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

1. Create Hire-Right Profiles
2. Improve Candidate Gravity
3. Maximize Hiring Styles
4. Conduct Experiential Interviews
5. Maintain a Talent Inventory
6. Keep the TAP Flowing
How do you hire 6x senior highly skilled and motivated talent
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
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
RECRUITMENT PROCESS

1. First challenge is delivered to candidates house
2. Candidate is motivated by challenge
3. Solves on table or desk
   - Solution
4. URL 1
   - Enters the flag
5. URL 2
   - Solution is a FLAG (key)
6. URL 3
7. OWASP Working Sessions across Table
8. Face to face meetings
9. Job offer
We’re hiring
Decrypt the code to access the recruitment challenges

project-cx.com/ enter ‘flag’

project-cx@photobox.com

v1.0

v1.1
Next we created https://pbx-group-security.com

All content: 

All code: 

[open source logo]
Static website created by and hosted by
OUR MISSION

TO SECURE OUR CUSTOMERS' MAGIC MOMENTS ACROSS ALL OUR BRANDS
HOW WE THINK ABOUT SECURITY IN RECRUITMENT

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.

WE NEED YOUR HELP

BY DINIS CRUZ

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 placements. If you or someone you know has the skills and experience we're looking for, we'd love to hear from you.

SEARCH

Categories

cybersecurity (1)
data-protection (1)
gdpr (1)
recruitment (2)

Tags

ciso
cto
HOW WE THINK ABOUT SECURITY

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.
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 activities 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 difference.
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.
WE'RE HIRING

JOIN OUR TALENTED, HIGH-FUNCTIONING 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.
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)

