Similarities with riskrecon

Note:

Red – We can make difference point in the area

Green – we can adopt

Working:

Step 1) Starts with Name:

- **Takes org name and domain**
- **RiskRecon analyst uses guided algo to discover public facing asset like system, network and domain**
- **Also discover core subsidiaries (maybe subdomain)**
- **Claims very low false positive**

Module 1: Asset discovery

- **Asset profile refreshes very 2 months**
- **Later the asset is discovered, analyst(human) uses machine learning module to efficiently mine accurate data which they have discovered**

Module 2: IT profiling

They group there discovered assets in following categories

- Software
- IT Infrastructure
- Geolocation
- Hosting Providers
- Fourth Parties
- Domains
- Systems
- Configurations
- We can add

For each security domain, RiskRecon reports overall current performance, trends, and industry benchmarks. Each issue is backed with detailed information issue summary and detailed descriptions, related CVEs, hostname, IP address, asset value, issue severity, and risk priority.

Module 2: Customize risk

- **Automatic data filtering**
- **risk prioritization**
- **Provision to make group policy**
- **Scan for Vendor compliance**

Step 2) Asset profile architecture

- **Build complete asset profile which are discovered**
- **With this, they allow you to get how your business has constructed there computation architecture**

Step 3) Analyze security criteria

- **They check for total 41 security criteria spanning 11 security domains**

Step 4) Asset value analysis

- **Basically, a customized technique to assess the discovered assets**

Step 5) Risk rating

- **They have some technique using which they rate the overall process and generate report**

Advantage over them: -

- **Scalable, we can add new modules without messing more on the system**
- **Effective and real time techniques to discover the assets which a attacker follows.**
- **Approach is Black box**
- **No human intervention**
- **Checking for basic vulnerabilities.**
- **ELK stack (Data lake)**
- **Easy deployment of SecEagle**
- **Fault tolerant Micro service architecture with the help of Kubernetes, change doesn't take efforts**
- **Enables API**
- **Aggressive scanning engine, pointing the view of attacker**
- **Discovery engine yields important data like JS files, code repo, etc.**
- **Ability to customize pipeline**

Add some according to you