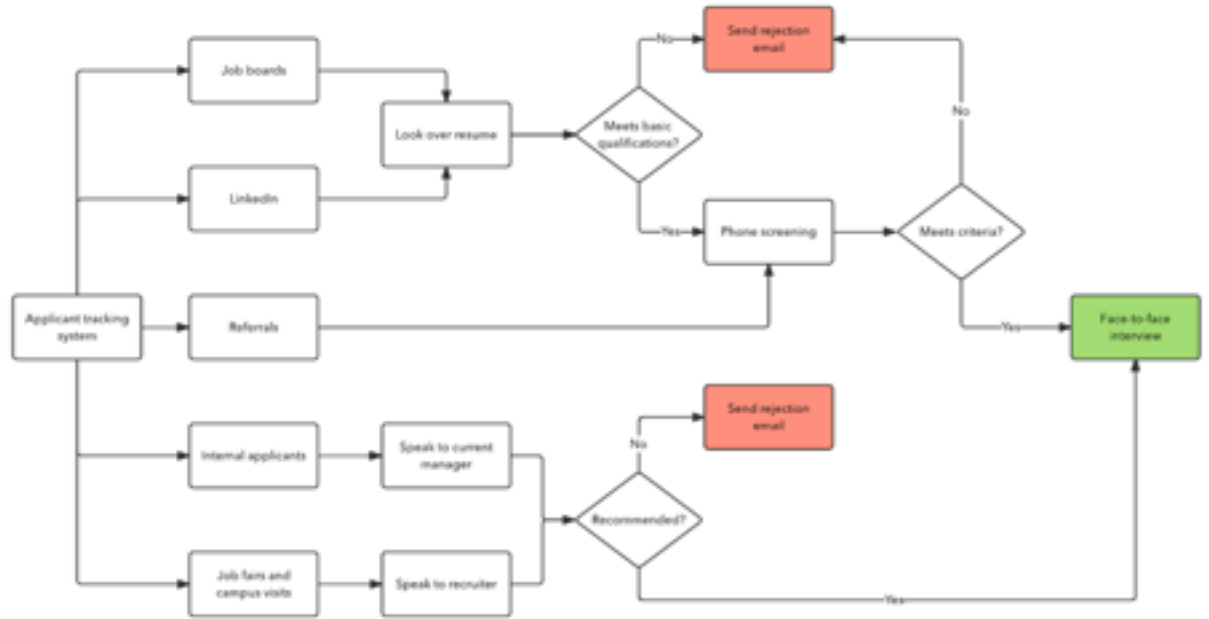# Improving the Quality of Your Cyber Security Hires via Pre-Interview Challenges
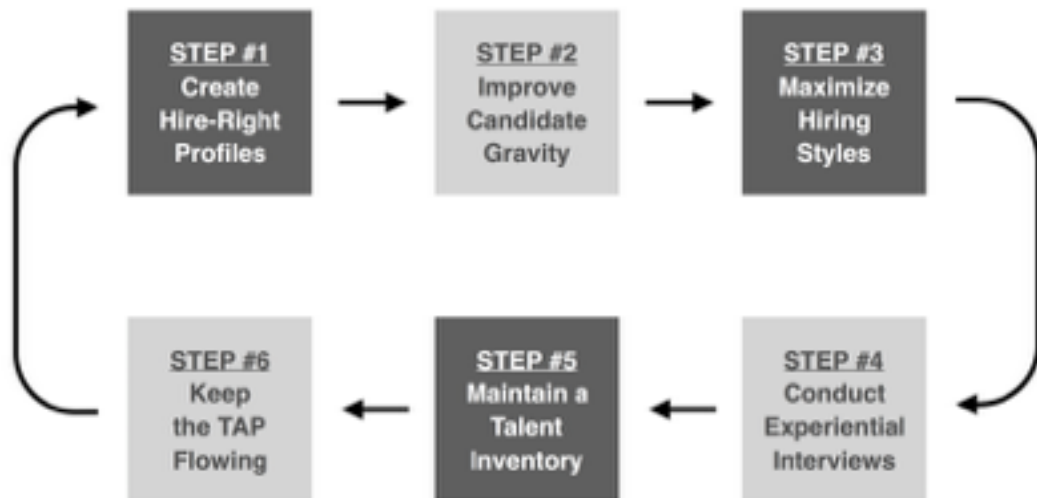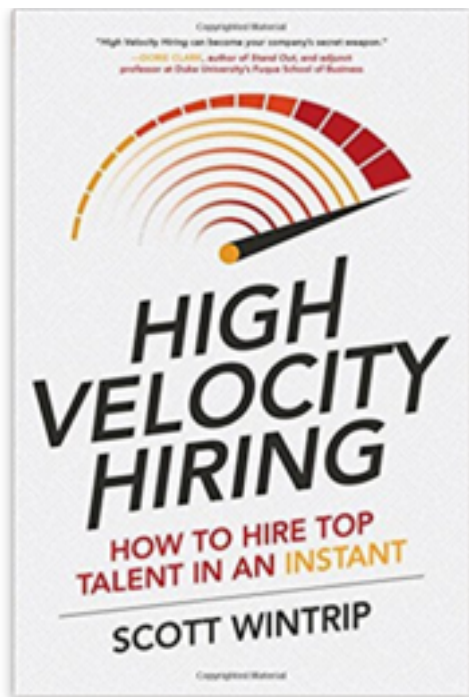
Dinis Cruz
CISO Photobox Group, 25th Jan 2017