<table>
<thead>
<tr>
<th>behaviours</th>
<th>Title</th>
<th>Difficulty</th>
<th>key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Sense</td>
<td>hard</td>
<td>BE-BS</td>
<td></td>
</tr>
<tr>
<td>Flexibility</td>
<td>medium</td>
<td>BE-FL</td>
<td></td>
</tr>
<tr>
<td>Teamwork</td>
<td>medium</td>
<td>BE-TE</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>compliance</th>
<th>Title</th>
<th>Difficulty</th>
<th>key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assisting a DPO</td>
<td>hard</td>
<td>CO-AD</td>
<td></td>
</tr>
<tr>
<td>Boardroom Reporting and Dashboards</td>
<td>medium</td>
<td>CO-BR</td>
<td></td>
</tr>
<tr>
<td>Compliance Policy</td>
<td>hard</td>
<td>CO-CP</td>
<td></td>
</tr>
<tr>
<td>GDPR Action Plan</td>
<td>medium</td>
<td>CO-GP</td>
<td></td>
</tr>
<tr>
<td>PIi Data Breach</td>
<td>medium</td>
<td>CO-PI</td>
<td></td>
</tr>
<tr>
<td>Working as a DPO</td>
<td>hard</td>
<td>CO-DP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>management</th>
<th>Title</th>
<th>Difficulty</th>
<th>key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Strategies</td>
<td>hard</td>
<td>MA-BS</td>
<td></td>
</tr>
<tr>
<td>Challenge of Recruiting</td>
<td>hard</td>
<td>MA-CR</td>
<td></td>
</tr>
<tr>
<td>Deliver Results Through Teamwork</td>
<td>expert</td>
<td>MA-DR</td>
<td></td>
</tr>
<tr>
<td>Develop and Attract Talent</td>
<td>hard</td>
<td>MA-TA</td>
<td></td>
</tr>
<tr>
<td>Improve on OWASP summit outcomes</td>
<td>hard</td>
<td>MA-00</td>
<td></td>
</tr>
<tr>
<td>Role Model</td>
<td>expert</td>
<td>MA-RM</td>
<td></td>
</tr>
<tr>
<td>programming</td>
<td>Difficulty</td>
<td>key</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>------------</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td>EC2 with Vulnerable Site</td>
<td>medium</td>
<td>PR-VS</td>
<td></td>
</tr>
<tr>
<td>Experience with Perl</td>
<td>medium</td>
<td>PR-EP</td>
<td></td>
</tr>
<tr>
<td>Graph-Based Schema</td>
<td>hard</td>
<td>PR-GS</td>
<td></td>
</tr>
<tr>
<td>Lambda - Stop EC2 Instances</td>
<td>hard</td>
<td>PR-LE</td>
<td></td>
</tr>
<tr>
<td>Programming Experience</td>
<td>medium</td>
<td>PR-PE</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>research</th>
<th>Difficulty</th>
<th>key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Book Review</td>
<td>medium</td>
<td>RE-PB</td>
</tr>
<tr>
<td>FinTech</td>
<td>medium</td>
<td>RE-FT</td>
</tr>
<tr>
<td>Industry Awards</td>
<td>expert</td>
<td>RE-IA</td>
</tr>
<tr>
<td>Inspirational Leaders</td>
<td>hard</td>
<td>RE-TL</td>
</tr>
<tr>
<td>Inspirational Security</td>
<td>medium</td>
<td>RE-IS</td>
</tr>
<tr>
<td>Interesting Research</td>
<td>medium</td>
<td>RE-IR</td>
</tr>
<tr>
<td>Open Source vs Proprietary Software</td>
<td>medium</td>
<td>RE-OS</td>
</tr>
<tr>
<td>Presentation or Blog</td>
<td>medium</td>
<td>RE-PB</td>
</tr>
<tr>
<td>Training - Creation and Delivery</td>
<td>medium</td>
<td>RE-TR</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>risk</th>
<th>Difficulty</th>
<th>key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable Use Policy</td>
<td>medium</td>
<td>RI-AU</td>
</tr>
<tr>
<td>GDPR Breach Notification to EU Regulator</td>
<td>expert</td>
<td>RI-BN</td>
</tr>
<tr>
<td>Gap Analysis</td>
<td>hard</td>
<td>RI-GA</td>
</tr>
<tr>
<td>JIRA Workflows</td>
<td>expert</td>
<td>RI-JW</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>hard</td>
<td>RI-RA</td>
</tr>
<tr>
<td>Risk Frameworks</td>
<td>hard</td>
<td>RI-RF</td>
</tr>
<tr>
<td>Risk Management and Acceptance</td>
<td>hard</td>
<td>RI-RM</td>
</tr>
<tr>
<td>Transformation Programmes</td>
<td>medium</td>
<td>RI-TP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>security</th>
<th>Difficulty</th>
<th>key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avatao for photobox</td>
<td>expert</td>
<td>SE-AB</td>
</tr>
<tr>
<td>Bug Bounties</td>
<td>expert</td>
<td>SE-BB</td>
</tr>
<tr>
<td>Security Threats</td>
<td>expert</td>
<td>SE-ST</td>
</tr>
<tr>
<td>Testing Vulnerabilities</td>
<td>hard</td>
<td>SE-TV</td>
</tr>
<tr>
<td>Vulnerabilities Discovered</td>
<td>medium</td>
<td>SE-VD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>setup</th>
<th>Difficulty</th>
<th>key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts Setup</td>
<td>medium</td>
<td>ST-AS</td>
</tr>
<tr>
<td>Pull Request</td>
<td>medium</td>
<td>ST-PR</td>
</tr>
<tr>
<td>Setup GitHub and Jekyll</td>
<td>medium</td>
<td>ST-GJ</td>
</tr>
<tr>
<td>Site Changes</td>
<td>medium</td>
<td>ST-AS</td>
</tr>
<tr>
<td>Write blog post</td>
<td>medium</td>
<td>ST-AS</td>
</tr>
<tr>
<td>Write blog post from transcription</td>
<td>medium</td>
<td>ST-BP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>standards</th>
<th>Difficulty</th>
<th>key</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBESt and CREST</td>
<td>hard</td>
<td>ST-CC</td>
</tr>
<tr>
<td>ISO Standards</td>
<td>expert</td>
<td>ST-TA</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>medium</td>
<td>ST-PD</td>
</tr>
<tr>
<td>Standards Advisor</td>
<td>expert</td>
<td>ST-SA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>technical</th>
<th>Difficulty</th>
<th>key</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Root Key</td>
<td>expert</td>
<td>TE-AW</td>
</tr>
<tr>
<td>Authentication and Authorisation</td>
<td>medium</td>
<td>TE-AB</td>
</tr>
<tr>
<td>Automated Build Tools</td>
<td>medium</td>
<td>TE-MB</td>
</tr>
<tr>
<td>AWS Root Key (continued)</td>
<td>expert</td>
<td>TE-AC</td>
</tr>
</tbody>
</table>
Real work scenarios

AWS ROOT KEY

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>TE-AW</td>
<td>expert</td>
<td>technical</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>RI-BN</td>
<td>expert</td>
<td>risk</td>
</tr>
</tbody>
</table>

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 them would be highlighted
Test candidate’s tech skills and CV claims

**SETUP GITHUB AND JEKYLL**

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST-GJ</td>
<td>medium</td>
<td>setup</td>
</tr>
</tbody>
</table>

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](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 h

