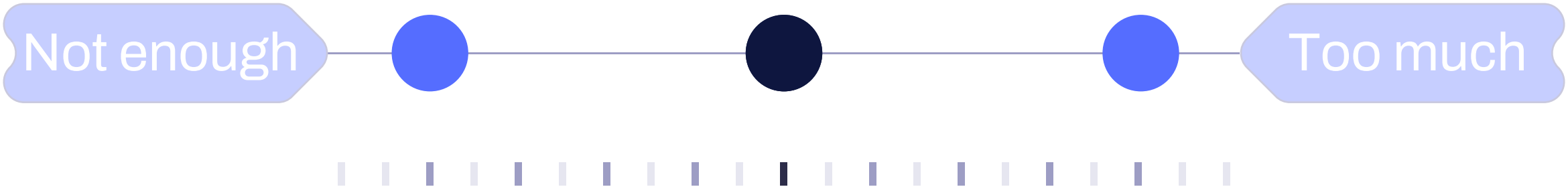
Require integration with separate API

- Promote User to Repository Admin – action logged is “edited”

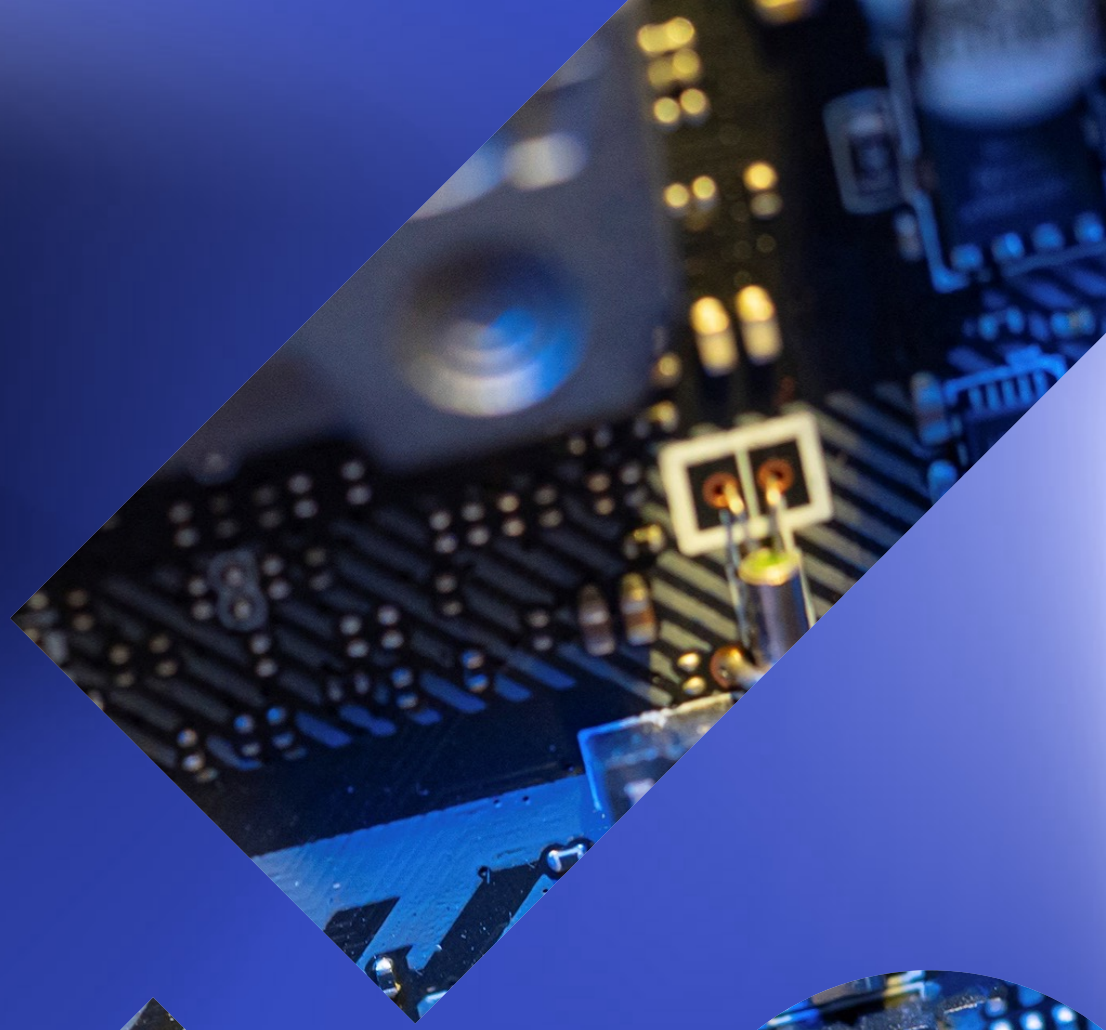


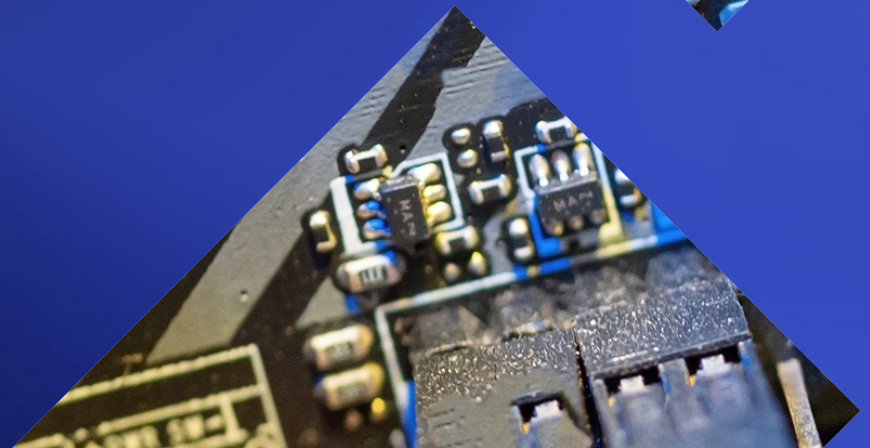
W / T H
secure

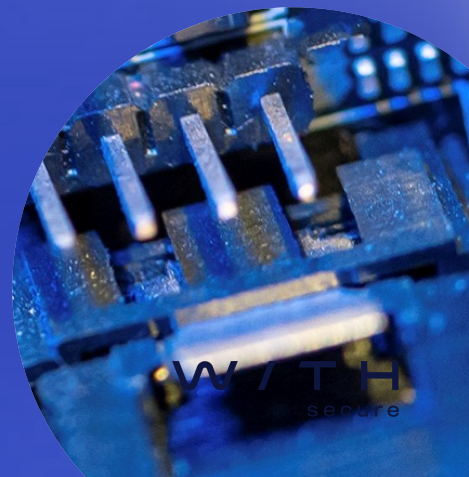
The difficulty that defenders face



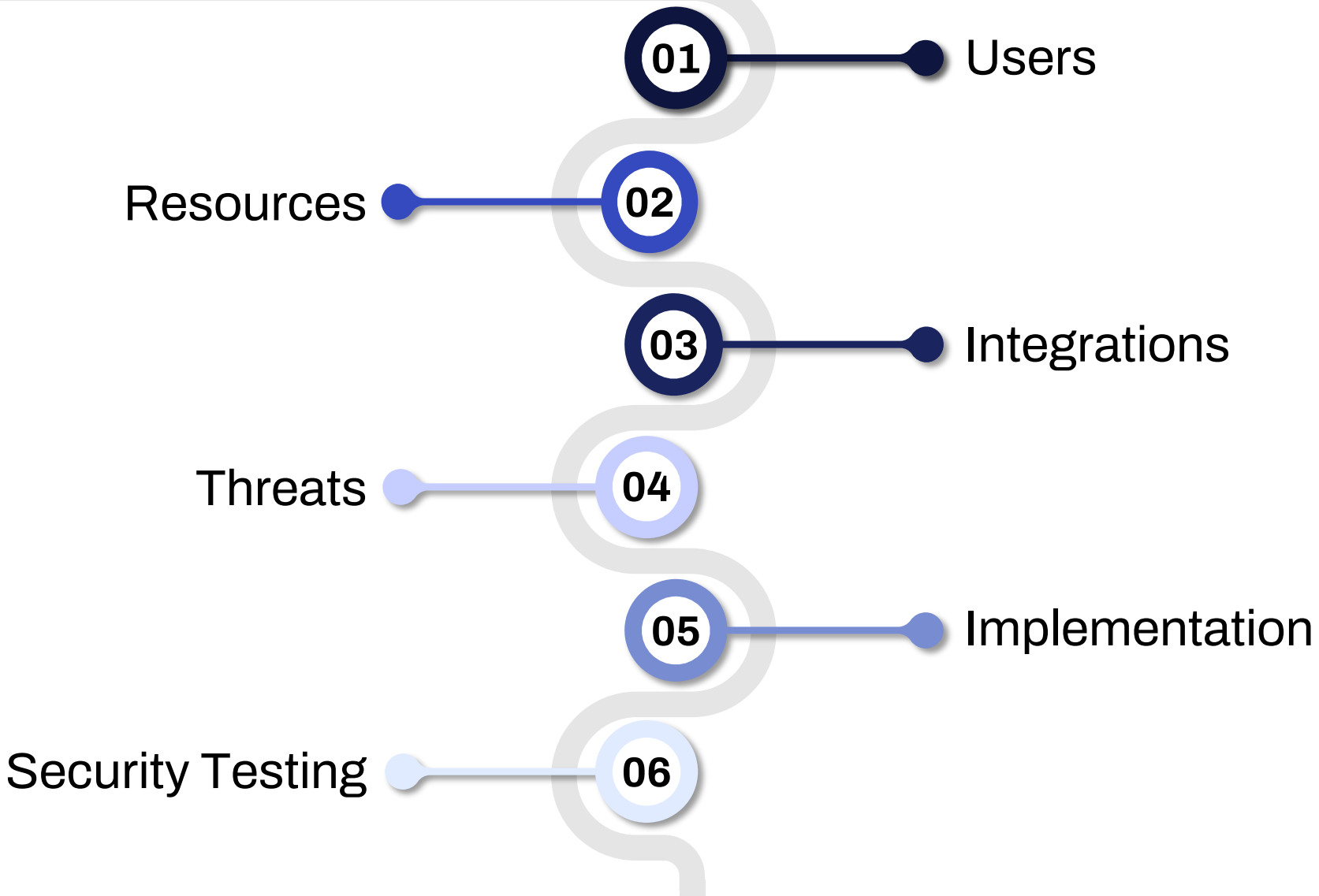
Bringing S(ecurity) to SaaS







Threat Modelling for SaaS



WITH secure

Users

01 Who Are The Users?

How widely used will this be?

What's the risk factor of these users?

03 Authentication Approach

Can you use SSO?

If local auth, how do we manage joiners/leavers?

02 Permissions System

How fine-grained can you make permissions?

Can you easily implement separation of duties/roles?

04 Secondary Auth Controls

Multi-factor authentication?

Conditional Access Policies?