The CV inefficient workflow

High Velocity hiring

STEP #1 Create Hire-Right Profiles → STEP #2 Improve Candidate Gravity → STEP #3 Maximize Hiring Styles → STEP #4 Conduct Experiential Interviews → STEP #5 Maintain a Talent Inventory → STEP #6 Keep the TAP Flowing → (cycle back to STEP #1)

How do you hire 6x senior highly skilful and motivated talent

Permanent Positions

Role
Head of AppSec
Head of Detect
Head of InfoSec
Head of Risk and Compliance
Head of SecOps
PosterXXL Information Security Officer
Senior Cloud Security Engineer

What we did

- We didn't want to do the normal recruitment process
- Photobox Group values are about shaking things and being innovative
- Opportunity to create a great experience for candidates and ourselves
- Win-win experience for all
- Create talent inventory

WE BELIEVE IN EACHOTHER

WE Shake THINGS Up

WE Win TOGETHER

• WE • MAKE • MAGIC • HAPPEN •

Proof that it is working

Hi James,

I wanted to thank you for the opportunity, but right now due to some things coming up I simply do not have time for these challenges. I think the fact I don't have time for the challenges is a good indicator that right now maybe this role isn't for me :-)

However, I wanted to feedback that this is one of the more interesting application processes I've seen - I think the challenges are excellent. I did a lot of research into PhotoBox Group Security before applying and it seems like a forward-thinking company that I would like to be a part of one day. The public-facing material such as the blog posts and the innovative challenges fit into what I would like to see coming from a company invested in the security industry (I'm bored of the norm I see at most companies I've interviewed with or looked into).

Although I will have to "take back" my application for now, I wanted to give you that feedback rather than ignoring your email or giving you a half-arsed "not interested" response. I will keep an eye on your careers page and potentially apply in the future once I've sorted some things out my end and am in a better position to apply.

Thanks again,
Gareth

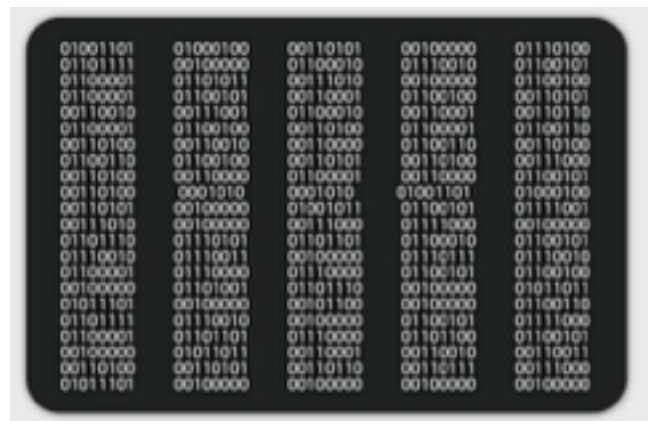the more interesting application processes I've seen - I think the challenges are excellent.

forward-thinking company

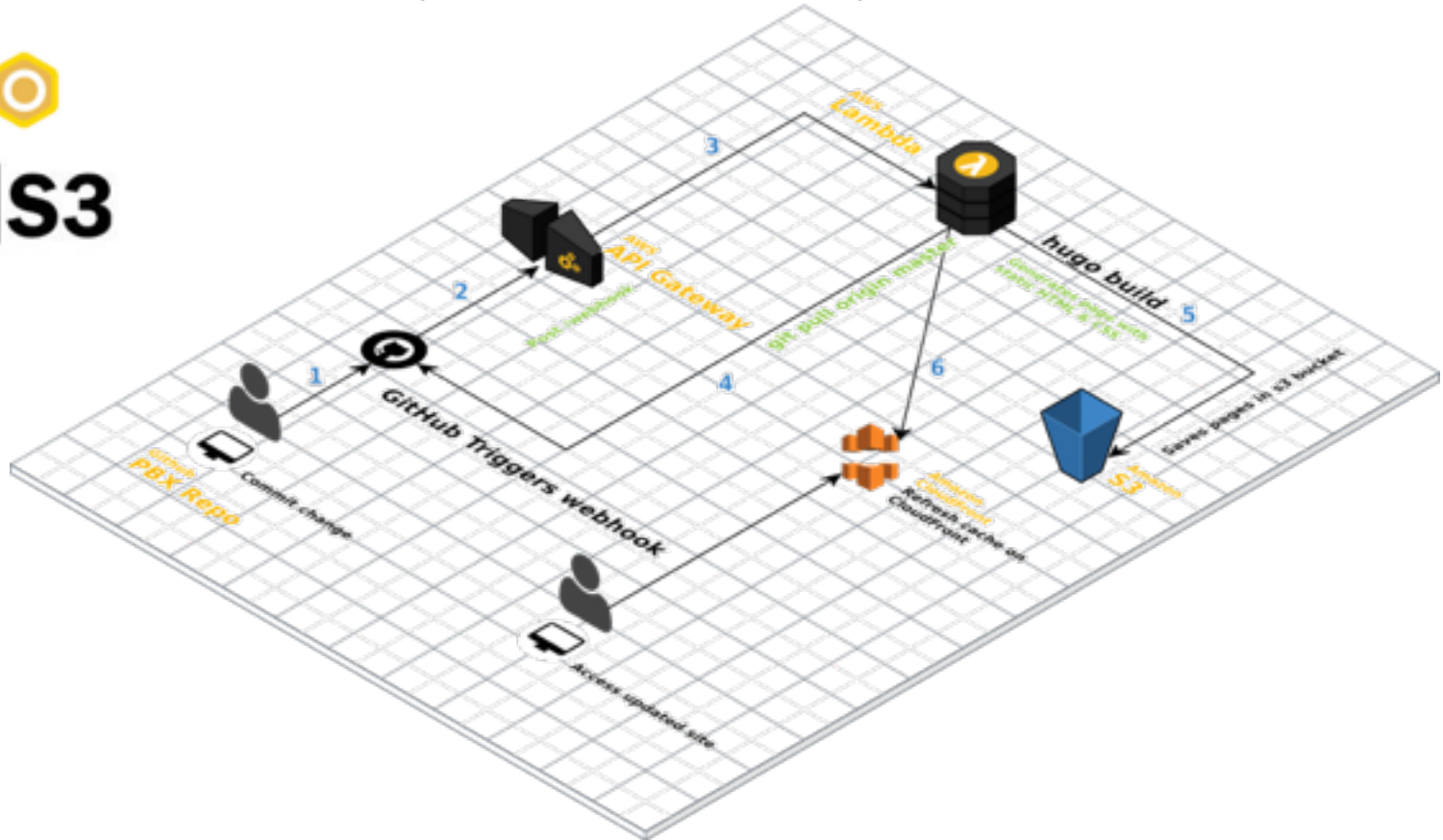to see coming from a company invested in the security industry

