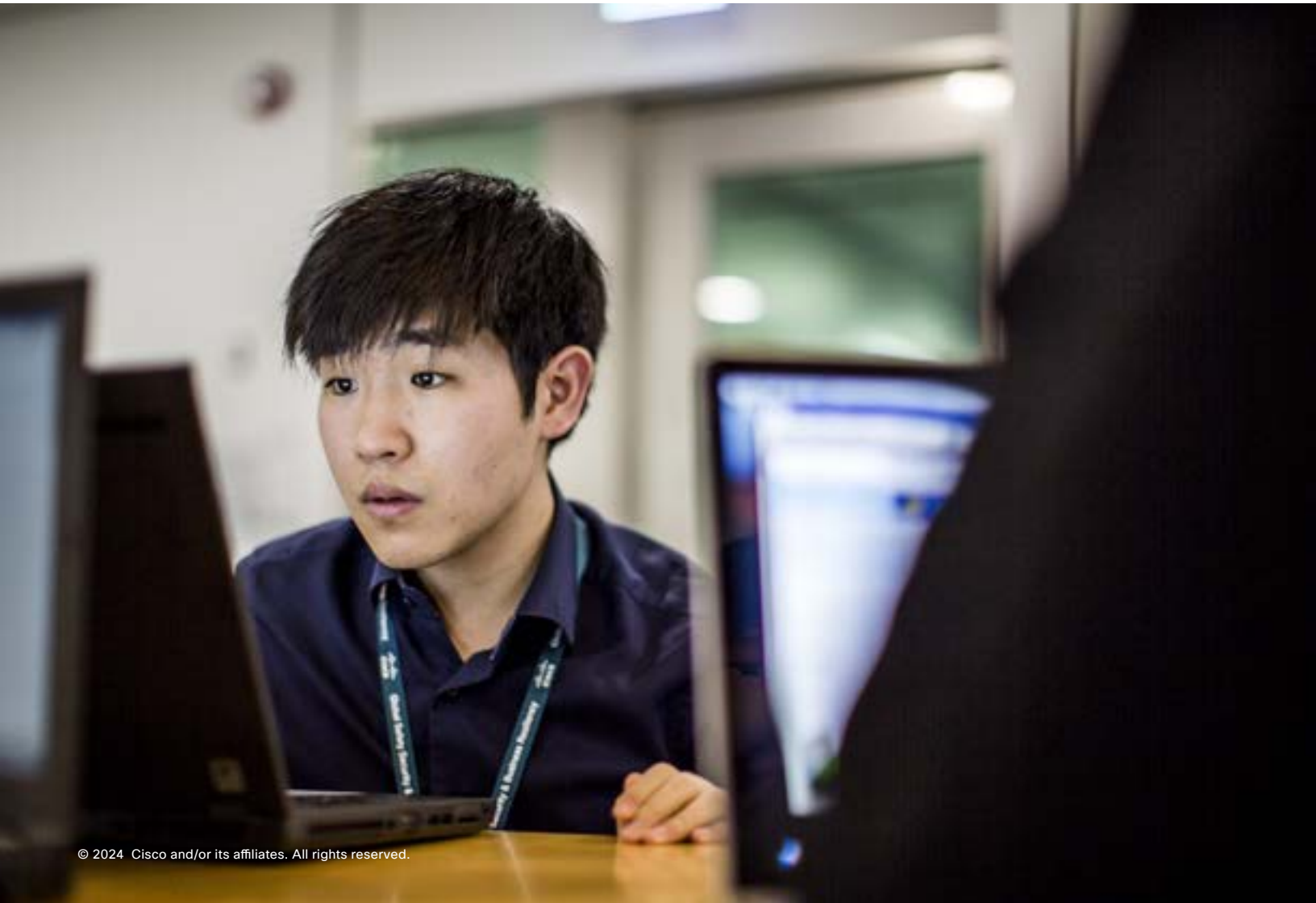
The bridge to possible

Experience the power of the Cisco Security Risk Score

A risk score is a crucial tool for organizations looking to effectively prioritize vulnerabilities within their environment. It can serve as a strategic guide that enables security teams to allocate resources efficiently and focus on addressing the most critical threats first.

However, not all risk scores are created equal. The variables used to form a risk score can make or break just how effective it is in prioritizing vulnerabilities and enabling teams to make the most informed decisions when it comes to reducing security risk. Let's dig into the variables and data science used by Cisco Vulnerability Management to form the Cisco Security Risk Score (formerly Kenna Risk Score).



