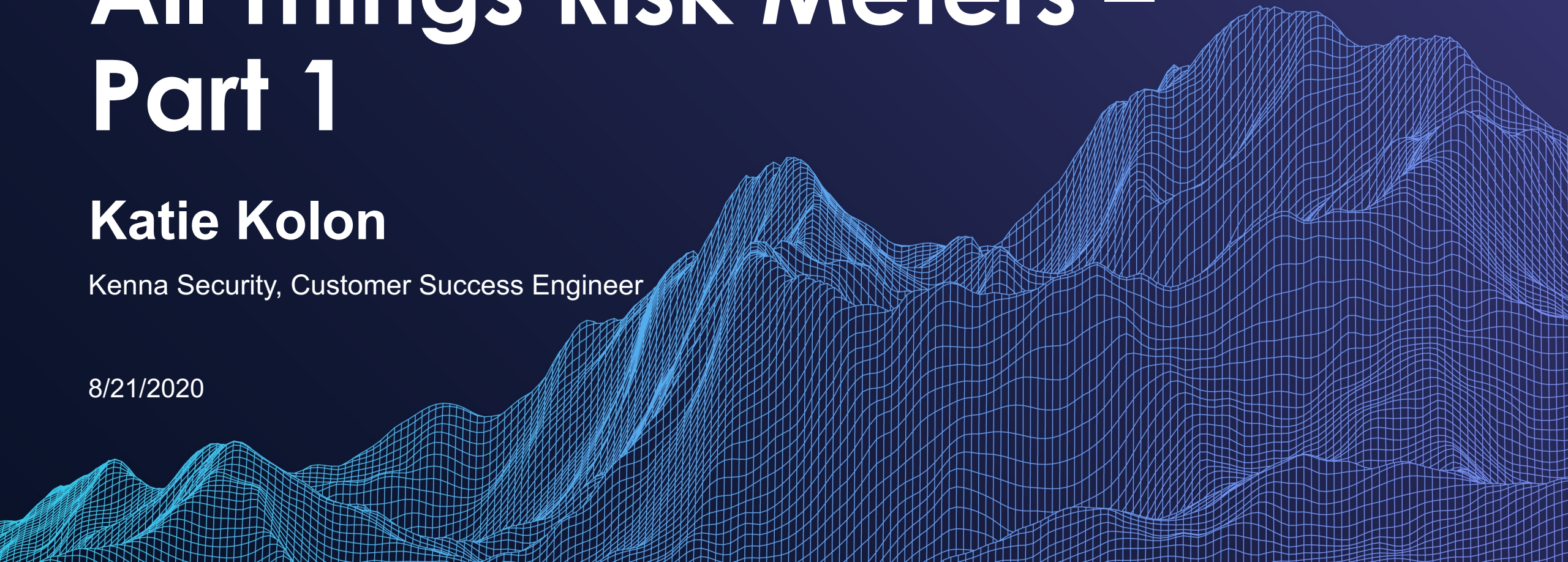
KENNA Security

All Things Risk Meters – Part 1

Katie Kolon

Kenna Security, Customer Success Engineer

8/21/2020



All Things Risk Meters – 2 Part Series

Part 1 – Best Practices for Organizing Your Data (Today)

- Risk Meter Introduction and Basics
  - Useful Categories of Risk Meters
  - Creating and Editing Risk Meters
  - Using Advanced Searching for Fancy Use Cases
- Risk Meter Organization
  - Dashboard Views
  - RBAC
  - Hierarchical Risk Meters

Part 2 – Reporting and Top Fixes (September)

KENNA Security

All Things Risk Meters – 2 Part Series

Part 1 – Best Practices for Organizing Your Data (August)

Part 2 – Reporting and Top Fixes (September)

- Reporting Overview, Use Cases
- Measuring Performance with Reporting
- How Reports Are Calculated
- Creating Reporting Templates
- Top Fixes Overview
- Top Fixes Best Practices

KENNA Security

Risk Meter Introduction and Basics

- What is a Risk Meter?

  A Risk Meter is a grouping of assets and their associated vulnerabilities created by saving a search.

- What does it provide?