v1.0

photoboxgroup
security

We're hiring
Decrypt the code to access the
recruitment challenges

project-cx.com/ [enter 'flag']

project-cx@photobox.com

Project secureV0.2

v1.1

photoboxgroup
security

project-cx.com/ [enter 'flag']

project-cx@photobox.com

We're hiring
Decrypt the code to access the recruitment challenges

Next we created
https://pbx-group-security.com

All content:

All code:

open source

Static website created by and hosted by

photobox**group**
security

OUR MISSION

TO SECURE OUR CUSTOMERS' MAGIC MOMENTS ACROSS ALL OUR BRANDS

WE'RE HIRING

WHY WORK AT PHOTOBOX

BLOG

BLOGS

HOW WE THINK ABOUT SECURITY

IN **RECRUITMENT**   December 17, 2017

Our group of companies provide an incredible service for our customers, we work in a special space for them, helping them create something unique; a snapshot of a time and a place perhaps, the capturing of a memory, the gift that shows someone else how much they care for them. They trust us to be there for them and to protect those magical and intimate moments, it's something we are proud to take very seriously.

CONTINUE READING

WE NEED YOUR HELP

BY **DINIS CRUZ**   December 11, 2017

How can you help with the Group Security recruitment process? Group Security is currently recruiting for a number of new senior positions as well as short-term

SEARCH

Search   [🔍]

CATEGORIES

cybersecurity (1)

data-protection (1)

gdpr (1)

recruitment (2)

TAGS

🏷 **CISO**   🏷 **CTO**

CTO blog entry

DECEMBER 17, 2017

Our group of companies provide an incredible service for our customers, we work in a special space for them, helping them create something unique; a snapshot of a time and a place perhaps, the capturing of a memory, the gift that shows someone else how much they care for them. They trust us to be there for them and to protect those magical and intimate moments, it's something we are proud to take very seriously.

Every day we produce tens of thousands of unique and complex items, we ingest millions of photos into our sites and store them, we support hundreds of colleagues in multiple sites across Europe, our data set is at petabyte scale and we add terabytes more every day.

Our own technology enables every aspect of what we do for customers, from our web sites to our factories we rely on our engineering teams to build, maintain and evolve our services to cope with our growing customer base, the pace of our product evolution and our ever changing manufacturing capabilities.

SEARCH

Search

CATEGORIES

cybersecurity (1)

data-protection (1)

gdpr (1)

CISO blog entry

WHY JOIN PHOTOBOX GROUP SECURITY?

BY DINIS CRUZ | DECEMBER 11, 2017

The Photobox Group represents a really good opportunity for security professionals who want to make a difference and want to take their ideas to the next level. The security team within Photobox Group is in a really privileged position. We have support from all levels of the organisation:

- Board
- CTO
- Brand owners
- Even the developers and technologists on the ground

Everyone, within the group, understands security is important and we have to get it right. With great security actvities underway, there is an opportunity to take them to the next level.

What attracted me to work for Photobox Group was its environment, the ability to scale security and make a

Security team blogs (this one on GDPR history)

WARREN & BRANDEIS – THE RIGHT TO CURATE AN IDENTITY

BY ROBERT GRACE | DECEMBER 4, 2017

Warren & Brandeis: The Right to Curate an Identity

Mrs Warren's Profession

- No, not THAT Mrs Warren.
- Our Mrs Warren was a hostess and the problem started with what Mr Warren perceived as unwelcome and intrusive reportage on his wife's "at Homes" and his daughter's wedding.
- The sensational and salacious coverage outraged Warren and he consulted Brandeis on the matter of privacy and the law.

SEARCH

Search 🔍

CATEGORIES

cybersecurity (1)

data-protection (1)

WE'RE HIRING

JOIN OUR TALENTED, HIGH-FUNCTIONING TEAM

JOIN A MODERN SECURITY TEAM

We are recruiting for the following new roles within the Photobox Group Security team.

Here are some of the reasons you should join our team:

- How we think about Security
- Why join Photobox Group Security
- Why Challenges

For Recruiters

Photobox Group is not looking to work with recruitment agencies for any permanent roles listed on this site.

If you have any suitable candidates for the contract positions listed below please email us.

RECRUITMENT CHALLENGES

Please see below the links to the challenges that we have created for the different roles (we are adding more every day, so if the role you want to apply for is not there, keep an eye on this page).

See the Why Challenges? blog post for more thoughts on the concept of challenges.