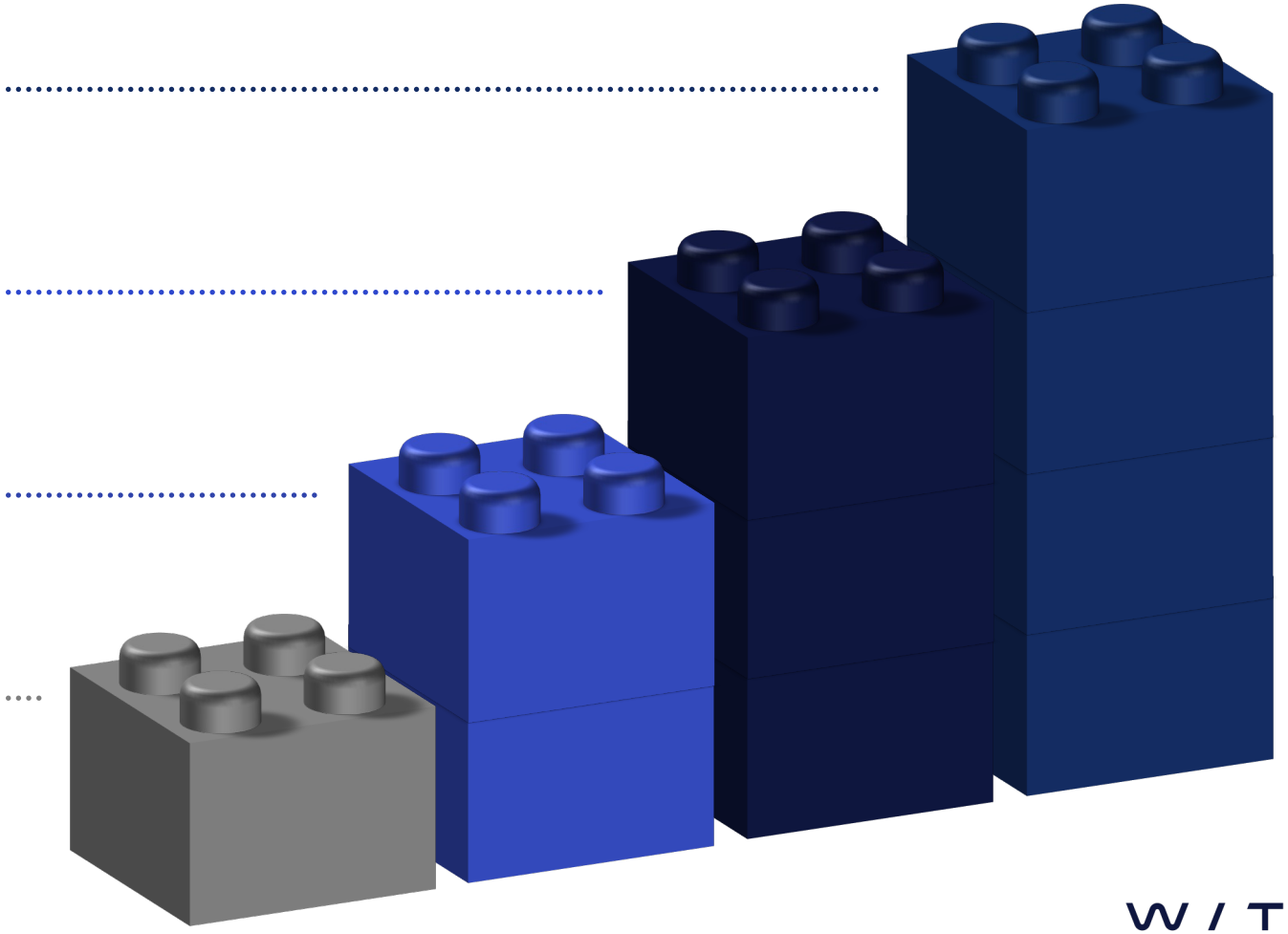
Resources

Application Purpose
Why has this been purchased, how is it used?

Types of Data
What types of data is the app storing? How critical is the