KENNA
Security

Best Practices for Remediation

Katie Kolon and Katie Conners

Kenna Security, Customer Success Manager

12/18/2020

Best Practices for Remediation

Agenda

- Setting the Foundation
  - Ingesting Accurate Data
  - Organize with Tags/CMDB
  - Scheduling of Connector Runs
- Remediation Tools
  - Manageable Risk Meters for Remediation
  - Effective Use of Top Fixes
  - Leveraging SLAs
- Change Management
  - Incentives, gamification and positive reinforcement
  - Customer Examples
  - Interactive Poll

Tips on Setting the Foundation

- Ingest Accurate Data
  - Make sure the user account associated with the scanner brings all the scans you want to ingest and only the scans you want to ingest
  - The locator order of assets may need to be changed to avoid duplicate assets
- Organize data with tags or CMDB
  - Tags and CMDB may require cleanup before you bring in that data to Kenna
  - Tags help group assets into remediation buckets
  - CMDB helps bring in additional metadata used to group assets as well as asset owner
- Scheduling Connector Runs
  - The more frequently you scan, the more frequently you can run your connectors, resulting in faster updates to risk scores in Kenna
  - At a minimum, try to run your connectors as soon as possible after your scans complete

Remediation Tools

- Manageable Risk Meters for Remediation
  - Risk Meters by asset owner
  - Risk Meters by OS
  - Risk Meters by business unit
  - Risk Meters by vuln criticality
- Effective Use of Top Fixes
  - Use only with asset-based risk meters
  - Use in conjunction with Explore view or a Risk Meter focusing on critical vulns
- Leveraging SLAs
  - SLA adherence provides an effective measurement for remediation success
  - Once you are on top of your critical vulns and have reduced your risk score into the orange, consider switching to reducing your MTTR by following risk-base SLAs