See this page for All Challenges with skills information.

All Challenges (mapped by Area)

behaviours x3		
Title	Difficulty	key
Business Sense	hard	BE-BS
Flexibility	medium	BE-FL
Teamwork	medium	BE-TE

compliance x6		
Title	Difficulty	key
Assisting a DPO	hard	CO-AD
Boardroom Reporting and Dashboards	medium	CO-BR
Compliance Policy	hard	CO-CP
GDPR Action Plan	medium	CO-GP
PII Data Breach	medium	CO-PI
Working as a DPO	hard	CO-DP

management x6		
Title	Difficulty	key
Business Strategies	hard	MA-BS
Challenge of Recruiting	hard	MA-CR
Deliver Results Through Teamwork	expert	MA-DR
Develop and Attract Talent	hard	MA-TA
Improve on OWASP summit outcomes	hard	MA-OO
Role Model	expert	MA-RM

programming x5

Title	Difficulty	key
EC2 with Vulnerable Site	medium	PR-VS
Experience with Perl	medium	PR-EP
Graph-Based Schema	hard	PR-GS
Lambda - Stop EC2 Instances	hard	PR-LE
Programming Experience	medium	PR-PE

research x9

Title	Difficulty	key
Book Review	medium	RE-PB
FinTech	medium	RE-FT
Industry Awards	expert	RE-IA
Inspirational Leaders	hard	RE-TL
Inspirational Security	medium	RE-IS
Interesting Research	medium	RE-IR
Open Source vs Proprietary Software	medium	RE-OS
Presentation or Blog	medium	RE-PB
Training - Creation and Delivery	medium	RE-TR

risk x8

Title	Difficulty	key
Acceptable Use Policy	medium	RI-AU
GDPR Breach Notification to EU Regulator	expert	RI-BN
Gap Analysis	hard	RI-GA
JIRA Workflows	expert	RI-JW
Risk Assessment	hard	RI-RA
Risk Frameworks	hard	RI-RF
Risk Management and Acceptance	hard	RI-RM
Transformation Programmes	medium	RI-TP

security x5

Title	Difficulty	key
Avatao for photobox	expert	SE-AB
Bug Bounties	expert	SE-BB
Security Threats	expert	SE-ST
Testing Vulnerabilities	hard	SE-TV
Vulnerabilities Discovered	medium	SE-VD

setup x6

Title	Difficulty	key
Accounts Setup	medium	ST-AS
Pull Request	medium	ST-PR
Setup GitHub and Jekyll	medium	ST-GJ
Site Changes	medium	ST-AS
Write blog post	medium	ST-AS
Write blog post from transcription	medium	ST-BP

standards x4

Title	Difficulty	key
CBEST and CREST	hard	ST-CC
ISO Standards	expert	ST-TA
PCI DSS	medium	ST-PD
Standards Advisor	expert	ST-SA

technical x24

Title	Difficulty	key
AWS Root Key	expert	TE-AW
Authentication and Authorisation	medium	TE-AB

Real work scenarios

AWS ROOT KEY

key	difficulty	area
TE-AW	expert	technical

A legacy SVN server is found to be exposed on the internet Review of the source code identifies a number of secrets:

- Usernames and passwords of production DBs and Servers
- AWS key Upon review, the AWS key is active and has root privileges

Objective: Understand and contain issue(s) without any pushes to production

- You can use any technology you want (ideally ones you have experience with) and any Group Security team size
- Describe what you would do and how you would act (ideally in diagram format)
- Who would you talk to?
- What actions would you take to contain and remediate the issue(s)?

GDPR BREACH NOTIFICATION TO EU REGULATOR

key	difficulty	area
RI-BN	expert	risk

Write an GDPR breach notification letter to one of the EU Regulator (for example ICO in the UK) with a breach notification for (at least) one of the following scenarios:

- 1024 PhotoBooks and cards sent to the wrong recipient
- Customer's Usernames and Passwords available to download in S3 bucket (via exposed API key and Secret)
- HR system exposed sensitive employee data to internal employees
- Non-opted in customers received marketing communications
- ... Another scenario that you have personal/professional experience in...

Notes

- You have creative license to expand the chosen scenarios
- You can chose an EU Regulator from one of the four companies the Photobox Group operates (UK, France, Spain and Germany)
- It would be very interesting to see the same scenario sent to multiple regulators, where the differences between then would be highlighted

Test candidate's tech skills and CV claims

SETUP GITHUB AND JEKYLL

key	difficulty	area
ST-GJ	medium	setup

In order to respond to the challenges in a scalable and collaborative way, we ask candidates a Jekyll based website. which will be setup for you.

1. clone the repo https://github.com/project-cx/pbx-candidate-answers
   - if you are happy for your answers to be publicly available, you can just fork it
   - note that GitHub charges for private repos, but BitBucket doesn't
2. set-up dev/test environment (optional, but will help when writing content or modifying template)
   - if you are running locally, setup Jekyll to run the build (either on your host or us docker).
   - if you are running from GitHub, in your repo settings, set the master brach to ho

CBEST AND CREST

key	difficulty	area
ST-CC	hard	standards

Define your involvement with CBEST and CREST;

- Are you a CREST certified professional?
  - If so, which certification do you have? (and when did you take the exam
  - What was the most interesting part of the exam?
  - What was the most challenging part of the exam?
  - In which area of the exam did you excel?
  - In which area of the exam did you find difficult?
- What kind of CBEST/CREST engagements have you been involved in?