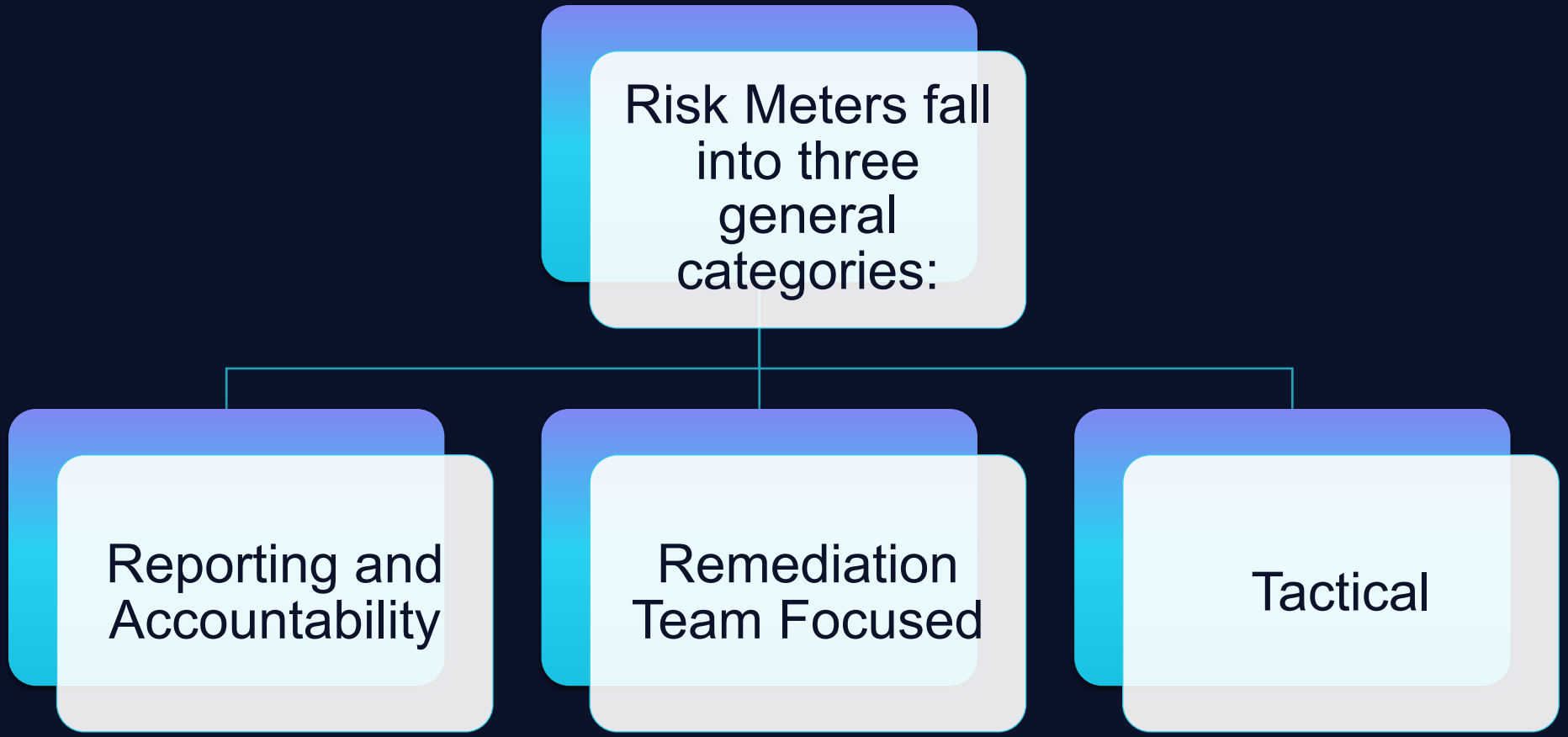
  Risk Meters provide reporting and Top Fixes, and are a way to monitor data, task out work, and measure performance.

- How is it scored?

  A risk meter score is the average of all non-zero scored assets in the group, ranging from 0-1000 (1000 being the most risky/critical).