data? What are the risks if stolen/tampered with?

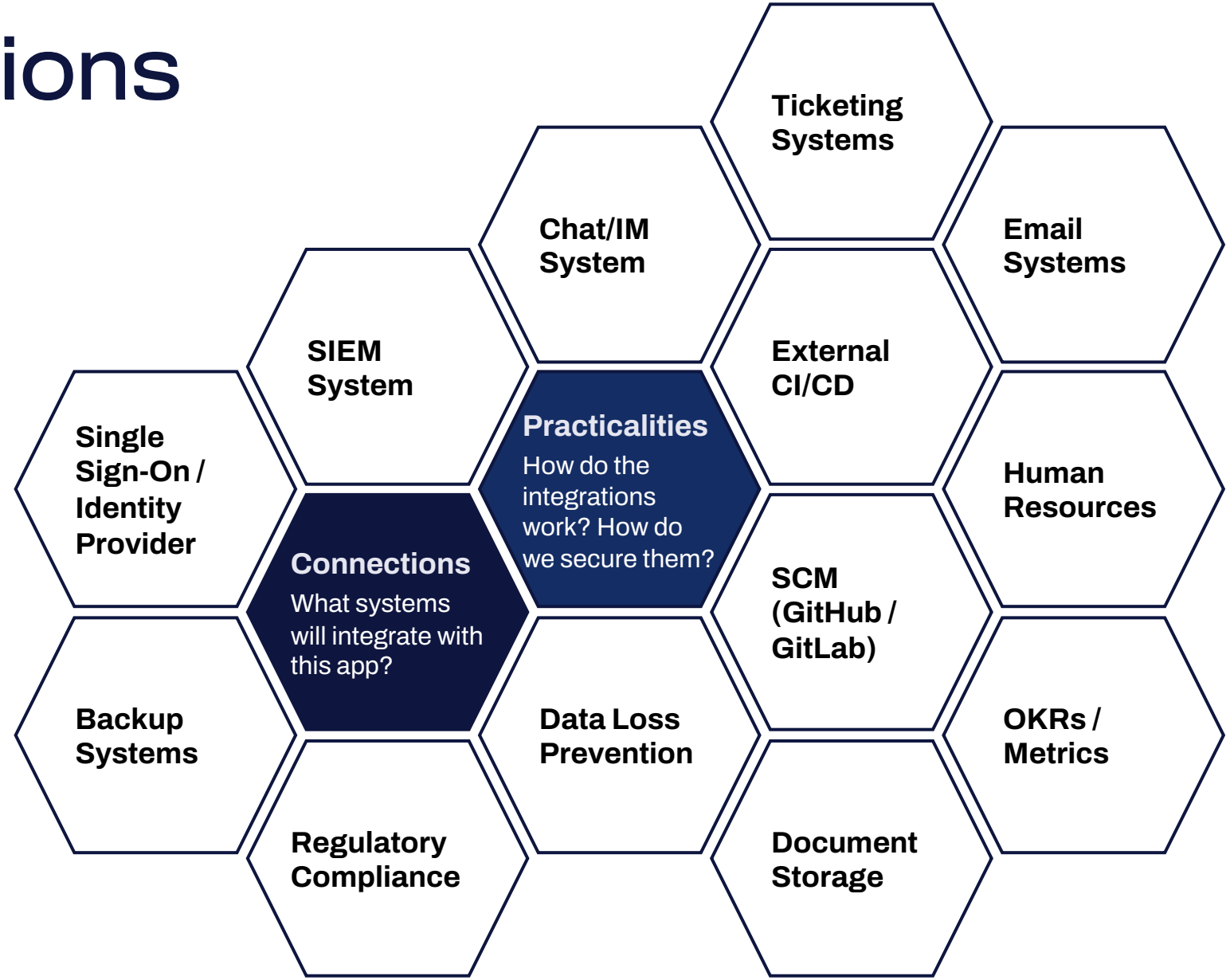
Data Storage
How does the data storage work? Is it encrypted? How? What access does the provider have?