Permanent Positions

Role	Contract Type	Location	Apply
Head of AppSec	Permanent	London, Paris, Valencia or Munich	here
Head of Detect	Permanent	London, Paris, Valencia or Munich	here
Head of InfoSec	Permanent	London, Paris, Valencia or Munich	here
Head of Risk and Compliance	Permanent	London, Paris, Valencia or Munich	here
Head of SecOps	Permanent	London, Paris, Valencia or Munich	here
PosterXXL Information Security Officer	Permanent	Munich	here
Senior Cloud Security Engineer	Permanent	London, Paris, Valencia or Munich	here

Contract Positions

Role	Contract Type	Location	Apply
Perl Security Developer	Contractor	London, Paris, Valencia or Munich	here
SOC Engineer and Incident Response	Contractor	London and Remotely (2 to 5 days per week)	

Upwork

Role	Contract Type	Location	Apply
Technical Writer	Upwork	Remote (up to 20h week)	here

HEAD OF RISK AND COMPLIANCE

Contract Type	Location	Apply
Permanent	London, Paris, Valencia or Munich	here

The Role

As the Head of Risk and Compliance, you will work alongside the Group Security management team and act as an ambassador for PhotoBox Group's compliance culture and standards, enabling the highest standards of compliance with GDPR and PCI. You will advise the company on the impact of regulation on all aspects of the business, while creating a modern risk culture powered by real time risk visualisation and monitoring.

What will you do?

- Take overall responsibility for managing and developing PhotoBox Group's risk and compliance systems
- Advise in the creation and implementation of risk and compliance policies, regularly presenting issues and recommendations
- Ensure compliance with GDPR and PCI, and be the key point-of-contact for the four main EU Supervisory Authorities (UK, France, Spain and Germany)
- Take responsibility for all risk and compliance policies and complete annual reviews, proposing improvements to better manage risk
- Manage the further development of PhotoBox Group's risk assessment system, ensuring that each matter is managed and monitored by the appropriate system and that the various risk controls are populated
- Support investigations into any breaches – or potential breaches – and report on possible violations of, or legal jeopardy posed by, all regulations and statutes covering Photobox Group

Who are you?

- Well-versed in the range of risk management frameworks, including but not limited to operational, financial, data protection, and information security
- Strong understanding of emerging UK and European legislation, such as IDD and GDPR, codes of practice and industry guidelines potentially affecting the Photobox Group
- Able to form close working relationships and influence senior stakeholders
- Able to operate effectively within a fast-paced organisation.
- Educated to degree level (or equivalent)

Tech Stack

- GRC, ISMS, GDPR, PCI, ISO 27001
- Security Policies, Risk Management
- Risk Visualisation
- Python, R (language)

Challenges (required)

#1: Setup GitHub and Jekyll

key	difficulty	area
ST-GJ	medium	setup

In order to respond to the challenges in a scalable and collaborative way, we ask candidates to use a Jekyll based website. which will be setup for you.

1. clone the repo https://github.com/project-cx/pbx-candidate-answers
   - if you are happy for your answers to be publicly available, you can just fork it
   - note that GitHub charges for private repos, but BitBucket doesn't
2. set-up dev/test environment (optional, but will help when writing content or modifying the template)
   - if you are running locally, setup Jekyll to run the build (either on your host or using docker).
   - if you are running from GitHub, in your repo settings, set the master brach to host the GitHub pages site
3. add your answers as an entry to `_posts` folder (see examples)
4. push your changes to your repo
5. send us an email to project-cx@photobox.com

#2: Develop and Attract Talent

key	difficulty	area
MA-TA	hard	management

MA-TA-01
Describe a time when you had to give constructive feedback to a direct report that was not well received. How did you handle the situation?

MA-TA-02
Describe the steps you have taken to foster a positive team environment that encouraged your direct reports to do their best.

MA-TA-03
Describe a time when you transformed a struggling team member into a major contributor.

#3: Programming Experience

key	difficulty	area
PR-PE	medium	programming

How much programming experience do you have?

- What languages can you program in?
- What is your favorite language and why?
- How do you use those skills in real-work (business) situations

#4: Inspirational Leaders

key	difficulty	area
RE-TL	hard	research

Describe three inspirational leaders who you'd like to work for. They must be alive today.

- Tell us why you'd like to work for them
- Create a graph showing how you could get a job offer to work for them

#5: PII Data Breach

key	difficulty	area
CO-PI	medium	compliance

By the nature of the business, our servers host our customers images and personal information i.e. name, address, email address, etc.

The following are two possible scenarios:

- Photobox has discovered a data breach that has allowed millions of our customers images to be exposed online. These images were not available in the public domain and may contain photographs of children, elderly relatives and residential property
- Photobox has discovered a data breach that has allowed millions of our customers name, address, password and email address to be exposed online. There is no credit card or financial information within the data breach

Of these two scenarios, which do you deem to be the most serious and why?

Key Questions

- Which of the above constitutes PII data?
- Which of the above would you report to the ICO or relevant body?
- Would you contact the customers affected in both scenarios?

#6: PCI DSS

key	difficulty	area
ST-PD	medium	standards

Define your involvement with PCI/DSS;

- Have you been involved in a PCI/DSS certification process
- What are your views of this standard?
  - Current version vs original versions
  - What is new/interesting in the latest version?
- Where does PCI/DSS work?
  - Where doesn't it work?
  - What would you do better?
- Should PCI/DSS be a company wide standard for websites that handle customer data?

Challenges (optional)

#1: Role Model

key	difficulty	area
MA-RM	expert	management

MA-RM-01
Describe a time when you set a positive example that had a significant impact on peers or direct reports.

MA-RM-02
Describe a time when you motivated others through your commitment to delivering results.