**CBEST AND CREST**

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST-CC</td>
<td>hard</td>
<td>standards</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Contract Type</th>
<th>Location</th>
<th>Apply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head of AppSec</td>
<td>Permanent</td>
<td>London, Paris, Valencia or Munich</td>
<td>here</td>
</tr>
<tr>
<td>Head of Detect</td>
<td>Permanent</td>
<td>London, Paris, Valencia or Munich</td>
<td>here</td>
</tr>
<tr>
<td>Head of InfoSec</td>
<td>Permanent</td>
<td>London, Paris, Valencia or Munich</td>
<td>here</td>
</tr>
<tr>
<td>Head of Risk and Compliance</td>
<td>Permanent</td>
<td>London, Paris, Valencia or Munich</td>
<td>here</td>
</tr>
<tr>
<td>Head of SecOps</td>
<td>Permanent</td>
<td>London, Paris, Valencia or Munich</td>
<td>here</td>
</tr>
<tr>
<td>PosterXXL Information Security Officer</td>
<td>Permanent</td>
<td>Munich</td>
<td>here</td>
</tr>
<tr>
<td>Senior Cloud Security Engineer</td>
<td>Permanent</td>
<td>London, Paris, Valencia or Munich</td>
<td>here</td>
</tr>
</tbody>
</table>

## Contract Positions

<table>
<thead>
<tr>
<th>Role</th>
<th>Contract Type</th>
<th>Location</th>
<th>Apply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perl Security Developer</td>
<td>Contractor</td>
<td>London, Paris, Valencia or Munich</td>
<td>here</td>
</tr>
<tr>
<td>SOC Engineer and Incident Response</td>
<td>Contractor</td>
<td>London and Remotely (2 to 5 days per week)</td>
<td>here</td>
</tr>
</tbody>
</table>

## Upwork

<table>
<thead>
<tr>
<th>Role</th>
<th>Contract Type</th>
<th>Location</th>
<th>Apply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Writer</td>
<td>Upwork</td>
<td>Remote (up to 20h week)</td>
<td>here</td>
</tr>
</tbody>
</table>
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 ISO 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**: ST-GJ
- **difficulty**: medium
- **area**: 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](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 branch 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**: MA-TA
- **difficulty**: hard
- **area**: 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**: PR-PE
- **difficulty**: medium
- **area**: 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

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE-TL</td>
<td>hard</td>
<td>research</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO-PI</td>
<td>medium</td>
<td>compliance</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST-PD</td>
<td>medium</td>
<td>standards</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA-RM</td>
<td>expert</td>
<td>management</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE-OS</td>
<td>medium</td>
<td>research</td>
</tr>
</tbody>
</table>

Write a business, technical and moral case:
- for open source vs proprietary software
- for proprietary software vs open source

#3: JIRA Workflows

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>RI-JW</td>
<td>expert</td>
<td>risk</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>RI-RM</td>
<td>hard</td>
<td>risk</td>
</tr>
</tbody>
</table>

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 initiative?
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

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE-TR</td>
<td>medium</td>
<td>research</td>
</tr>
</tbody>
</table>

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?

### Challenges (optional)

#### #1: Deliver Results Through Teamwork

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA-DR</td>
<td>expert</td>
<td>management</td>
</tr>
</tbody>
</table>

- 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

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO-PI</td>
<td>medium</td>
<td>compliance</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>key</th>
<th>difficulty</th>
<th>area</th>
</tr>
</thead>
<tbody>
<tr>
<td>RI-RR</td>
<td>hard</td>
<td></td>
</tr>
</tbody>
</table>

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
## Content for PBX Group Security website

[https://pbx-group-security.com/](https://pbx-group-security.com/)

### Repository Information

- **1,287 commits**
- **8 branches**
- **1 release**
- **17 contributors**
- **Apache-2.0 License**

### Branches

- **Current Branch:** master

### Files and Changes

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>.vscode</td>
<td>added vscode workspace config for everyone to use with default to 2 sp...</td>
<td>11 days ago</td>
</tr>
<tr>
<td>bin</td>
<td>commit for github push</td>
<td>13 days ago</td>
</tr>
<tr>
<td>content</td>
<td>Update working-sessions.md</td>
<td>an hour ago</td>
</tr>
<tr>
<td>data</td>
<td>Update 4.yaml</td>
<td>29 days ago</td>
</tr>
<tr>
<td>i18n</td>
<td>fix issue 88</td>
<td>a month ago</td>
</tr>
<tr>
<td>layouts</td>
<td>- Added events shortcode for the Working Sessions page</td>
<td>a day ago</td>
</tr>
<tr>
<td>src</td>
<td>- Added events shortcode for the Working Sessions page</td>
<td>a day ago</td>
</tr>
<tr>
<td>static</td>
<td>- Added events shortcode for the Working Sessions page</td>
<td>a day ago</td>
</tr>
<tr>
<td>.gitignore</td>
<td>updated .gitignore to also have the .idea folder</td>
<td>23 days ago</td>
</tr>
<tr>
<td>CONTRIBUTING.md</td>
<td>Update CONTRIBUTING.md</td>
<td>a month ago</td>
</tr>
</tbody>
</table>
The challenge file (note the file name)

Darktrace Alert

Difficulty: hard
Skills: Briefing, Analysis, Planning

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.

