KENNA Security

Steps to Risk-Based Remediation using Kenna

Step 1 – Use Kenna's Threat Intelligence to Drive Remediation Decisions

- Let the Kenna patented algorithms do the hard work!
- Kenna correlates various threat intelligence with your vulnerability data to help you determine what to fix first.
- We create a normalized Kenna Risk Score for each CVE based on our threat intelligence.
- Using the Kenna Risk Score to drive remediation decisions rather than CVSS, scanner score, or the hottest new CVE will significantly reduce the number of critical vulnerabilities which need remediation.

Step 2: Operationalize Kenna

- Define your risk tolerance. What is an acceptable risk score to drive remediation?
    - Do you want to remediate faster than your peers? Faster than attackers?
    - What resources and capacity to remediate does your program currently have? Make sure your risk tolerance is in line with what you can accomplish.
- Once the tolerance is defined, document this in your Security policies.
    - Use the Kenna Risk Score to drive SLAs. If your teams base SLAs on scanner score or CVE severity, they will be overloaded with work and your Kenna Risk Score will never go down.
- Set short- and long-term goals - SMART goals (Specific, Measurable, Achievable, Relevant and Time-bound) for positive reinforcement. For example:
    - Short term – remediate all 90s and above in your team's risk meter within three months.
    - Long term – reduce the MTTR (Mean Time To Remediate) for high risk vulnerabilities across the organization from 60+ days to under 30 days within six months.

- Encourage end-users to use Kenna as a self-service portal. (drop the spreadsheets!)
    - Build risk meters for each remediation group and place users into specific roles so their view in Kenna focuses on what they need to fix.
    - Users will know what needs to be accomplished because the risk tolerance has been defined and documented.
    - When teams log into Kenna themselves, they can leverage the reporting and metrics that come with each risk meter.
- Educate leadership and organization on the Kenna Risk Score with the goal of it becoming a common metric across the company.
    - Encourage friendly competition between remediation teams using the language of Kenna and create positive performance-based incentives.
    - Develop specific reports on relevant risk meters for management so they can see how teams are progressing at a glance using metrics like MTTR and SLA adherence in addition to the overall Kenna Risk Score.

Step 3 - Optimize Kenna

- Create risk-based SLAs based on the policy and risk tolerance defined in Step 2.
    - Kenna generates SLAs automatically using our intelligence to guide you on the remediation time frame required to achieve your selected risk tolerance.
- Track progress using a variety of risk-based performance metrics.
    - Adjust the reporting timeline for the date range you want to track.
    - Metrics drive remediation because it holds teams' feet to the fire. For example:
        - Track SLA adherence using the Vulnerabilities by Due Date and Past Due Vulnerabilities by Risk Score and Past Due Vulnerabilities Over Time charts.
        - Track MTTR using the Mean Time To Remediate Vulnerabilities chart.
        - Track percentage of closed vs open vulnerabilities over time with the Vulnerability Count by Status donut graph.
        - Track decrease in high-risk vulnerabilities using the Total Vulnerabilities by Risk timeline.