MA-RM-03
Describe a time when you demonstrated to others the importance of taking accountability for business outcomes.

#2: Open Source vs Proprietary Software

key	difficulty	area
RE-OS	medium	research

Write a business, technical and moral case:

- for open source vs proprietary software
- for proprietary software vs open source

#3: JIRA Workflows

key	difficulty	area
RI-JW	expert	risk

Photobox Group Security uses JIRA for risk management and acceptance.

Our team, outputs and philosophy is based around graphs and workflows.

Below is a risk acceptance workflow, critique this workflow and tell us what you would do differently.

#4: Risk Management and Acceptance

key	difficulty	area
RI-RM	hard	risk

Photobox Group Security uses JIRA for risk management and acceptance.

- Which tools have you used to manage this process?
  - Was this your decision or a business led choice?

HEAD OF INFOSEC

Contract Type	Location	Apply
Permanent	London, Paris, Valencia or Munich	here

The Role

As the Head of Infosec you will support the CISO with the management of the Group Security function, including all information systems related to customers, product, factory, compliance, audit, physical, and staff security.

You will be responsible for driving the Group's enterprise security and risk management vision, strategy and programme to ensure protection of information assets and technologies. You will lead in the creation of an accountable, information security-conscious culture and a system security architecture built on high-quality standards, as well as regular status monitoring and quality reporting activities.

What will you do?

- Consult, approve and/or validate existing business strategic directions and investment plans as they relate to the protection of systems and data
- Get the big information security risk management picture including third parties, service providers, and integrating with internal control, compliance, and risk management functions
- Setting strategic direction
- Ensuring the privacy and protection of Personally Identifiable Information (PII) of customers and employees
- Management of IT investigations, digital forensics, e-discovery, breach response, and reaction plan responsibilities
- Information Risk Management standards and practical application using recognised standards (ISO, NIST, etc.)
- Information Security Management System (ISMS) designed to ensure comprehensive and documented assurance relevant to the organisation
- Represent the Group as the authority for security and controls to clients and customers, partners, competitors, auditors, regulators and internal stakeholders
- Line management of sub-teams within the group security team
- Liaise with brands under Photobox Group to support security and compliance processes
- Support the creation of KPIs for OKR setting
- Ensure recurring processes are documented, recorded, and evidenced by relevant teams/staff
- Present to SMT/Exec on security-related concerns/developments on a regular basis

Who are you?

- Strong technical knowledge

#4: Training - Creation and Delivery

key	difficulty	area
RE-TR	medium	research

Provide details of training that you have delivered recently

- what was the subject matter?
- how many people did you train?
- how did you prepare for this training? i.e. did you produce materials and handouts? Did you use visual aids? etc.
- If you could do this training session again, what would you do differently?

#5: Programming Experience

key	difficulty	area
PR-PE	medium	programming

How much programming experience do you have?

- What languages can you program in?
- What is your favorite language and why?
- How do you use those skills in real-work (business) situations

#6: Vulnerabilities Discovered

key	difficulty	area
SE-VD	medium	security

What kind of vulnerabilities have you discovered in real-word applications?

- How did you find them?
- How did you report them?
- Did you write tests/PoCs that the developers could use to replicate the issue?
- Did you received a bug-bounty payment for them?

Challenges (optional)

#1: Deliver Results Through Teamwork

key	difficulty	area
MA-DR	expert	management

MA-DR-01
Describe a time when you had to translate an organisational strategy into concrete deliverables that resulted in positive business outcomes.

MA-DR-02
Describe a time when your team's workload was unbalanced. How did you prioritise and delegate the work?

#2: PII Data Breach

key	difficulty	area
CO-PI	medium	compliance

By the nature of the business, our servers host our customers images and personal information i.e. name, address, email address, etc.

The following are two possible scenarios:

- Photobox has discovered a data breach that has allowed millions of our customers images to be exposed online. These images were not available in the public domain and may contain photographs of children, elderly relatives and residential property
- Photobox has discovered a data breach that

#3: Risk Rating

key	difficulty	area
RI-RR	hard	

How would you define a system for risk rating?

Have you used one in the past?

- What worked
- what didn't work?
- How did that solution scale?

All content in Markdown and managed at **GitHub**

⊙ Unwatch ▾ 22   ★ Star 3   ⑂ Fork 21

<> **Code**   ⓘ Issues **64**   ⧠ Pull requests **30**   ⊞ Projects **7**   ▥ Wiki   ⊪ Insights   ⚙ Settings

Content for PBX Group Security website   https://pbx-group-security.com/   Edit

Add topics

⊙ **1,287** commits	⑂ **8** branches	⬱ **1** release	⬚ **17** contributors	⚖ Apache-2.0

Branch: master ▾   New pull request   Create new file Upload files Find file **Clone or download ▾**

📌 **JemmaDSmith** Update working-sessions.md   Latest commit 6a5979a an hour ago

📁 .vscode	added vscode worspace config for everyone to use with defualt to 2 sp...	11 days ago
📁 bin	commit for github push	13 days ago
📁 content	Update working-sessions.md	an hour ago
📁 data	Update 4.yaml	29 days ago
📁 i18n	fix issue 88	a month ago
📁 layouts	- Added events shortcode for the Working Sessions page	a day ago
📁 src	- Added events shortcode for the Working Sessions page	a day ago
📁 static	- Added events shortcode for the Working Sessions page	a day ago
📄 .gitignore	updated .gitignore to also have the .idea folder	23 days ago
📄 CONTRIBUTING.md	Update CONTRIBUTING.md	a month ago

