< PU CODE HACKATHON >

Track 1 – Cyber Security

Table of Contents

Problem 1: How do we reduce or eliminate password sharing?

Problem Statement: How do we reduce or eliminate password sharing?

More about the problem:

- This is a human nature problem. There are plenty of tools trying to prevent sharing now, but they can still be hacked around. For example:
    - SMS or Email verification codes can be hacked or shared
    - Security questions can be hacked or shared
    - The same IP address can be used (i.e. someone else logins in from the same computer)
- Ultimately, because we cannot change human nature, how do we start moving away from passwords as a means of authentication? Biometrics are being used for phone logins and purchases. How can more physical computers and digital software embrace a similar model that consumers will also enjoy.

What companies are doing now to solve the issue:

- Basic cybersecurity training
- Password rotations
- 2 factor authentication

Additional Resources:

- Password Security Policy: Managing the threat of shared passwords in enterprises https://www.isdecisions.com/blog/it-security/password-security-policy-managing-the-threat-of-shared-password/#:~:text=If%20a%20password%20is%20shared,falsely%20accused%20of%20the%20violation.
- Get the latest cybersecurity news and updates sent straight to your inbox: https://www.keepersecurity.com/blog/2021/07/06/4-rules-for-safe-password-sharing-in-the-workplace/
- Netflix testing a new feature to curtail password sharing: https://www.cbsnews.com/news/netflix-password-sharing-crackdown-feature/

Problem 2: How do we have visibility of cyber risks when companies primarily run out of the cloud with 3rd party services?

Problem Statement: How do we have visibility of cyber risks when companies primarily run their business via 3rd party cloud services?

More about the problem:

- Companies can do a good job standardizing company equipment, including internal servers, PCs, etc. However, more and more small businesses are running applications from the cloud.
- How do companies running on AWS, Google cloud services, and cloud SaaS monitor threats? In other words, how do they know if a threat is coming in via AWS or a 3rd party SaaS?
- Companies have process in place when threats occur - but this is more of a visibility issue. In addition, this is more a centralized cloud monitoring situation for SMBs with a smaller budget.

What companies are doing now to solve the issue:

- If they can afford it, companies are hiring a cybersecurity employee to help manually monitor attacks. However, most SMBs (especially in the early stages) do not have the budget for a full time cyber employee.
- There are other tools that can help monitor a specific cloud service, but not a centralized tool that auto-tracks all at the same time.

Problem 3: How can we streamline legal work for our cybersecurity company?

Problem Statement: How can we streamline legal work for our cybersecurity company?

Business Impact: Because the legal paperwork is not streamlined, it takes businesses a longer time to actually close sales. Also, each legal team is different, and there is not a standardized process (even though many of the legal paperwork itself is pretty standard). As a result, sales cycle times become less predictable - which impacts business forecasting plans (which impacts staffing, resources needed, and investments).

More about the problem:

- To be clear, this a problem many companies have, including cybersecurity companies themselves.
- The bigger the deal ($ sales amount), the more legal paperwork there is.
- Generally, both companies have lawyers and send drafts back and forth to each other, asking for revisions and changes. There is a formal process often used called "red lining"
- This cybersecurity company is trying to speed up the process by doing the following:
- Make it easier for both lawyer teams to collaborate and make changes quickly - ideally reducing email chains as much as possible
- Make it easier to identify which changes are small (nevertheless required) and some changes that are deal breakers (non-negotiable or significantly change the spirit of the agreement).

Problem 4: How can digital cybersecurity tools integrate more with physical security?

Problem Statement: How can digital cybersecurity tools integrate more with physical security?

More about the problem:

- In some companies, physical security and digital cybersecurity don't coordinate. For example, if John's keycard is used to open a door at 2 a.m., there is software that will notify the digital team. But then communication usually stops until someone manually sends a message to the physical security team.
- How can a cybersecurity system integrate better with a physical security team. So the logic would detect "John never comes at 2 a.m. Send a message to the security guard to investigate?"

Problem 5: How can companies reduce the white noise of constant cybersecurity warnings?

Problem Statement: How can companies reduce the white noise of constant cybersecurity warnings?

More about the problem:

- Some cybersecurity monitoring tools do a great job of logging and monitoring every digital activity. But with so much data, it's hard to sift through what really matters.
- The same logic holds true for notifications. When notifications are sent for every possible cybersecurity threat, the notifications become white noise because the cyber team sees too many and everything is "always a threat."
- With limited bandwidth, how do we let teams and employees know what they should be doing or monitoring now, based on business priorities.

Problem 6: How do we balance insider threat detection with data privacy laws?

