Delivering OFFENSIVE_INSIGHTS _to_the_Blue_Team

CornCon11

4dw@r3

CornCon11

Sean/4dw@r3

BurbSec Organizer

Senior Security Engineer

Dog Petter

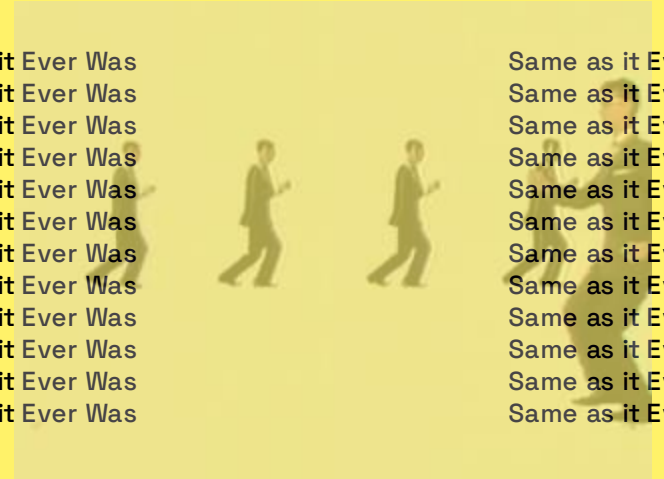
SOUNDCLOUD

Are you finding the same thing across each customers pentest?

Findings

Resolutions

THEY HAVEN'T FIXED THE FINDINGS FROM LAST YEAR! AGAIN!



So why do they keep asking for this?

Mandated by

Insurance

Regulation

Contracts

etc

Let’s help the Blue Team

Because they won’t do it themselves

I’ve heard this a lot!!

Between BurbSec, BSides, or at Def Con

The predictable isn’t interesting

Let’s work together!

Pen-tests shouldn’t be a formula

It’s the Blue Teams opportunity to explain *what* they need

So you can show their execs, *why* they need it

Help the Blue Team be tactical

Aid them picking a target, something broken but exec refuses to budget for

Show the client why it needs to be fixed

Strategic planning

You		They
Limit the Scope	Enumerate on it	Find the cost
Focus on a sticky issue	Discover specifically what goes wrong	Examine the actual business impact

Limit your scope

Find their ~~biggest~~ *best* target(s):

