Executive Summary

Prioritization to Prediction

Analyzing Vulnerability Remediation Strategies

KENNA Security

Let's acknowledge one truth right from the beginning: being a cyber security professional in today's environment is challenging.

The pressure to digitally transform businesses, coupled with a tech stack of ever increasing complexity have created such a deluge of data that it is simply impossible for any organization to remediate every vulnerability and ensure 100% coverage of its attack surface.

Effective remediation depends on quickly determining which vulnerabilities warrant action and which of those have highest priority, but prioritization remains one of the biggest challenges in vulnerability management. For the first time, Kenna Security and the Cyentia Institute took a quantitative look at the effectiveness of common remediation strategies and used that data as a baseline to compare against a cutting-edge predictive model.

The results of this research are detailed in the new report, *Prioritization To Prediction: Analyzing Vulnerability Remediation Strategies.*

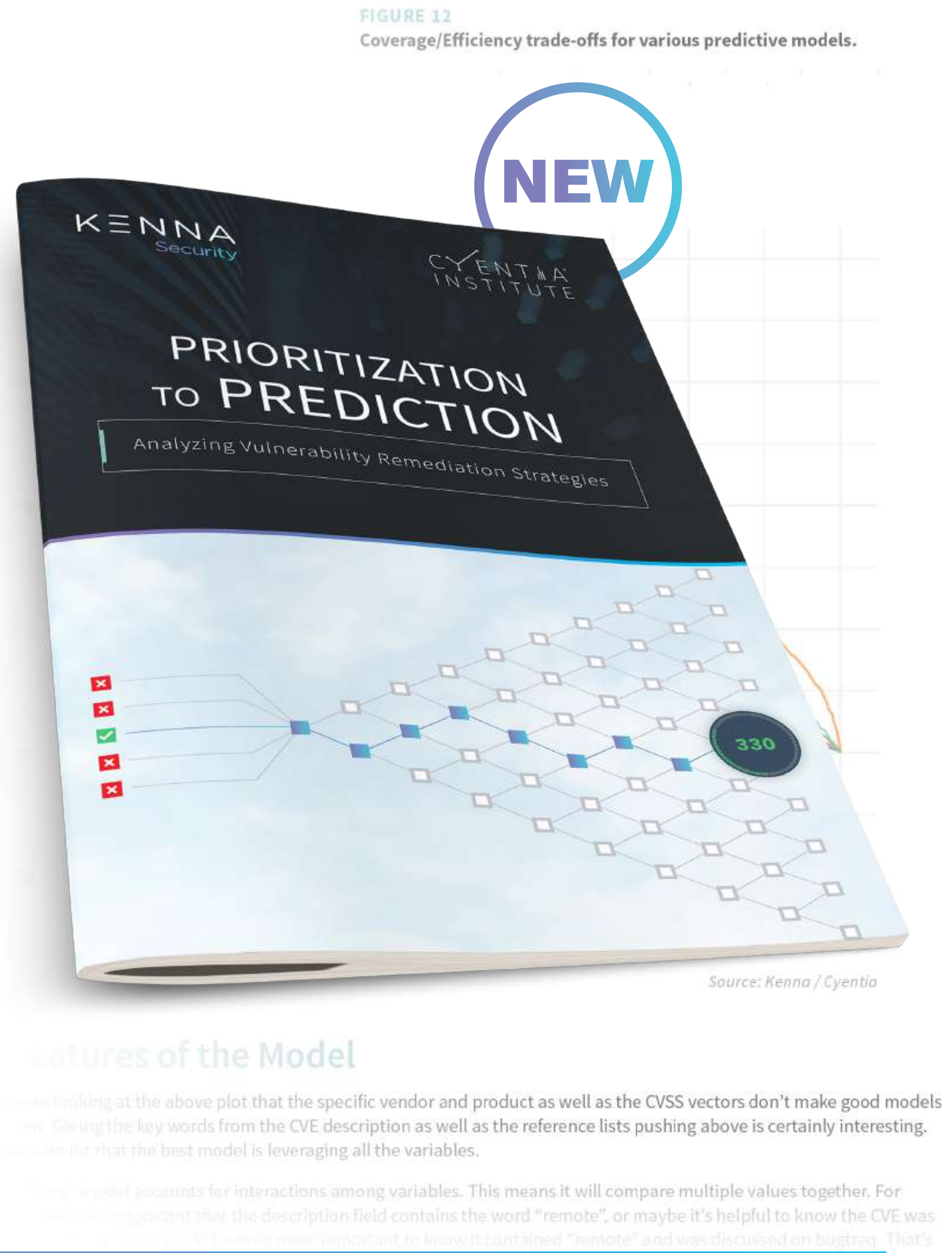
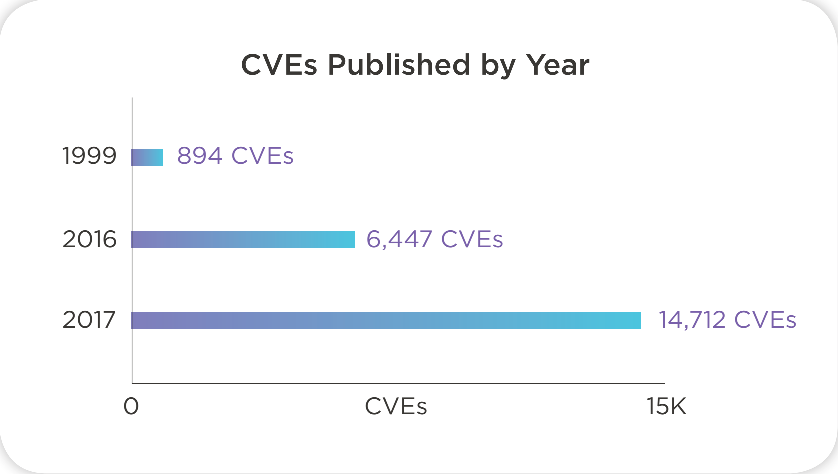