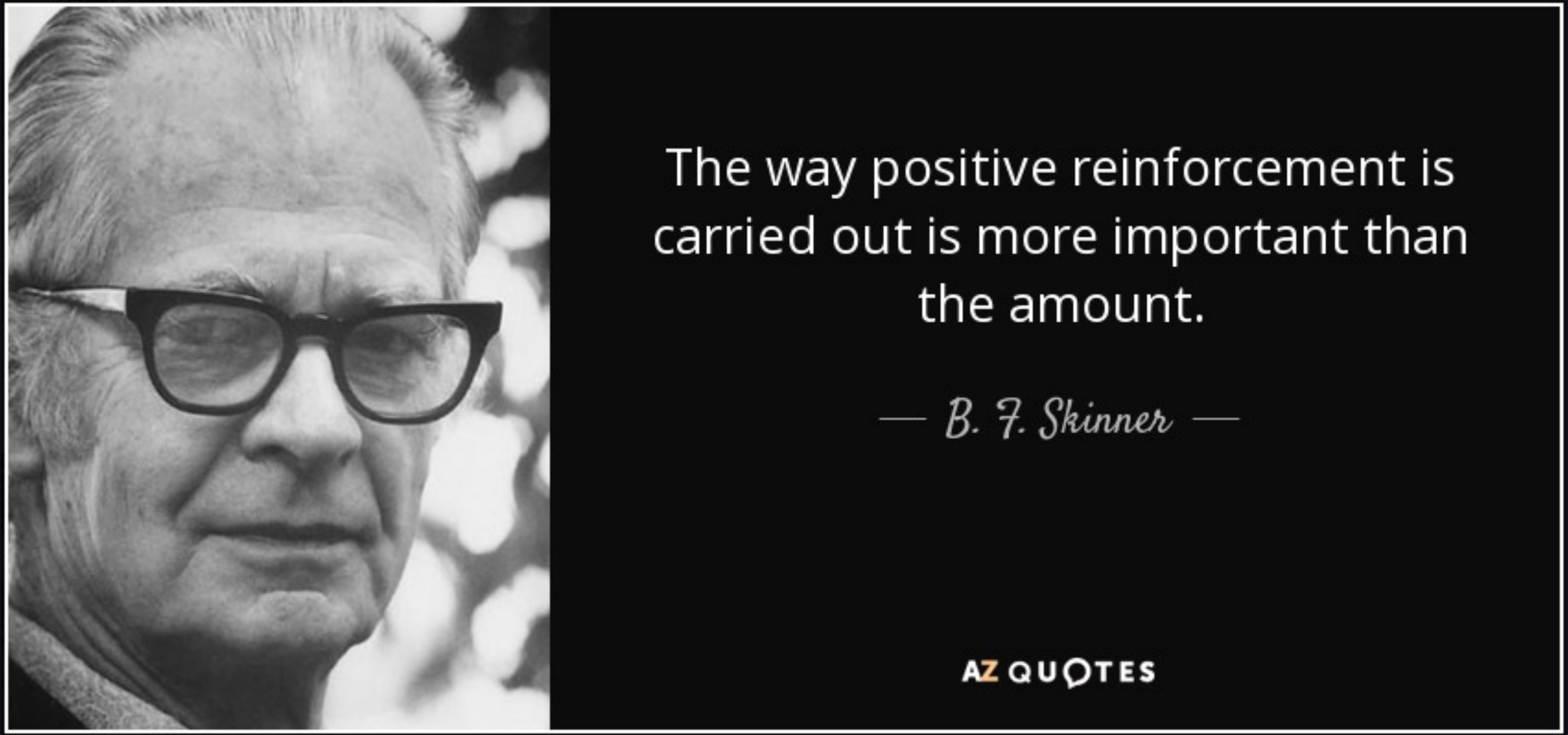
KENNA Security

Demo Time

- Show some example Risk Meters for Remediation (Windows HRM)
- Review use of Top Fixes
- Highlight reports on SLAs and MTTR
- Demo some useful SLA-based queries
  - *Fixed on Time* - Syntax: not_closed_by_due_date:false AND status:closed
  - *Fixed Late* - Syntax: not_closed_by_due_date:true AND status:closed
  - *Open and Late* - Syntax: not_closed_by_due_date:true
  - *Due within 30 Days* – Syntax: due_date:(<now+30d AND >now)

Change Management

Incentives, gamification, and positive reinforcement!



The way positive reinforcement is carried out is more important than the amount.

— B. F. Skinner —

AZ QUOTES

Change Management (See Resources for cheat sheet)

Step 1 – Use Threat Intel to Drive Remediation Decisions

- Let the Kenna patented algorithms do the hard work!
- Move to the Kenna Risk Score to drive remediation decisions rather than CVSS, scanner score, or the hottest new CVE

Step 2 – Operationalize Kenna

- Define your risk tolerance – What is an acceptable risk score to drive remediation?
- Once your tolerance is defined, document this in your Security policies
- Set short- and long-term SMART goals for positive reinforcement
- Encourage end-users to use Kenna as a self-service portal through incentives (drop the spreadsheets!)
- Educate leadership and organization on the Kenna Risk Score with the goal of it becoming a common metric across the company

Step 3 – Optimize Kenna

- Create risk-based SLAs based on the policy and risk tolerance defined in Step 2
- Track progress using a variety of risk-based performance metrics like SLA adherence and MTTR

KENNA Security

The Modern Vulnerability Management Journey

LOWER RISK

with continuously improving economics

infrastructure, applications, IoT

Table Stakes

- Prioritization & Action driven by CVSS or Scanner Score
- Security driven, IT resistance, limited justification for fixes
- Success = Reduce number of “high-risk” vulnerabilities

Intel Driven

- Prioritization & Action driven by threat intelligence on top of scanner score / CVSS
- Security driven, IT resistance, better justification for fixes
- Success = Reduce vulnerability risk score

Operationalized

- Risk-prioritized “next best action” driven by real-time threat intel and data science
- Shared incentives based on risk scores. IT self-serve remediation. Security focused on reporting, oversight, and exception handling
- Success = Risk Score as common metric across the business, with aligned goals

Optimized

- Risk-prioritized “next best action” driven by real-time threat intel, data science, organizational risk tolerance, and SLA adherence
- Shared incentives based on risk scores and agreed SLA’s. IT self-serve remediation. Security focused on reporting, oversight and exception handling
- Success = Systematic, ongoing response to discovered risk within target timeframes

Customer Examples and Discussion

Customer Examples

- Ensure leadership and remediation teams understand Kenna scoring and what is needed to achieve desired risk tolerance
- Create internal documentation around the Kenna methodology and what is expected
- Ease into goal expectations and set SMART goals within specific time frames (ex. Remediate all 90s and above in the first 90 days/risk meter score under 900)
- Set MBOs/bonuses based on achieving goals noted above
- Create friendly competitions between teams based on Kenna metrics
- Get your CISO involved in noticing and comparing team scores

Interactive Poll

What has worked for you and what has not?

KENNA Security

KENNA Security

KENNA Security

Thank you

Katie Kolon, Customer Success Operations Specialist

Katie Conners, Sr. Customer Success Engineer