Bigger < Best
Likely > Flashy

Resolvable not the moon

Unless they desperately need the moon

Knowing their moon shoes

Something they know is either a massive undertaking or incredibly expensive

BUT

Could bankrupt the client if it's ignored

Enumerate on it

Find each business sector affected by the attack

One database could impact not just sales but also data, marketing, or FP&A

Each pivot could increase recovery time, impacting bottom line

Show me where it hurts

Their executives don’t care if a server gets ransomwared or a database breached

Show me where it hurts

They care if sales decrease, if subs drop, or click-through rates slow, etc

Revenue impacting events: RIE

Find the cost

Budget is spent on **revenue**, generating more of it or stopping the loss of it

Who predicts that? FP&A or Financial Planning & Analysis Departments

They've done 90% of this sections work already

Find the cost

FP&A know how much revenue is lost per hour per service

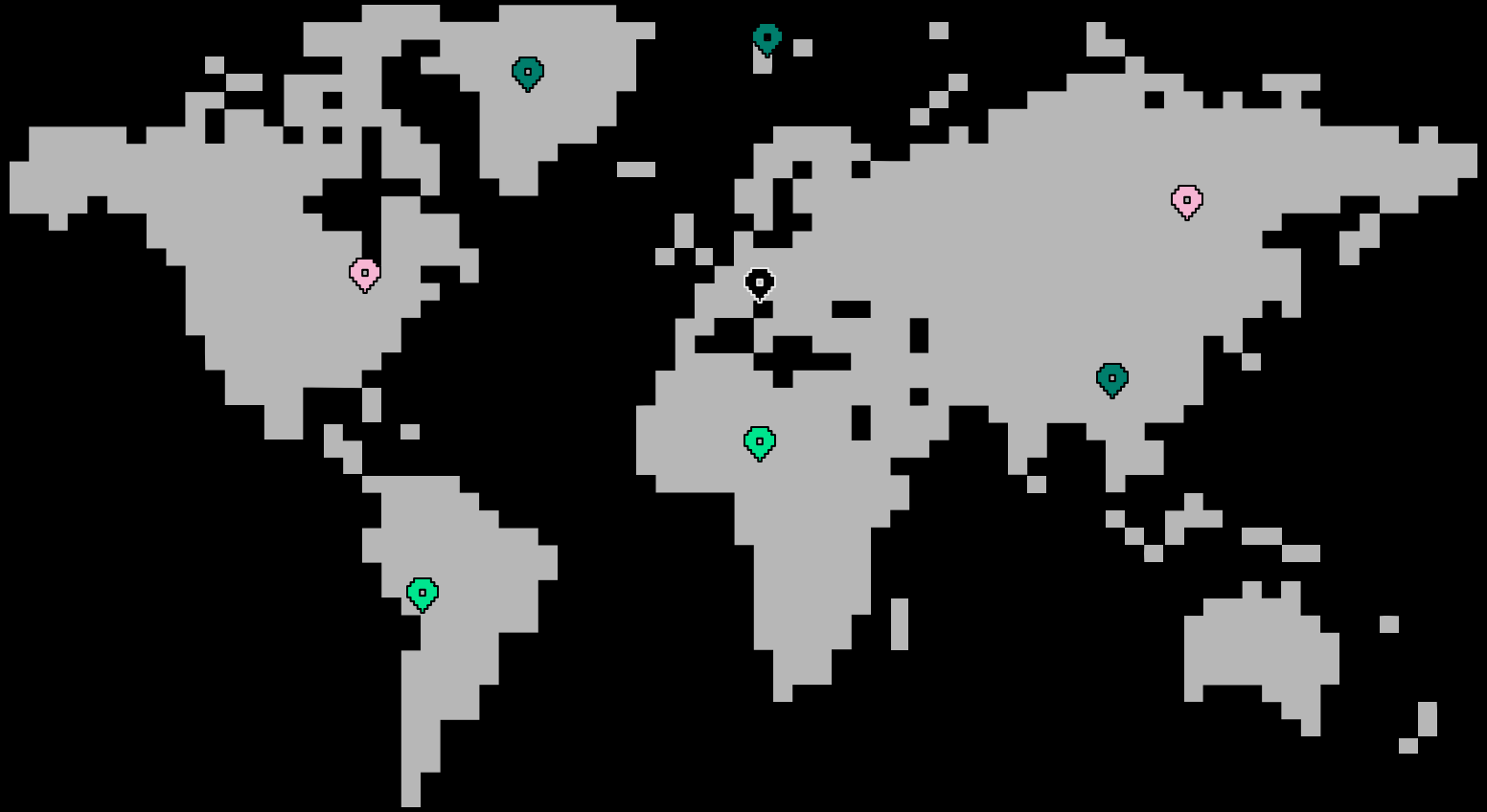
The client know the average time to get a service back up and running

Bring it to exec

The executive summary should include the business impacts and potential events

Send a internal supplement, what actions are needed and how much will it cost

AND how much it can cost if *they* don't budget appropriately



Thanks for listening!

Oh you had a question?

How do you actually get there and craft that plan with Blue Team Clients?

Clear communication of needs

Short-Links/orPhaned Services

Known issue for 8 years

Orphaned Service Backlog-Hell

Yes I know, you probably didn't become pentesters to use people skills

Clear communication

Gives you the opportunity

To level up your attacks

Get into more interesting issues

Are you here for the cutting edge or just a paycheck?

There is **nothing** wrong with being here for the check

Pre-Engagement

Define your goal

Close a risk

Staff for response

Defend PII

Scope the request

Specific service

Multi-service system

High impact infra

Target the impact

Prevent actual impact

Create RIE targets

Support the goal

Potential loss should exceed your goal

RIE vs Goal

If a revenue impacting event costs $110,000

And you need $95,000

Most executives will say no….

Shades of grey

White Box

Black Box

Grey Box

Finding your shade is a balancing act, ensure they can achieve your goal

The Pentesters Goal

Help you Find potential RIEs so you avoid a RGE

Pre-Engagement Readiness

- Read back the goals and objectives
- Establish clear boundaries/limits
- Prepare lines of communication
- Double check the scopes

The test

Don’t tell the Blue Team!

Remember the phases!

The Test

Phases:
Intelligence Gathering
Threat Modeling
Vulnerability Analysis
Exploitation
Post Exploitation

During engagement

Keep lines of communication ready

Stick to the planned level of ‘radio silence’

What a short section...

