SecurityScorecard

Cyber Ratings: Partnering with Your Suppliers to Defend the Extended Attack Perimeter

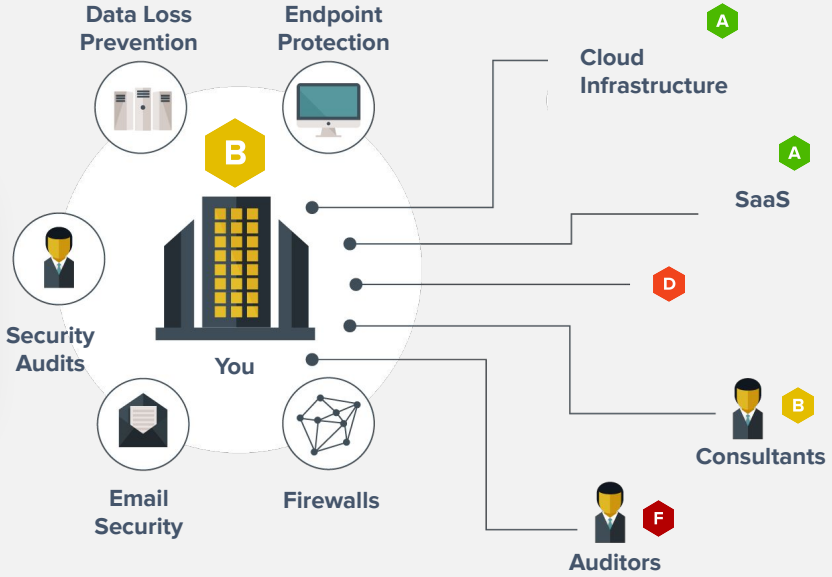
Alex Rich, Senior Director, Alliances

Oct 12, 2021

Cyber Ratings: What + Why

There is no gold standard to measure and communicate security performance

How do I understand and **communicate the value of my security program**?



How do I know if my third parties are diligent about protecting the data?

53% of organizations have experienced one or more data breaches caused by a third party (Ponemon Institute)

How Ratings Work

How Ratings Work

ISACA Los Angeles Chapter

1 Data Collection

- **Global sensor network** crawling the Internet from over 45 locations
- **25B+** vulnerabilities gathered per week and **500M+** malware infections per day (top 5 sinkhole)

2 Attack Surface Discovery

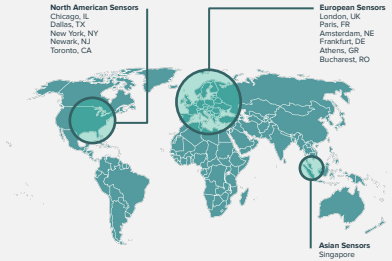
- Patented capabilities discover company attack surface
- Attribution of attack surface to any organization worldwide

3 ML-Powered Data Processing

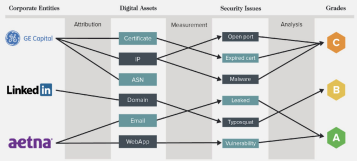
- Data processing engine aggregates signals to enhance accuracy
- Hundreds of risk factors over 10 security categories
- **ML based risk severity** model that learns from user feedback

4 Ratings

- **Fair, accurate, and predictive scoring model** with low scores 5x-7x more likely to breach
- **7 years** of historical data + user contributed data



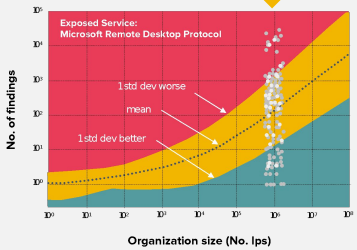
Automated Attack Surface Discovery Engine



U.S. Patent No. 10,560,474
"Entity IP Mapping"

U.S. Patent No. 10,515,328
"Non-intrusive techniques for discovering and using organizational relationships"

$$TS_{df} = \frac{\sum_i w_i \times g(FS_{df}) \times FS_{df}}{\sum_i w_i \times g(FS_{df})}$$



Meaningful Correlation with Breach Risk

Organizations with an F have **7.7x higher likelihood of breach** compared to organizations with a grade of A.

