KENNA Security

A Race Against the Bad Guys (Risk – Based SLAs)

Katie Conners - Sr. Customer Success Engineer
Justin Fong - Sr. Customer Success Manager

Kenna Security, Customer Success Team

03/26/2021

Risk - Based SLAs

Agenda

- Intro to SLAs
- Standard SLA Structure
- Value of Risk Based SLAs
  - How we do it?
- Risk-Based SLA Structure
- [DEMO] How to Deploy Risk Based SLAs
  - Define a risk tolerance for various parts of the network
  - Build SLA policies that match the documented policy
- [DEMO] Tracking SLAs
  - SLA metrics in reporting tab
  - Edge case risk meters to track SLA adherence

KENNA Security

Intros to SLAs

- An SLA for Vulnerability Management is a defined time based requirement in which a vulnerability must be fixed on.
- Hold teams accountable for mitigating risk.
- Define SLAs in a Security Standard or Policy so teams understand how long they have to remediate.
- Documenting the SLA policies for client audits and regulators.
- In most if not all cases, the organization can define severity levels and the SLAs associated to them. As long as they are following those requirements, then passing audits and assessments will be ok.

KENNA Security

Standard SLA Structure - How are they determined?

	High	Medium	Low
External	15 days	30 days	45 days
Internal	30 days	60 days	90 days

- Typically based on a 30/60/90 day structure
- Mirrors monthly patch cycles
- Arbitrary from an IT perspective

KENNA Security

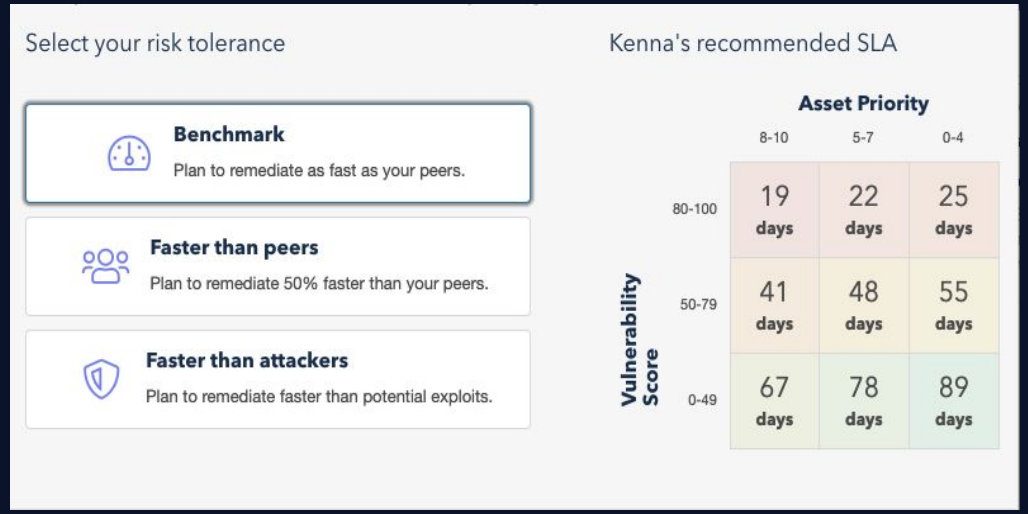
Value of Risk Based SLAs

- Data Science-driven recommendations based on your organization's appetite for risk
- No more arbitrary remediation timeframes
- Lower tolerance, faster remediation
- Key Factors:
  - Risk Tolerance
  - Asset Priority
  - Vulnerability Risk Score (High, Medium Low)

KENNA Security

Risk Tolerance - Benchmark

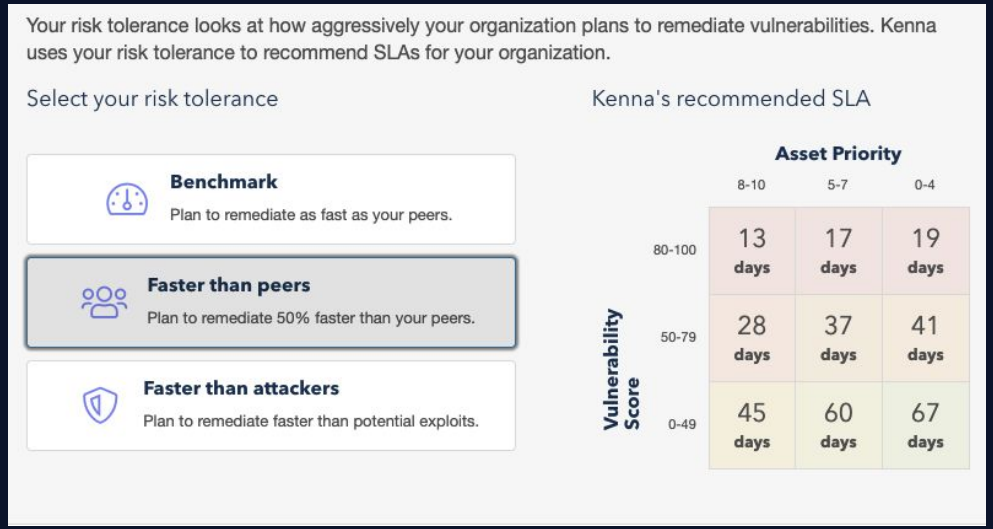
- Plan to meet the mean time to remediate (MTTR) benchmark
- Higher risk tolerance
- Tracking and following your peer's performance