Keep track of what services/functions are hit

Document the unexpected

Post-attack huddle

Verify potential impact

Use targeted language

Note strengths

Client Verification

Verify how each machine service can effect app function

Account for secondary effects from linked processes

Diagram the chain of application effects

Diagram effects

Work with the client to craft a digestible diagram

Map your activity, to the ‘spectator view’ of business impact

Remind the client both staff and customer views

Stages of Cyber Attaick Rttailebsite

Scanning & Probing

Maintaian Access

- Twerermet Festing the customers

Reconnaissance

- Retail business
- Retail Business Eroger tre Wetail Crstoiners

Gaining Access

- Websing the
- Website's functions fnce customers

Covering Tracks

- Websing Pracks
- Website's functions the customers

Use targeted Language

Phrase key items for the audience

Every company has a dialect

Targeted Language

A hidden social engineer

Helps convey the message in familiar terms

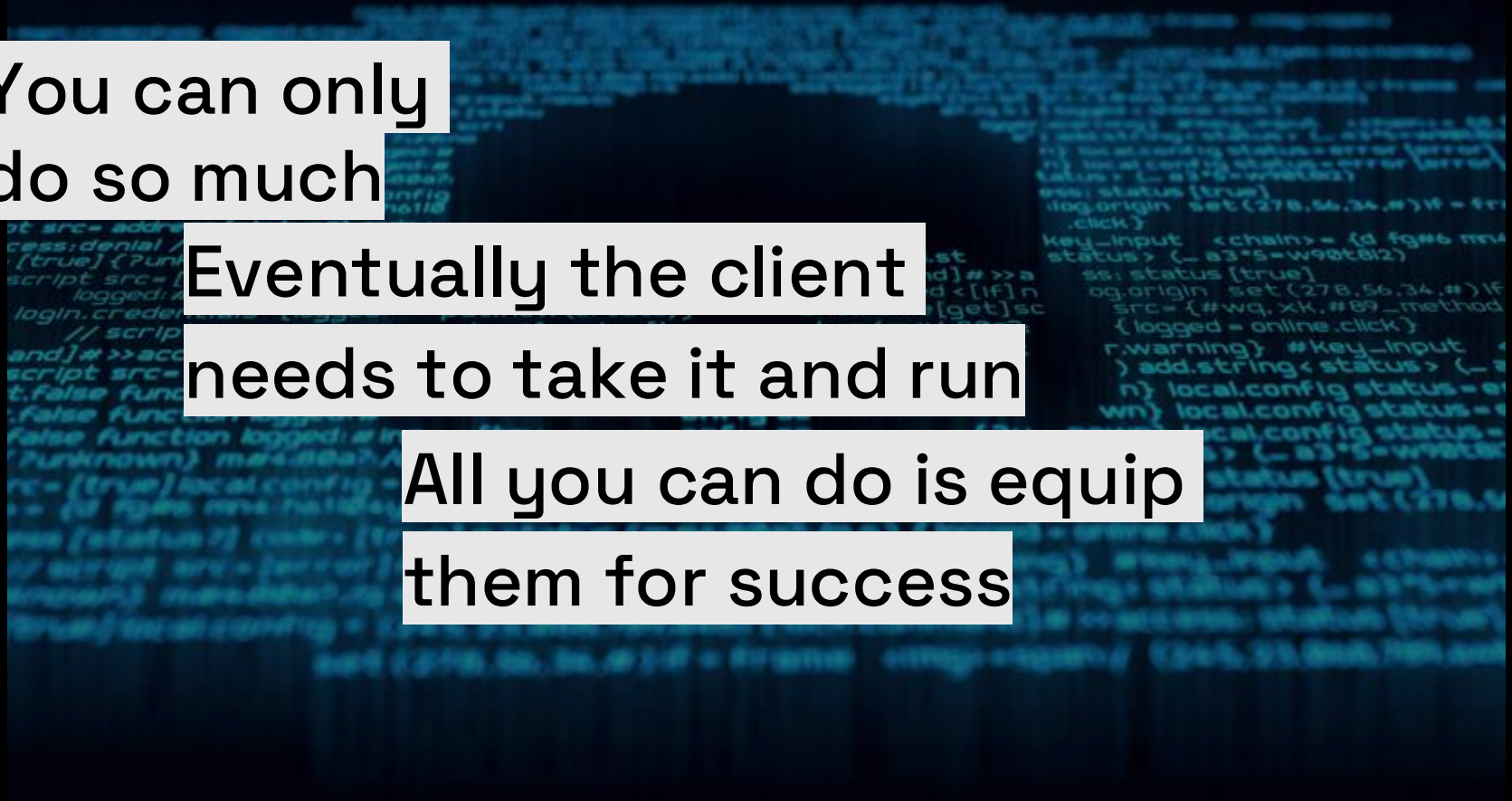
Note client strengths

Showcase positive feedback in the report

Doom and gloom, decreases appeal. Brag and Beg

‘You’re doing great, but need this as well…’

Wrap up the hunt



You can only do so much

Eventually the client needs to take it and run

All you can do is equip them for success

Questions?

SOUNDCLOUD

SOUNDCLOUD