Study Parameters

Evaluation Period	3 Years
No. Data Breaches	2,228
No. Organizations	99,076

Supply Chain Use-Case

The Third Party Challenge

- Build vs. Buy decision has been made
  - Companies buy + outsource whenever possible
  - Average company relies on hundreds, if not thousands, of Vendors
- Vendors become extension of our attack perimeter when we:
  - Provision network access
  - Share sensitive data
- We don’t have the continuous visibility into + control over 3rd party security


You
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties

Third Party Attack Trends

- Attackers Target Company's Third Parties vs. Company directly
  - Exponential increase in entry points + potential attack vectors
  - Soft spots result from varying degrees of cyber competency
- Compromise Company via Third Party Privileges
  - Phishing Attack, Compromised Credentials, Remote Updates
- Third Party attacks ramping in terms of frequency and impact
  - SolarWinds, Colonial Pipeline and Kaseya

Challenges with Current VRM Approaches

- We use static measurements - cybersecurity is dynamic
- Outputs are subject to bias + self-serving outcomes
- Manual + human processes are plagued by human error
- Activities are time consuming + have in-person requirements
- Methods are expensive + lack scalability

Traffic Cop

- Map component of Rating to an Assessment Activity
  - EG. Top Level score and Questionnaire
- Create threshold that triggers activity + only trigger when crossed
  - EG. only send questionnaire if Top Level score falls below C
- Tailor activity to focus on findings or factors that tripped threshold
  - EG. If CVEs brought score below C, ask questions re: patching
- Right-sized, just-in-time Assessment Activities - avoid unnecessary

Collaborating + Engaging with Suppliers

- Invite Vendor to platform + to claim their scorecard
- Establish SLAs to govern relationship + embed in contract
  - Minimum grade requirement + ”No-Go” issues list
  - Remediation window for raising score + addressing issues
- Use rules + alerts to monitor for compliance and automate responses
- Track remediation progress + ensure compliance via History view

Automated Backlog Prioritization

- Organization has large vendor assessment backlog
- No time to perform inherent risk assessment that informs prioritization
- How do we ensure prioritization of High Critical + low security vendors?
- Sort backlog using grades (low to high) – asses low score vendors first
- Instant + low effort prioritization that guarantees prioritization goals

Streamlined Assessments

- Establish grade requirement for a supplier (must be above C)
  - Tailor requirement based on use-case + supplier type
- Pass / Fail supplier based on performance against requirement
- Leverage for high-volume + early stage assessments (RFP)
- Leverage for low risk suppliers (tailor effort to asses with risk posed)

Additional Ratings Use-Cases

Ratings Use-Cases

Executive Level Reporting

Enterprise Risk Management

Third Party Risk Management

Due Diligence

Service Providers

Compliance

Cyber Insurance

Regulatory Compliance Gap Analysis, Monitoring and Enablement for First and Third Parties

ISACA Los Angeles Chapter

- Identify controls that can be assessed from outside
  - *Does organization have patching program?*
- Map controls to relevant issue(s) in platform
  - *CVEs imply weak or missing program*
- Perform gap analysis against framework
- Identify remediations required for compliance
- Continuously monitor compliance on ongoing basis

Supported Frameworks:

- *CMMC*
- *PCI*
- *GDPR*
- *HIPAA*
- *ISO*
- *NIST (800-171, 800-53, 1.1)*
- *NERC*
- *NY DFS*
- *SIG (Core, Full & Lite)*
- *TISAX*

Enterprise “Self-Monitoring”

- Identify and track publicly facing assets - manage shadow IT
- Quantify and contextualize security issues using NIST
- Leverage IP-Level detail to drive remediation and automation
- Build dynamic + automated remediation plans via grade requirements
- Use grades to report to stakeholders + non-tech audiences (BOD)

ISACA-LA Member Offer

- All members entitled to Complimentary Enterprise Starter License:
  - Continuous Monitoring of own Organization
  - Continuous Monitoring of up to Five Third Parties
  - Existing Customers receive Five complimentary “Slots”
- Access to dedicated SecurityScorecard Customer Success Manager
- Preferred pricing on select Slot + Atlas bundles
- Sign-up via www.securityscorecard.com/isaca-la

Questions?

Alex Rich - arich@securityscorecard.io

Thank You!