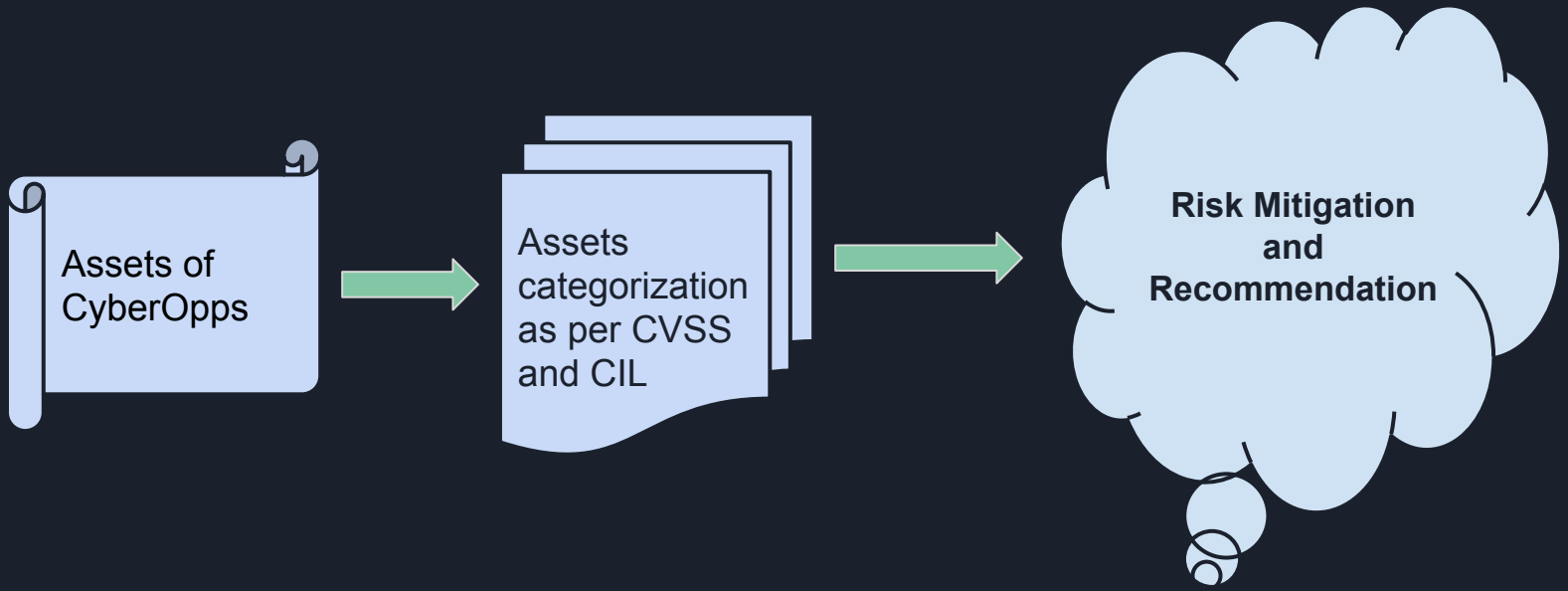
Security Categorization Case Study

Executive Summary



Assets of CyberOpps

1. Unique and high value programs (and program structure)
2. SQL Database of employees & Clients
3. 2019 Windows Server (Unpatched)

Assets categorization as per CVSS and CIL

1. Unique and High Value Programs(and Program Structure)

   CVSS Base Score: 7.8(High) assuming following,

➔ As company has unique & high value programs, it can be vulnerable locally, may be threat from inside who knows the value of such programs.
➔ Considering local/insider threat to the company asset, Low privilege may work for attacker to target.
➔ Impact Metrics will all be High, as programs are unique

Assets categorization as per CVSS and CIL

2. SQL Database of Employees and Clients

CVSS Base Score: 7.8 (High)

- ➔ Considering CVN ID: CVE-2022-34006, which had similar vulnerability found on June 19, 2022.
- ➔ SQL database, it can be vulnerable locally, may be threat from inside who knows the vulnerability
- ➔ Considering Local/insider threat to the company asset, Low privilege may work for attacker to target.
- ➔ Impact Metrics will all be High, as database of employees and clients are sensitive.

Assets categorization as per CVSS and CIL

3. 2019 Windows Server (Unpatched)

CVSS Base Score: 8.4 (High)

- ➔ Considering CVN ID: CVE-2022-42973, which had similar vulnerability found on January 31, 2023.
- ➔ Impact Metric would be high for this as unpatched server is vulnerable
- ➔ Kevin knows about the unpatched windows 2019 server, which can be exploited through Titan Ftp, makes exploitability very high.

Risk Mitigation Recommendation

1. Conduct through security check in order to identify any vulnerabilities
2. Define control so only required data can be accessed by employee
3. Patch and update automatically, both Operating systems and applications
4. Encrypt sensitive data within the SQL database to protect employee and client information from unauthorized disclosure.
5. Train employees on best practices on frequent reviews
6. Follow zero trust model or at least a model of least privileges