Problem Statement: How do we balance insider threat detection with data privacy laws?

More about the problem:

- Cyber threats are easier to detect as a company has more data about the individual or actor.
- However, legislation is becoming more strict, which blocks or prevents cyber teams from collecting, storing, or sharing information.
- There is a current conflict of interest between the direction of legislative laws and the needs of a cybersecurity team.

Problem 7: How do we remove much of the manual effort needed to monitor cybersecurity now?

Problem Statement: How do we remove much of the manual effort needed to monitor cybersecurity now?

More about the problem:

- Even with A.I. and M.L on the rise, much of cybersecurity is still manual. Examples include:
    - A human has to teach the cyber software what to look for. Because dynamics are always changing, it can take a full time employee to adjust the algorithm.
    - Notifications are often manual. For example, a cyber software can create a flag for a human to read. Once the human reads the data, they can create a customer care ticket, or manually start the communication process. But most cyber software are not taking action. They monitor and alert - they don't communicate and try to resolve.
- As a result, cyber becomes very expensive very fast. You have to pay for the software and the employees to understand and run it. Even if they have the

capital, the need (and delay) of using a human, gives threats more time to do damage than if there was an automated process.

Problem 8: How can we prevent the soon-to-come ransomware attacks on individuals?

Problem Statement: How can we prevent the soon-to-come ransomware attacks on individuals?

More about the problem:

- Ransomware has plagued businesses for $100,000's to even millions of dollars.
- Most experts agree that ransomware tactics will be attacking normal individuals before long.
- Companies life Life Lock can prevent unwanted purchases, but what's preventing hackers from stealing sensitive info, photos, etc. and using them for ransomware.
- Because consumers have some many products (PC, phone, laptop, tablet, smart home devices), how are they going to prevent attacks?

Problem 9: how we can overcome the data encryption for digital evidences?

Problem Statement: How we can overcome the data encryption for digital evidences?

More about the problem:

- The popularity of data encryption on devices or networks is a significant hurdle for forensic investigators, limiting their ability to access data and gather evidence in an analysis-ready manner.
- The crucial need for specialized decryption tools arises as a pressing problem, necessitating novel solutions to enable successful data retrieval and ease forensic investigations in an encrypted digital environment.

Problem 10: How we can solve the Large data volumes in CSP Storage?

Problem Statement: How can we Solve the Large data volumes in CSP Storage?

More about the problem:

- In contemporary Cloud Service Provider (CSP) storage environments, the exponential growth of data volumes, reaching the scale of petabytes, poses a significant challenge in the realm of digital forensics and investigative processes. The sheer magnitude of data stored within these facilities introduces complexities in efficiently identifying and extracting relevant digital evidence crucial for investigative purposes. This challenge directly hampers the speed and efficacy of data processing procedures aimed at uncovering pertinent information.
- The existing research landscape reveals notable gaps in methodologies related to data reduction, data mining, intelligence evaluation, and the effective utilization of both open and closed-source information. Despite advancements in cloud technology, the ability to handle, sift through, and extract meaningful insights from these vast datasets remains an ongoing concern. As such, there is a pressing need to develop and implement comprehensive strategies for information collection and filtering tailored to the unique demands of cloud infrastructures.
- Addressing these challenges requires innovative solutions that go beyond traditional forensic approaches, delving into the realms of data reduction methodologies and intelligent information processing. The development of robust frameworks for managing and analyzing large datasets within cloud environments is imperative to ensure timely and accurate extraction of digital evidence for investigative purposes. Efforts must focus on bridging the existing research gaps and establishing best practices that enable efficient handling of massive data volumes while maintaining the integrity and reliability of digital evidence in cloud storage facilities.

Problem 11: How can we address the problem of data hiding in storage space caused by an attacker?

Problem Statement: How can we address the problem of data hiding in storage space caused by an attacker?

- **More about the problem:**
- The advent of data concealing strategies within storage spaces, organized by attackers, presents a significant problem for digital forensic investigations.
- In this case, data is purposely buried so that it is invisible to ordinary system instructions and programme, resulting in a complicated and time-consuming investigation procedure.
- This clandestine technique adds another degree of complexity for forensic investigators, who must deal with not just data obfuscation but also the risk of data corruption.
- Among the various tactics used by attackers, rootkits stand out as one of the most common approaches for attaining stealth in data concealing within storage areas.
- **Key Challenges**:

Invisibility to Standard System Operations

Complexity in Forensic Inquiries

Extended Investigative Timelines

Potential Data Corruption

Rootkit Utilization

Need for Specialized Forensic Approaches