KENNA Security

Useful Categories of Risk Meters



KENNA Security

Risk Meters for Reporting and Accountability

- Large asset groupings / Parent Risk Meters
  - Business units
  - Geographical areas
  - OS
- Reporting to management on progress
- Gauging remediation team's performance

KENNA Security

Remediation Team Risk Meters

- Asset groups by owner
- Asset groups by OS
- Asset groups by business unit
- Groups by vuln criticality

KENNA Security

Tactical Risk Meters

- Monitoring assets subject to PCI compliance
- Looking for high risk vulns that were seen in the last 7 days
- Monitoring for overdue vulns by SLA
- Checking for assets with manually set status such as assets that were recently seen but manually marked inactive
- Watching for a specific CVE (ex. Bluekeep 2019-0708)
- And countless others dependent on your use case

KENNA Security

Demo Time! – Creating and Editing Risk Meters

- Risk Meters are saved searches
- You can use the asset/vuln filters, the search box or a combination of the two
- The search box has an easy help shortcut with syntax and examples
- Search box is built on Apache Lucene Query Parser Syntax
- How you edit varies depending on whether HRM is turned on for you

KENNA Security

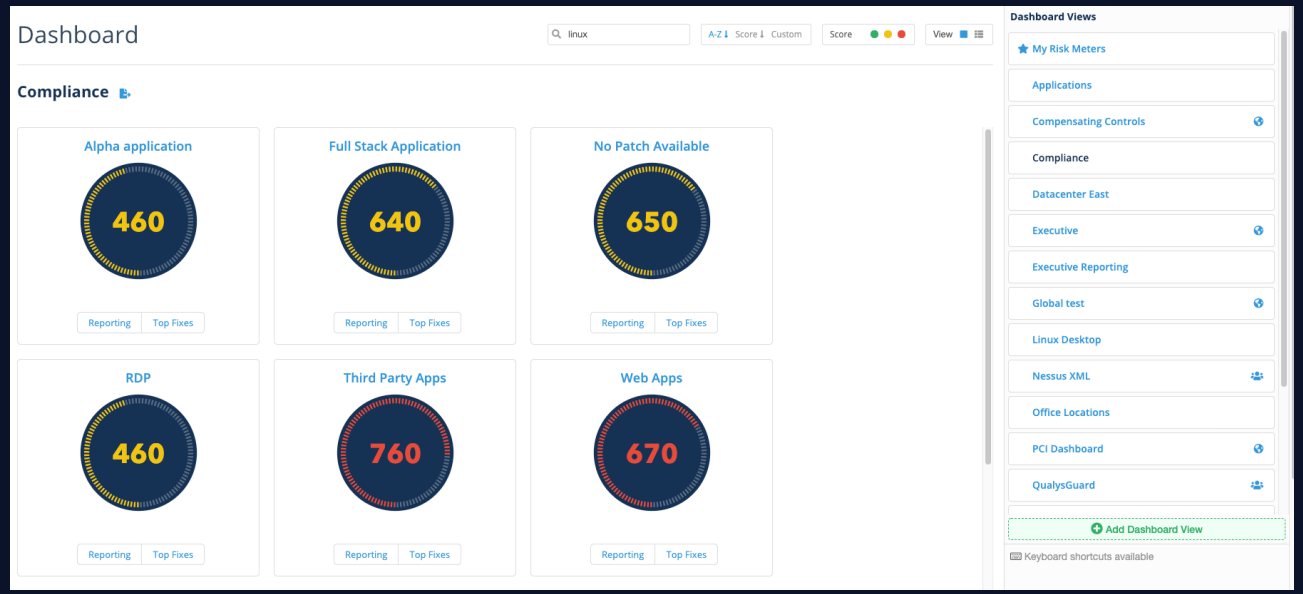
Demo Time!- Using Advanced Searching

- Checking for assets with manual override on status
  - asset_last_seen:<30d (old active assets which should be inactive per your inactivity limit)
  - asset_last_seen:>30d (inactive assets which have been seen recently and should be active)
- Vulnerabilities in breach of SLA
  - due_date:<now-7d (vulnerabilities past 1 week overdue)
  - not_closed_by_due_date:true
- Looking for recently found critical vulnerabilities that have a fix available
  - vulnerability_found:>now-7d AND vulnerability_score:>79 AND _exists_:fix
- Looking for highly critical Java vulnerabilities
  - fix_title_keyword: “java” AND vulnerability_score:>89
- Tips and Tricks
  - Date operators: h/d/w/m/y, now
  - Wildcards: * or ?
  - Logical Operators must be upper case: AND / OR
  - For searches between terms, only AND is supported
  - When searching for multiple options under one term, use parenthesis