Data Transmission
What protocols is the data accessed over? Where is the application expecting to send/receive data?



W / T H
secure

Integrations



W / T H
secure

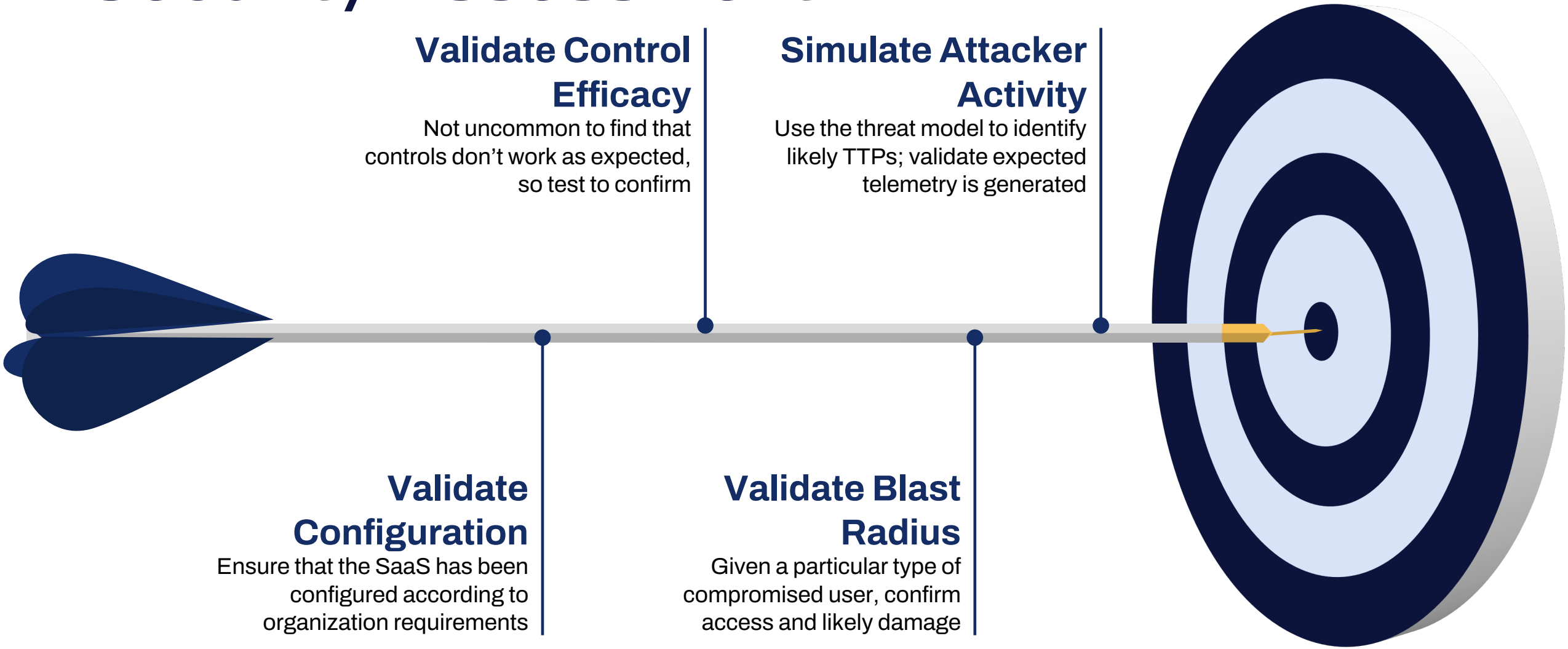
Security Assessment

Validate Control Efficacy

Not uncommon to find that controls don't work as expected, so test to confirm

Simulate Attacker Activity

Use the threat model to identify likely TTPs; validate expected telemetry is generated



