Product Brainstorm Doc

1. Final Product
    - Integrate notifications through slack (PagerDuty)
    - Web app
    - iOS app
    - AWS - using CDK vs Terraform

2. Use Cases:

a) **Threat and vulnerability management** - Ability to identify and patch the most critical vulnerabilities first. For example, using real-time threat intelligence combined with the results from a vulnerability scanner
    i) **Automatically preventing and remediating issues where users accidentally configure services in an insecure way**. For example, preventing a user from creating a public S3 bucket, deleting the bucket and notifying them of the deletion
        1) https://github.com/aws-samples/automating-a-security-incident-with-step-functions
        2) https://github.com/aws-samples/aws-security-hub-response-and-remediation

b) **Incident response** - Ability to automate many of the tasks required to respond to security events. For example, blocking IP addresses outside of corporate network ~~associated with a brute force login attempts~~
    - As a financial services provider, I would like to block certain IP addresses so that I can prevent brute force login attempts.
    - As a financial services provider, I would like to be notified when IP addresses outside of Australia are used to log in, so that I know when someone outside of the operating area is logging in.
    - As a financial services provider, I would like to block IP addresses outside of Australia that are used to log in, so that we do not allow people from outside our operating area to log in.
    - Using existing findings/alerts from GuardDuty vs generating these ourselves?

c) **Security operations automation** - Ability to automate the routine and most time consuming tasks conducted by their security operations team. For example, the manual enrichment of alerts with additional context such as geo-location information (based on IP).
    i) https://www.maxmind.com/en/home
    ii) Certain IP ranges are more ‘risky’ than others - also tag it with risk

d) Preventing unauthorised access to resources and services
    i) **IAM least privilege policy generator**
    https://github.com/salesforce/policy_sentry/#terraform

e) **Maintain visibility of potential vulnerabilities**
   i) https://vul-mgmt-program.awssecworkshops.com

3. AWS tools that might be useful
   a. GuardDuty tester - generate basic detections of the GuardDuty service using a simulated environment, targeting 5 common attack types https://github.com/awslabs/amazon-guardduty-tester

4. Other tools that might be useful
   a. Endgame - AWS pentesting tool that backdoors 18 aws services using rogue aws account - docs are good for prevention and detection info
      i. https://endgame.readthedocs.io/en/latest/prevention/
   b. Policy Sentry by Salesforce - generates least privilege policies for IAM https://github.com/salesforce/policy_sentry/#terraform
   c. rpCheckup - similar to Endgame https://github.com/goldfiglabs/rpCheckup

5. Questions

Pain Points

- Timeline documentation - it is often difficult to edit descriptions of security events timeline in real-time
  - **automate reporting of event timeline to provide a better overview of how events have unfolded (daily briefing style report?)**
- Important pieces of info needed to handle the incident are not communicated fully, or communicated in an unstructured manner which makes aggregation and searching difficult
  - **automate aggregation of event info such as CloudWatch logs, GuardDuty insights**
- Potential to be swept away easily from the work at hand (due to incidents)
  - **simplify tools for responding to events + make it easier to get back to work**