KENNA Security

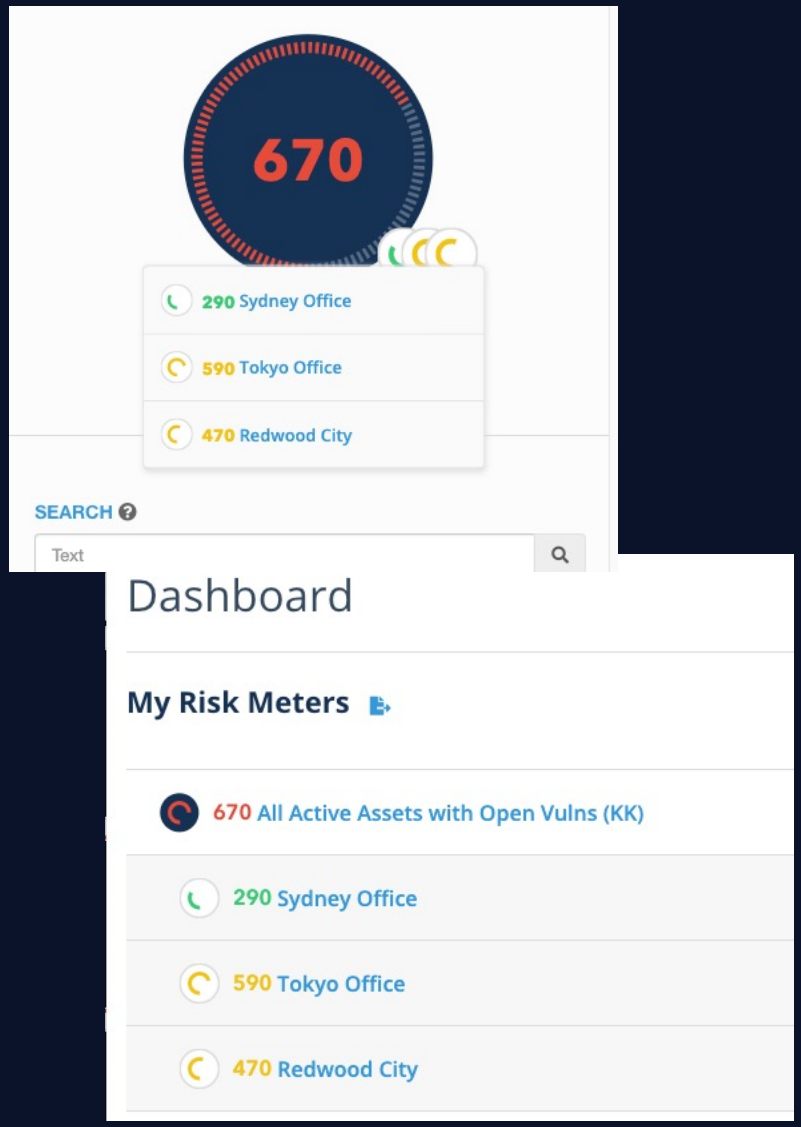
Demo Time! – Risk Meter Organization

- Dashboard Views
  - Use to organize your own view, or other users' views when there are many risk meters
- RBAC
  - Through user roles, you can also limit access by risk meter, which focuses users on what they need to see
  - Used in combination with HRM, by providing a user access to a parent risk meter, they receive access to all the children and the organizational structure therein



KENNA Security

Demo Time! – Hierarchical Risk Meters



- HRM is optional and must be enabled.
- Groups sidebar must be disabled to enable HRM.
- Descendants must be created anew. We cannot associate old risk meters as descendants of parents.
- All descendant risk meters inherit user role permissions from their parent, which helps with user role management.
- Editing/deleting a parent impacts all descendant risk meters.
- Each descendant risk meter (parent, child, grandchild etc) has its own independent Reporting and Top Fixes views.
- Each descendant risk meter has its own score.
- You may have 10 levels of descendants, but there is no limit to the number of descendants per level.

KENNA Security

All Things Risk Meters – 2 Part Series

Part 1 – Best Practices for Organizing Your Data (August)

Part 2 – Reporting and Top Fixes (September)

- Reporting Overview, Use Cases
- Measuring Performance with Reporting
- How Reports Are Calculated
- Creating Reporting Templates
- Top Fixes Overview
- Top Fixes Best Practices

KENNA Security

Q & A

KENNA
Security

Thank you

Katie Kolon

Kenna Security, CSE