Validate Configuration

Ensure that the SaaS has been configured according to organization requirements

Validate Blast Radius

Given a particular type of compromised user, confirm access and likely damage

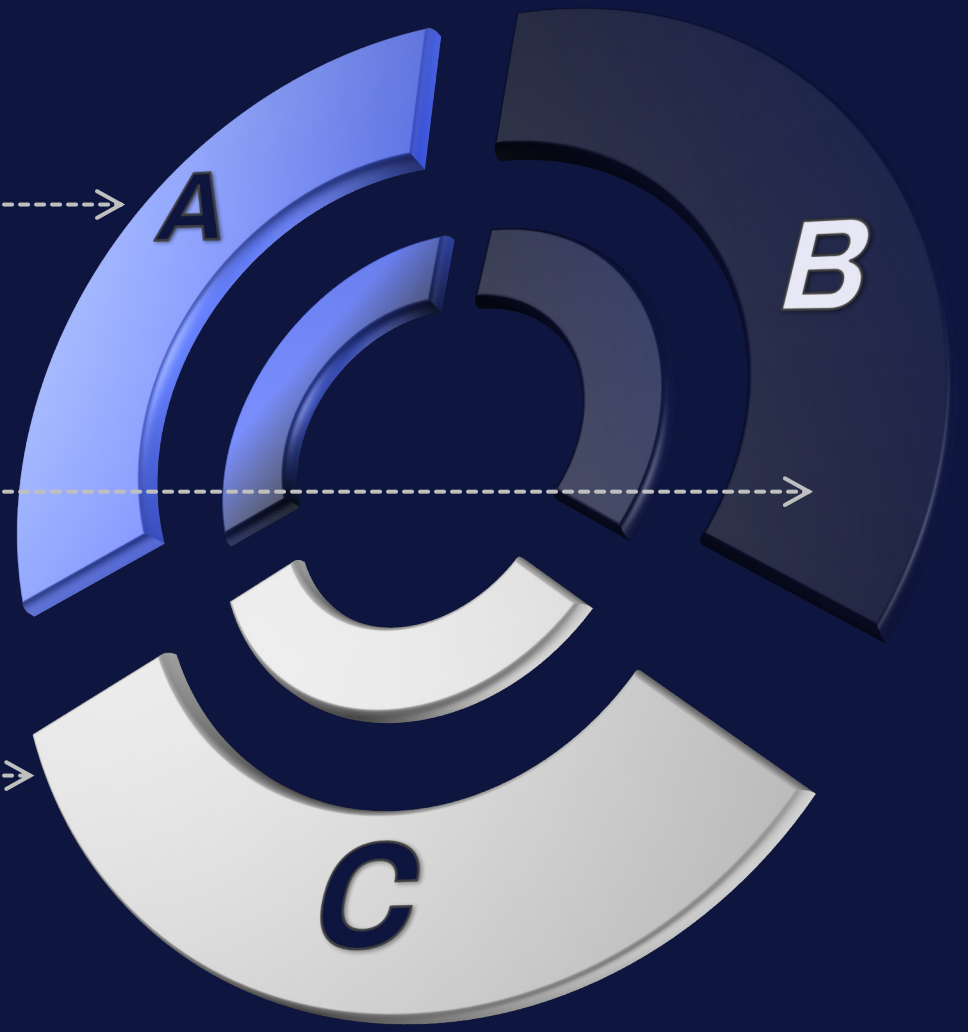
WITH secure

Process

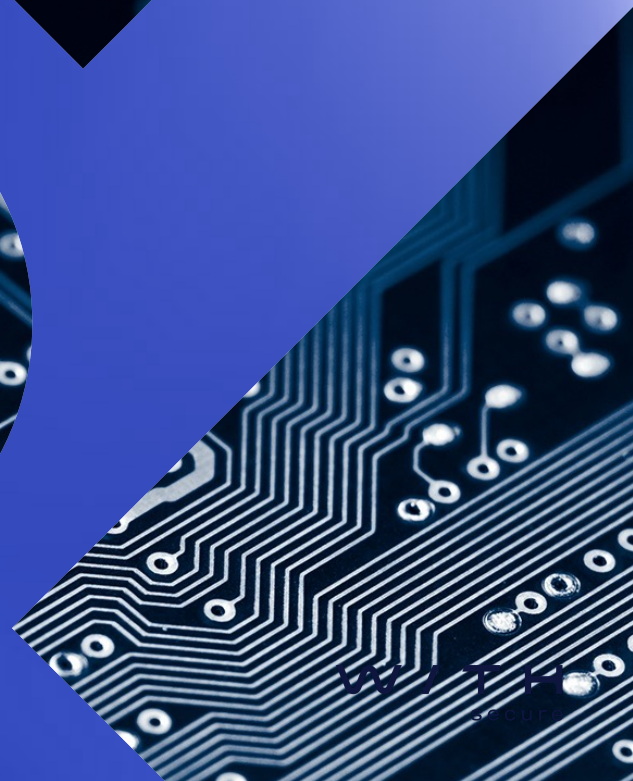
A IMPLEMENT DETECTIONS
Develop a set of use cases for the app, given the threat model