The challenge file (note the file name)

pbx-group-security / content / challenges / technical / TE-DA-darktrace-alert.md 📋 or cancel

<> Edit file   ⊙ Preview changes   Spaces ⬍   2 ⬍   Soft wrap ⬍

```
 1  ---
 2  title      : Darktrace Alert
 3  key        : TE-DA
 4  area       : technical
 5  difficulty : hard
 6  skills     : Briefing, Analysis, Planning
 7  ---
 8
 9  DarkTrace (AI-based network IDS) raises an alert caused by the download of an unknown executable by a user with administrator
    privileges. Further analysis of DarkTrace logs for the affected device shows unusual network activity.
10
11  Describe how you would proceed to achieve the same understanding in TechOps, DevOps, Business, and Management.
12
13  *Bonus points for mapping what could be the possible malicious and non-malicious (benign) root cause of this incident*
14
15  **Objective: Understand and contain issue(s) without any pushes to production**
16
17  * You can use any technology you want (ideally ones you have experience with) and any Group Security team size
18  * Describe what you would do and how you would act (ideally in diagram format)
19  * Who would you talk to?
20  * What actions would you take to contain and remediate the issue(s)?
```

The role file (note the content as metadata)

pbx-group-security / content / roles / contract / `soc-engineer.md`

Contract Type	Location
Contractor	London and Remotely (2 to 5 days per week)

<> Edit file   ⊙ Preview changes

```
1   ---
2   title            : SOC Engineer and Incident Response
3   layout           : role
4   date             : 2017-12-06
5   contract_type    : Contractor
6   location         : London and Remotely (2 to 5 days per week)
7   apply_Link       :
8
9   what_will_you_do:
10      - You will be responsible for initial analysis/investigation of data an
    day-to-day basis.
11      - The role requires you to have previous experience of working in a SOC
    define and build monitoring and detection capabilities.
12
13  who_are_you:
14      - Knowledge of AlertLogic and AlienVault or Elastic Stack/ELK
15      - AWS Security
16      - Experience of Security Information & Event Management (SIEM)
17      - Experience in Akamai Kona (WAF), monitoring and writing rules
18      - Experience in creating and deploying AWS WAF rules powered by Lambda(
19      - Experience in creating network diagrams (ideally from code/data)
20      - Programming experience (Python, JavaScript or Bash)
```

The Role

Help us define, manage, and expand our day-to-day operations within our e
SOC. Handle Security incidents and help to fix root causes.

What will you do?

- You will be responsible for initial analysis/investigation of data and t
  escalation and management of incidents on a day-to-day basis.
- The role requires you to have previous experience of working in a SO
  along with hands-on experience in helping to define and build monito
  and detection capabilities.

Who are you?

- Knowledge of AlertLogic and AlienVault or Elastic Stack/ELK
- AWS Security
- Experience of Security Information & Event Management (SIEM)
- Experience in Akamai Kona (WAF), monitoring and writing rules
- Experience in creating and deploying AWS WAF rules powered by
  Lambda(s)
- Experience in creating network diagrams (ideally from code/data)

Challenges mapping is easy

```
24  tech_stack:
25      - AlertLogic and AlienVault or Elastic Stack/ELK
26      - AWS, Akamai, WAF, Lambda
27      - Risk Visualisation
28      - Python, Javascript, Bash
29      - Kibana, Grafana or Nagios
30
31  challenges_required:
32      - ST-SA-github-and-jekyll.md
33  #   - CP-CB-collaboration.md
34      - PR-LE-lambda-stop-ec2.md
35      - SC-VD-vulnerabilities-discovered.md
36      - PR-PE-programming-experience.md
37      - RE-IR-interesting-research.md
38
39  challenges_optional:
40      - TE-LA-log-analysis.md
41      - PR-VS-ec2-with-vuln-site.md
42      - TE-DB-dashboards.md
43  #   - CP-PL-planning.md
44      - TE-DA-darktrace-alert.md
45      - TE-AW-aws-root-key.md
46
```

Challenges (required)

#1: Setup GitHub and Jekyll		
key	difficulty	area
ST-GJ	medium	setup

In order to respond to the challenges in a scalable and collaborative way, we ask candidates to use a Jekyll based website, which will be setup for you.

1. clone the repo https://github.com/project-cs/jobs-candidate-answers
   - if you are happy for your answers to be publicly available, you can just fork it
   - note that GitHub charges for private repos, but BitBucket doesn't
2. set up dev/test environment (optional, but will help when writing content or modifying the template)
   - if you are running locally, setup Jekyll to run the build (either on your host or using

#2: Lambda - Stop EC2 instances		
key	difficulty	area
PR-LE	hard	programming

Create Lambda function to;
   - Show a list of running instances (all regions and metadata)
   - Stop EC2 instances that have not been accessed for a period of time or have a low CPU usage
   - Setup an Elastic (ELK) Stack, feed logs and create a dashboard.

#3: Vulnerabilities Discovered		
key	difficulty	area
SE-VD	medium	security

What kind of vulnerabilities have you discovered in real-word applications?
   - How did you find them?
   - How did you report them?
   - Did you write tests/PoCs that the developers could use to replicate the issue?
   - Did you received a bug bounty payment for them?