KENNA Security

Risk Tolerance - Faster than Peers

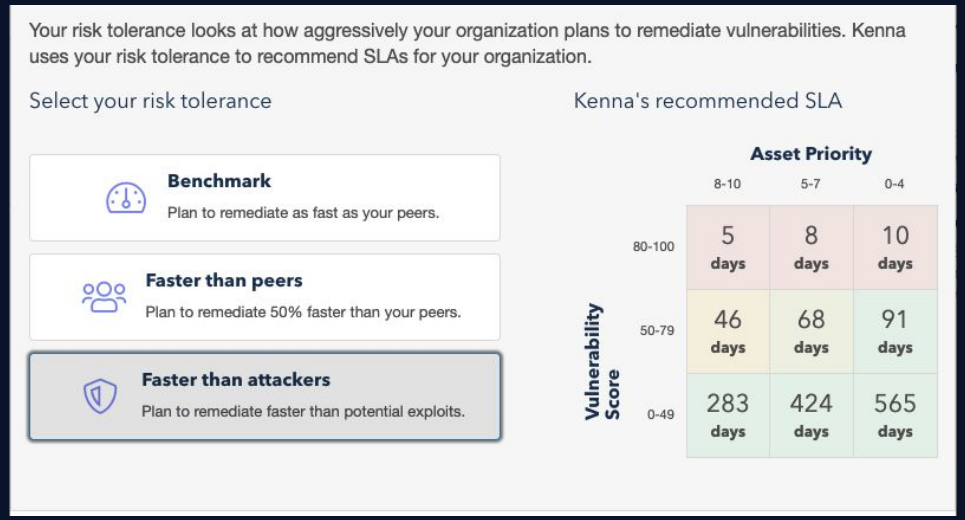
- Plan to remediate 50% faster than peers
- Medium risk tolerance
- MTTR based



KENNA Security

Risk Tolerance - Faster than Attackers

- Plan to remediate as early as a vulnerability is likely to be exploited
- Low risk tolerance
- Measuring data from Mean Time to Exploitation (MTTE)
- Leveraging threat and exploit intelligence to identify how fast attackers are exploiting vulnerabilities.



KENNA Security

Risk Based SLA Structure - Sample

	100-80	79-50	49-34	34-0
External Network (Asset Priority 10)	5	46	120	No SLA
Internal Network (Asset Priority 9)	19	60	180	No SLA

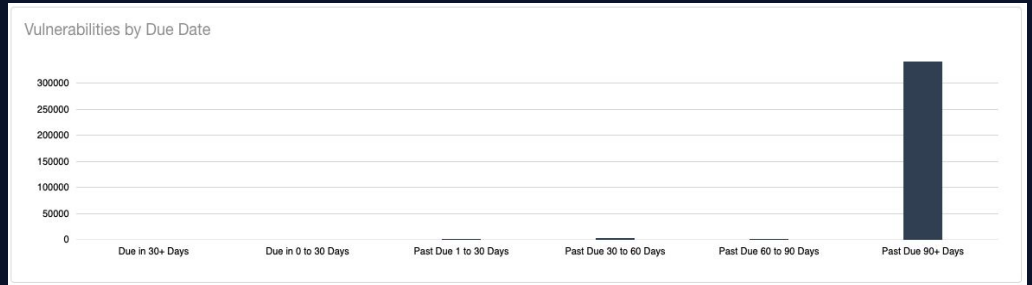
Low Tolerance

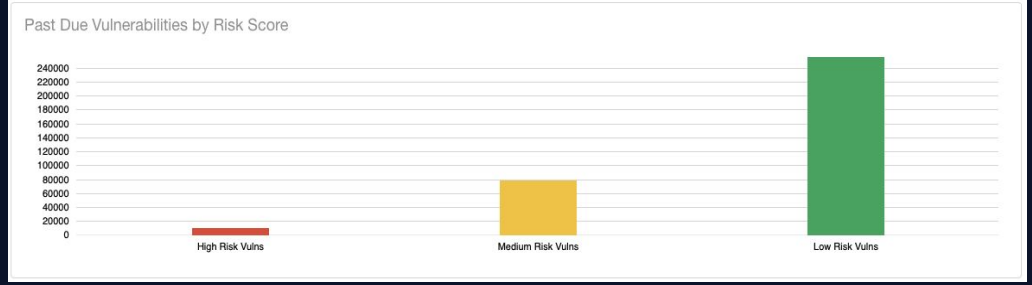
Benchmark

KENNA Security

Tracking SLAs - Reporting Tab

- Each risk meter has a reporting tab with a couple SLA related metrics
- Summary of Vulnerabilities by Due Date
- Past Due Vulnerabilities by Risk Score
- You cannot drill down into these but you can create risk meters to get the details





KENNA Security

Tracking SLAs - Edge Case Meters to Track SLAs

Edge Case	Search Syntax
Vulnerabilities not closed by due date	not_closed_by_due_date:true
Vulnerabilities closed by due date	not_closed_by_due_date:false
Vulnerabilities past a certain due date	due_date:<[ENTER PAST DATE]
Vulnerabilities coming due at a future date	due_date:>[ENTER TODAY'S DATE OR FUTURE DATE]
Vulnerabilities by due date range	due_date:[2019-01-01 TO 2019-09-20]
Vulnerabilities due in the next 30 days	due_date:<now+30d AND due_date:>=now

KENNA Security

Demo Time

KENNA Security

Interactive Poll

What has worked for you and what has not?

KENNA Security

KENNA
Security

KENNA Security

Thank you!

Justin Fong, Sr. Customer Success Manager

Katie Conners, Sr. Customer Success Engineer