B SIMULATE ATTACKS
Execute TTPs from the threat model against the application

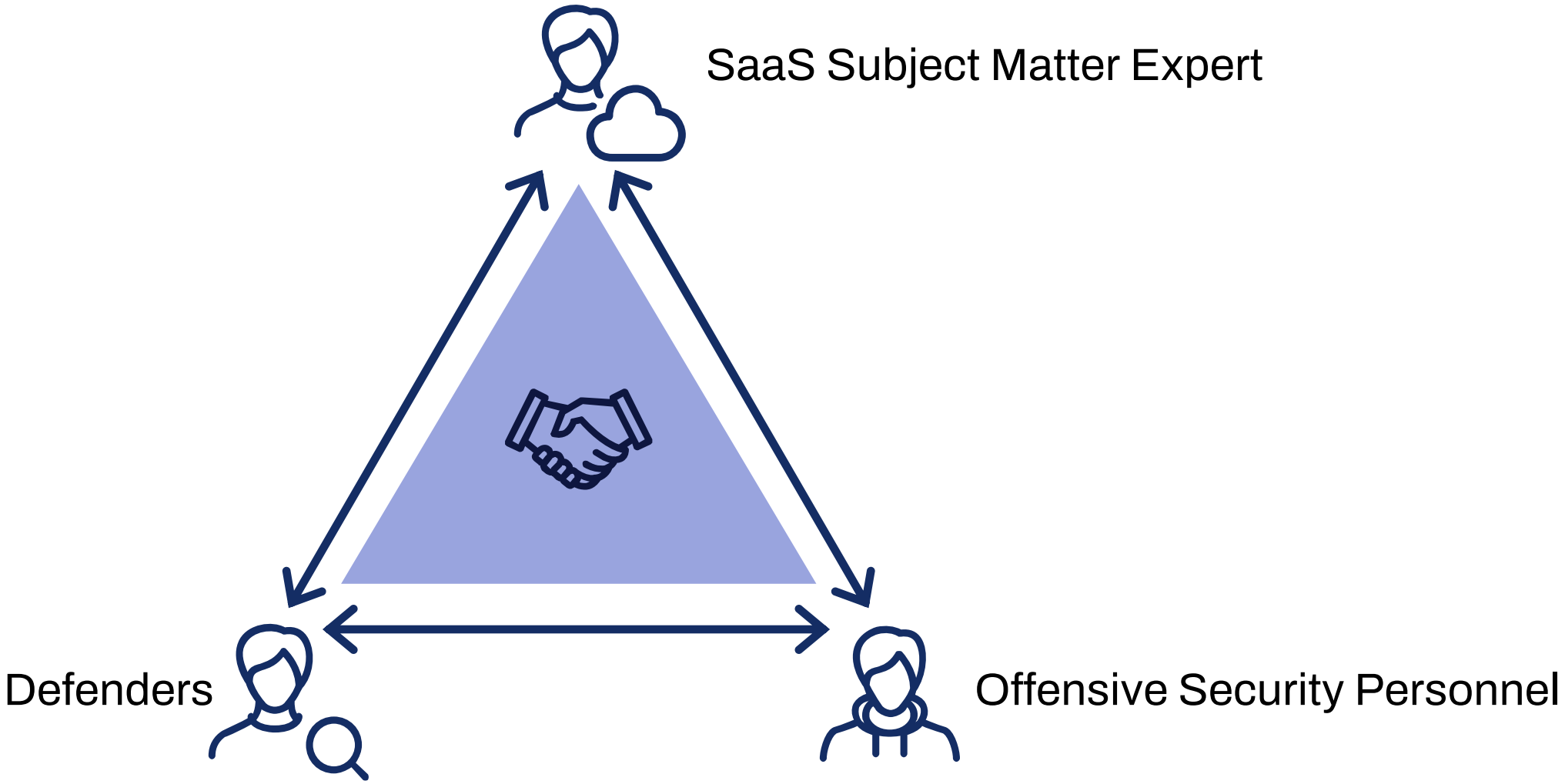
C EVALUATE RESULTS
Confirm detections behaved as expected, confirm necessary improvements or next detections to implement



Building Detection



Detection Collaboration



How to prioritise?

Use your risk models

- Are you a hospital? Start with patient data
- Payroll firm? Start with PII
- Tech firm? Software IP

Identity is the key

- If not sure where to start, begin with IdP
- For other systems, start with authentication use cases

What is the goal?