Describe how you would proceed to achieve the same understanding in TechOps, DevOps, Business, and Management.

*Bonus points for mapping what could be the possible malicious and non-malicious (benign) root cause of this incident*

**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)?
SOC Engineer and Incident Response

Contractor

London and Remotely (2 to 5 days per week)

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

What will you do?
- You will be responsible for initial analysis/investigation of data at day-to-day basis.
- The role requires you to have previous experience of working in a SOC, along with hands-on experience in helping to define and build monitoring 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
- Experience in creating network diagrams (ideally from code/data)
- Programming experience (Python, JavaScript or Bash)
Challenges mapping is easy

tech_stack:
- AlertLogic and AlienVault or Elastic Stack/ELK
- AWS, Akamai, WAF, Lambda
- Risk Visualisation
- Python, Javascript, Bash
- Kibana, Grafana or Nagios

challenges_required:
- ST-SA-github-and-jekyll.md
  - CP-CB-collaboration.md
  - PR-LE-lambda-stop-ec2.md
  - SC-VD-vulnerabilities-discovered.md
  - PR-PE-programming-experience.md
  - RE-IR-interesting-research.md

challenges_optional:
- TE-LA-log-analysis.md
  - PR-VS-ec2-with-vuln-site.md
  - TE-DB-dashboards.md
  - CP-PL-planning.md
  - TE-DA-darktrace-alert.md
  - TE-AW-aws-root-key.md
Welcome to your Challenge page

Thank you for your application with Photobox Group Security.

The next stage of the recruitment process is to complete multiple challenges that have been hand-picked for you. Your challenges are based on your previous experience.

Unique ID

You'll be provided with a unique ID in the subject line of your challenge email, allowing you to remain anonymous during your participative process. This ID can be used in any communication about this role with Photobox.

Your Current Challenge List

- Security Threats
- Testing Vulnerabilities
- EC2 with Vulnerable Site
- Presentation or Blog
- Log Analysis

How to Submit your answers

Please submit your answers using a clone of this GitHub repository, which is a Jekyll-based website. You can find more detailed instructions there.

Think agile and incremental changes

Your first priority should be:

- setup the website
- make it scalable

Challenge Details

#1: Security Threats

- What methods of identifying security threats have you been involved with? What is your typical role within this scenario?
- What is your preferred method of identifying security threats?
- Have you automated systems for identifying security threats? If so, please describe

#2: Testing Vulnerabilities

In order to(1) conclusively show existing security vulnerabilities (and the various ways they can be exploited) and (2) once the code has been modified to exclude them, prove that this has been done, how would you set up automated tests?

- What kinds of things would you include in your tests? How would you replicate the security issues?
- Would your tests pass or fail when the vulnerabilities exist? When they no longer exist?
- How would you ensure that the tests would catch new instances of similar vulnerabilities?
- Can you provide a diagram of your solution (optional)?

#4: Presentation or Blog

Create a blog post or presentation about a technical or business-related book you have read recently which inspired you.

Book suggestions:

- New Rules for the New Economy: 10 Ways the Network Economy Is Changing Everything by Kevin Kelly
- Graph Databases: New Opportunities for

#5: Log Analysis

You are given 5 GB, 50 GB or 500 GB of nginx server logs (pick the one you are most comfortable handling). These logs cover a period when we know a high level vulnerability was exposed.

Your job is to:

1. Build an AWS-based infrastructure to consume, query, and visualise the data.
2. Find reoccur if that vulnerability has been re-used.
Candidate answers provided via Hugo site

Welcome
My name is Charlie Hacker. Welcome to my site. I hope to work with you in the future.
I am applying for the role of Head of Application Security at Photobox Group Security. I've completed the challenges as specified in the job posting for the position.
Part of this challenge was to test the technical writer's ability to edit and continuously integrate changes to a live Web site.
Tip: the GitHub repo for this site is https://github.com/pbx-gs/demo-9ed192bb

Password protected site
Please enter your password to get access.

Password
Submit
Using Netlify for Candidates website’s CI
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**

<table>
<thead>
<tr>
<th>February</th>
<th>March</th>
<th>March</th>
<th>April</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>6</td>
<td>20</td>
<td>3</td>
</tr>
</tbody>
</table>
Latest research and capabilities on this repo
RECRUITMENT PROCESS

First challenge is delivered to candidates house

Candidate is motivated by challenge

Solves on table or desk

Solution is a FLAG (key)

URL 1

Enters the flag

Solution

URL 2

Job offer

URL 3

OWASP Working Sessions across Table

Face to face meetings

Job offer