The bridge to possible

Datasets used for risk scoring

To help organizations prioritize their vulnerability remediation efforts, Cisco Vulnerability Management analyzes two key datasets:

1. Internal enterprise security data from every available source across the customer's infrastructure, applications, and the Internet of Things (IoT), and
2. Ground truth telemetry, which includes custom-curated exploit and threat intelligence feeds

This data is analyzed by proven data science algorithms to deliver an accurate, granular, and quantifiable risk score for every vulnerability within seconds.

Ground truth telemetry

19+ exploit and threat intelligence feeds

15+ billion security events

12.7+ billion managed vulnerabilities

Exploit intelligence

- Metasploit
- Exploit DB
- ReversingLabs
- Proofpoint
- Secureworks CTU
- D2 Elliot
- Contagio
- Black Hat Kits on rotation (AlphaPack, Blackhole, Phoenix, more)
- Canvas Exploitation Framework
- CISA Known Exploited Vulnerabilities
- Github Exploit Feed: Cyentia Institute

Threat intelligence

- AlienVault OTX
- AlienVault Reputation
- Secureworks CTU
- Emerging Threats
- ReversingLabs
- Sans Internet Storm Centre
- X-Force Exchange
- Cisco Talos
- Silobreaker

Internal security data sources

- Any vulnerability scanner
- Asset- and network-specific data from configuration management database (CMDB) tools
- Penetration testing
- Bug bounty programs
- Static application testing
- Dynamic application testing
- Open-source tools
- Custom data sources in JSON format

The bridge to possible

Data science techniques used to understand risk

Cisco Vulnerability Management uses proven data science techniques, including machine learning, natural language processing, and predictive modeling to assess, prioritize, and even predict risk. These approaches allow us to dynamically calculate the risk of every vulnerability to enable security and IT teams to embrace risk-based vulnerability management.

Using predictive modeling, Cisco Vulnerability Management can calculate the risk of a vulnerability as soon as it is revealed. Advanced predictive modeling forecasts the weaponization of new vulnerabilities with a confirmed 94 percent accuracy rate, and then prioritizes remediation based on the risk of exploitation. This gives your organization the foresight needed to remediate high-risk vulnerabilities before attackers can mount an attack.

Natural language processing—a branch of artificial intelligence aimed at making sense of "natural" human language—investigates social media sites, the dark web, and other places where vulnerabilities are discussed, and extracts the language associated with vulnerabilities to assist in risk assessment. Natural language processing is also used to help score vulnerabilities that do not have a Common Vulnerability Scoring System (CVSS) score by analyzing various text keywords and phrases that are shown to be high indicators of risk.

Cisco Vulnerability Management then analyzes the data using a number of predictive technologies, including support-vector machines (SVM), random forest, logistic regression, and vulnerability inference. The data from the predictive models is then used by our risk scoring engine to produce an actionable, dynamic risk score for every vulnerability that is automatically updated as new intelligence is made available. Enter: **The Cisco Security Risk Score** (formerly Kenna Risk Score).

Gain actionable insights with the Cisco Security Risk Score

Leveraging ground truth telemetry and an extensive amount of internal security data, the Cisco Security Risk Score ties into Cisco Vulnerability Management's predictive model to algorithmically determine risk scores for each unique vulnerability, ranging from zero (no risk) to 100 (highest risk). And, in concert with asset criticality scores, Cisco Vulnerability Management determines an actionable risk score for each asset and group of assets that ranges from zero (no risk) to 1000 (highest risk).

The Cisco Security Risk Score takes into account all of the internal and external variables used in the predictive model that are high indicators of risk. Internal risk calculations factor in the number of instances of each vulnerability in your environment, their potential severity, and the criticality of the assets that are threatened as a result of each vulnerability. External risk calculations factor in more than just the CVSS score of the vulnerability by also including EPSS, threat intelligence information such as whether or not an exploit kit is available for the vulnerability, the volume and velocity of exploits that take advantage of the vulnerability, and the prevalence of the vulnerability seen throughout customer environments. With accurate and quantifiable risk scores, you will understand your organizations' current risk posture and identify the actions you can take to reduce the greatest amount of risk.

Ready to see the Cisco Security Risk Score in action?

Get in touch at https://www.cisco.com/go/vulnerability-management

1271441047 02/24