FIGURE 12
Coverage/Efficiency trade-offs for various predictive models.
NEW
KENNA Security
CYENTIA INSTITUTE
PRIORITIZATION TO PREDICTION
Analyzing Vulnerability Remediation Strategies
330
Source: Kenna / Cyentia
eatures of the Model
looking at the above plot that the specific vendor and product as well as the CVSS vectors don't make good models
Seeing the key words from the CVE description as well as the reference lists pushing above is certainly interesting.
that the best model is leveraging all the variables.
model accounts for interactions among variables. This means it will compare multiple values together. For
important that the description field contains the word "remote", or maybe it's helpful to know the CVE was

Key Findings

The number of CVEs published every year is steadily growing. Between its inception in 1999 through January 1st, 2018, over 120,000 vulnerabilities have been published to MITRE's Common Vulnerabilities and Exposures (CVE) database.

894 CVEs were published in 1999 and 6,447 CVEs published in 2016. 2017 saw a massive spike to 14,712 CVEs and 2018 is trending to meet the 2017 numbers.

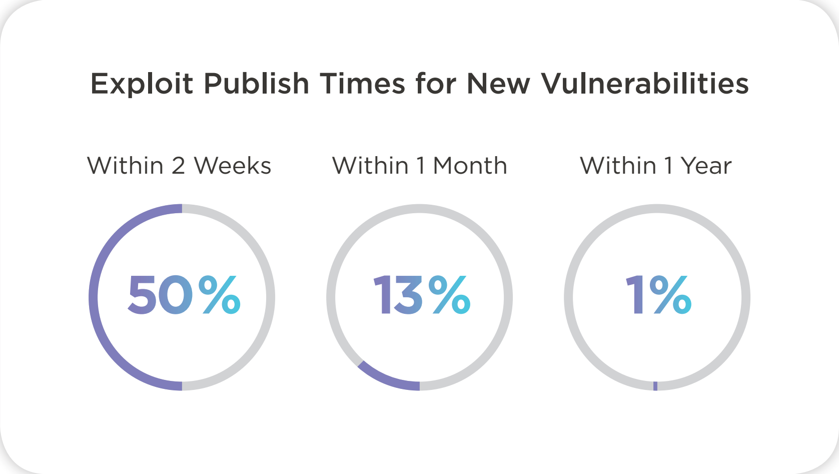


Most reported vulnerabilities are never acted upon by hackers. Out of the thousands of new vulnerabilities published every year, the vast majority (77%) never have exploits developed, and even fewer are actively attacked.

> *"Less than 2% of vulnerabilities are actively exploited in the wild, making traditional remediation very inefficient, costly, and time-consuming."*

Speed must be a priority. This won't come as a surprise, but remediating vulnerabilities quickly is essential to thwarting exploits, as our research indicates that the first month after a vulnerability is released is when the greatest number of exploits publish.

50% of exploits publish within two weeks of a new vulnerability and 13% of exploits hit a month or more after vulnerabilities publish, while only 1% emerge beyond 1 year.



Key Findings

Common strategies are about as effective as rolling dice. Most current approaches for prioritizing and fixing vulnerabilities – whether that is based on vendors with most CVEs, using CVSS scores, or relying on reference lists – are roughly as effective as random chance. To illustrate, below is an example of the efficiency, effort, and overall coverage achieved by a common remediation strategy.

Remediating Vulnerabilities for the 20 Vendors with the highest amount of CVEs:

- Efficiency = 12%
- Effort = 56,188 CVEs remediated
- Coverage = 21%
- **Random Chance:** Efficiency = 23%; Coverage = 42%

A Predictive Model increases efficiency, reduces workload, and increases coverage. Kenna's Predictive model offers huge improvements in effectiveness and efficiency over the vulnerability remediation strategies analyzed in the report. When comparing our predictive model against a relatively effective strategy of remediating vulnerabilities with a CVSS score of 7 or more, Kenna's predictive model achieved:

Kenna's Predictive Model

Twice the efficiency
61% vs. 31%

Half the effort
19K vs. 37K CVEs

One-third the false positives
7K vs. 25K CVEs

Better coverage
62% vs. 53%

Conclusion

A predictive model enables businesses to adopt a proactive model for vulnerability remediation that delivers the most efficient use of their people, tools, time, and ultimately dollars to address the threats that pose the greatest risk. To learn more, we encourage you to download the full report, which includes:

- **A detailed review of the data sources available for building or improving decision models for vulnerability remediation**

- **A discussion of the vulnerability lifecycle and examination of the timelines and triggers surrounding key milestones**

- **Identification of the attributes of vulnerabilities that correlate with exploitation**

- **A measurement of the outcomes of several remediation strategies, which we used to develop a model that optimizes overall effectiveness**

Click here to get your copy of

Prioritization To Prediction:

Analyzing Vulnerability Remediation Strategies

KENNA Security
CYENTIA INSTITUTE
PRIORITIZATION TO PREDICTION
Analyzing Vulnerability Remediation Strategies
330