COMPROMISED CODEBASE

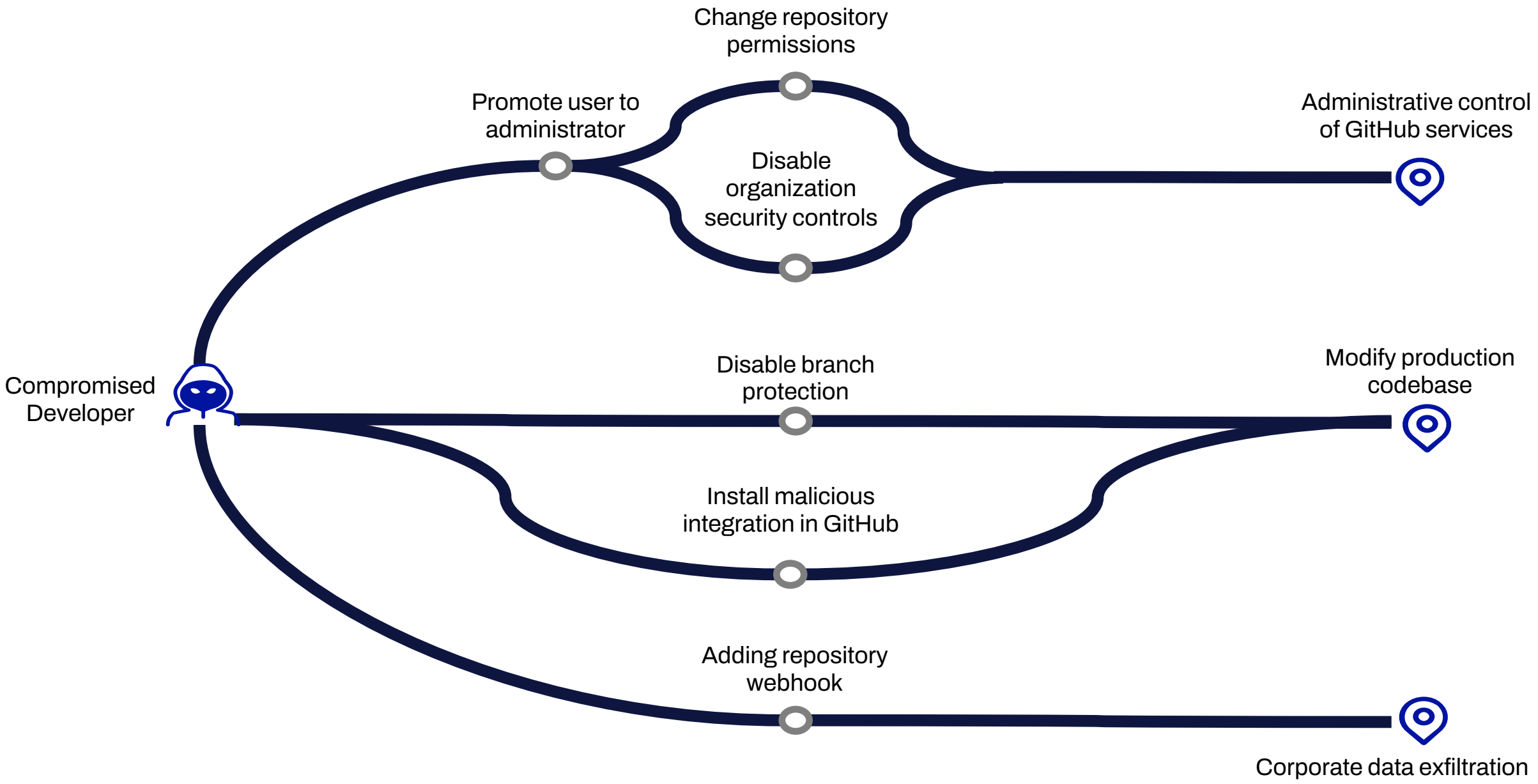
- Attacker has modified application codebase
- Attacker has modified Infrastructure-as-Code

SOCIAL MEDIA MANAGEMENT

- Attacker gains access to a Social Media Management app

COMPROMISED CI/CD PIPELINES

- Attacker has modified checks performed during a pipeline deployment


Change repository permissions
Promote user to administrator
Disable organization security controls
Administrative control of GitHub services
Compromised Developer
Disable branch protection
Modify production codebase
Install malicious integration in GitHub
Adding repository webhook
Corporate data exfiltration

WITH secure

On a scale of 1-10, how confident are you in your SaaS logging and monitoring?

Takeaways

Critical Data, Little Control

SaaS is unique in data criticality vs the data vs how little control and visibility is available

SaaS Detection is Nascent

Needs more research and investment, both from providers and client organizations

It’s a Team Effort

Combine offensive & defensive experience with product subject matter expertise for best effect

Some links

https://www.secwiki.cloud/saas/methodology

- High-level methodology for assessing SaaS applications

https://www.withsecure.com/en/expertise/resources/purple-teams-with-wings

- Paper from Nick Jones and Alfie Champion on purple teaming in the cloud

WITH®
secure

Twitter: @nojonesuk / @chrispy_sec