Customised candidates page

Candidate answers provided via Hugo site
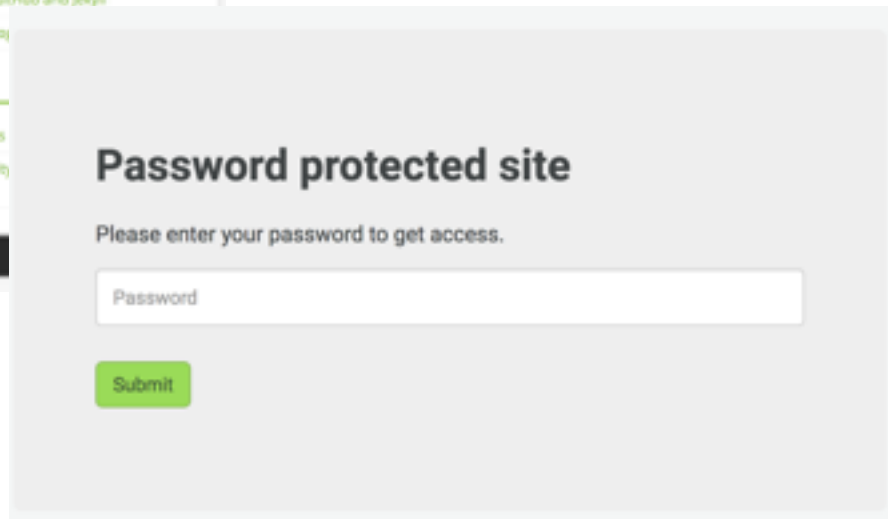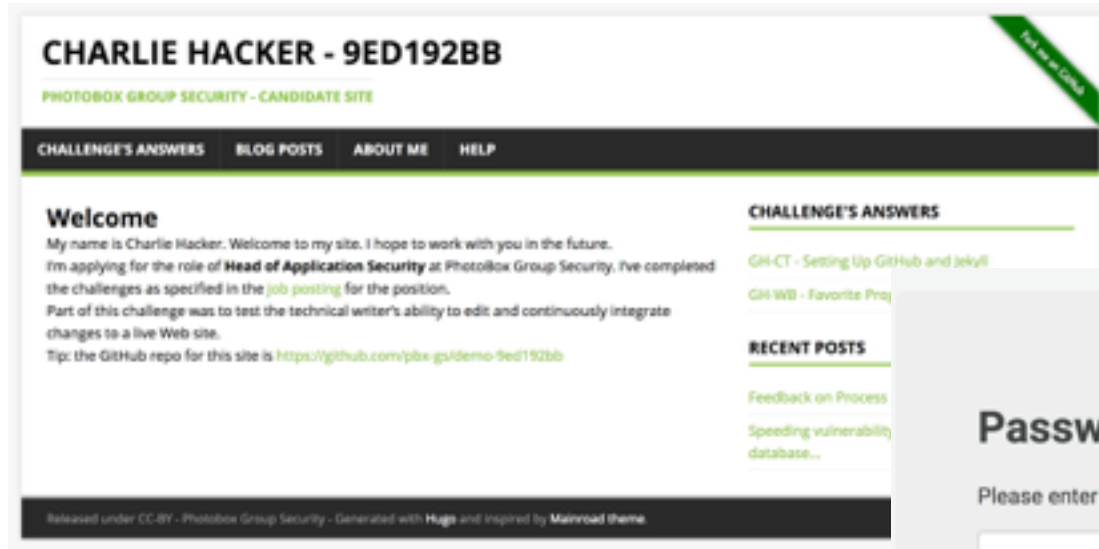
Using Netlify for Candidates website's CI
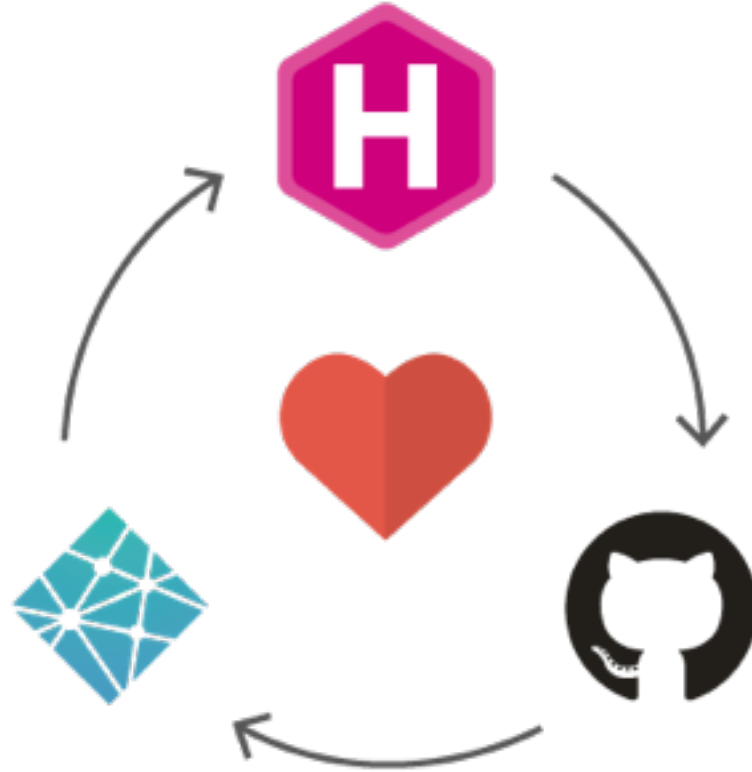
WORKING SESSIONS

Photobox Group, working with OWASP London Chapter, is hosting a number of working sessions to continue the great work done at the OWASP Summit 2017, and collaborate and share our knowledge on the following themes;

- Playbook common format
- SAMM
- GitHub security feature request
- GDPR and DPO AppSec implications

If you have a session idea email your suggestion to us

Book your place now

February	March	March	April
20	6	20	3

Latest research and capabilities on this repo