RETHINK REMEDIATION - LINEAR VS. LIFECYCLE

Brendan Hourihan
Senior Consultant, Threat & Vulnerability Management Remediation
DISCUSSION GOALS

Our discussion goal is to illustrate why there is missing value within current remediation efforts and discuss the benefit of leveraging a lifecycle approach versus a linear one.

Remediation programs come in all shapes and sizes. Our purpose is to step through the basics on how remediation is handled and illustrate hidden value when we change our thinking how we approach this task.
RETHINK REMEDIATION? WHY?

It is important to think beyond a traditional linear approach to remediation and focus more on a lifecycle-based methodology.

• As today's threat landscape brings increasing challenge to organizations, many leverage a traditional "toolset centric" approach when assessing organizational risk.

• Although tools, talent and services help develop a risk profile, there is often an additional missing element that can restrict key risk visibility. That missing link is "how" organizations approach remediation.

• Objective: Illustrate “why” there is missing value within current remediation efforts and discuss the benefit of leveraging a lifecycle approach versus a linear one.
REMEDIATION RISK SCORING BASICS

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics, as shown in Figure 1.

https://nvd.nist.gov/vuln-metrics/cvss
When the Base metrics are assigned values by an analyst, the Base equation computes a score ranging from 0.0 to 10.0 as illustrated in Figure 2.
METRICS IN COMMON TOOLSETS
METRICS IN COMMON TOOLSETS
METRICS IN COMMON TOOLSETS

When the Base metrics are assigned values by an analyst, the Base equation computes a score ranging from 0.0 to 10.0 as illustrated in Figure 2.

Linear approach

Limited Context

Severity based remediation approach

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2021 Optiv Security Inc. All Rights Reserved.
Customers can have the best of breed toolsets, teams and policies available. However, there still may be questions surrounding overall remediation such as:

- “Why aren’t we getting ahead in our vulnerability remediation program?”
- “Why are we not seeing desired results?”
- “We have the toolsets but not sure if we are still missing something within our remediation program?”
START RETHINKING REMEDIATION

Knowing remediation is traditionally linear in nature, start taking some of those great questions and begin the thought journey towards a lifecycle approach:

• “Do we have insight into key toolsets that could improve overall remediation?”

• “Is our organization remediation program aligned with our risk tolerance?”

• “How do we gage our current remediation program effectiveness?”

• “Is our remediation strategy inclusive of some or all of our systems?”

• “What is missing within our current remediation program”
THE BEGINNING FROM LINEAR TO LIFECYCLE

When we start challenging traditional remediation concepts, organizations begin the transition towards more of a lifecycle approach

- Build context surrounding asset identification, technical & business owners as well as asset criticality
- Leverage integration with other systems within the environment to improve vulnerability visibility
- Understand remediation toolsets. Try to avoid toolset overlap or are not leverage all capabilities
- Challenge stakeholder remediation program efficacy. Assuming all is well can have consequences
Remediation Lifecycle

Measurable outcomes / Toolset alignment

Risk Acceptance
Establish Indicators
Toolset Efficacy
Use Metrics That Work
Full Org. Support
Asset database (CMDB)
Endpoint Security
Active Directory
Capture all Devices
Threat Discovery
Assess Controls
Understand Organizational Risk

Measure Program effectiveness

Asset Discovery & Prioritization

Improved Remediation Context
Asset Lifecycle Visibility

Repeatable

Measurable

VISUALIZING TRANSFORMATION

Desired Future State

Establish Indicators
Toolset Efficacy
Use Metrics That Work
Full Org. Support
Asset database (CMDB)
Endpoint Security
Active Directory
Capture all Devices
Threat Discovery
Assess Controls
Understand Organizational Risk

Measure Program effectiveness

Asset Discovery & Prioritization

Improved Remediation Context
Asset Lifecycle Visibility

Repeatable

Measurable

Remediation

Full Org. Support
Asset database (CMDB)
Endpoint Security
Active Directory
Capture all Devices
Threat Discovery
Assess Controls
Understand Organizational Risk

Measure Program effectiveness

Asset Discovery & Prioritization

Improved Remediation Context
Asset Lifecycle Visibility

Repeatable

Measurable

Remediation

Full Org. Support
Asset database (CMDB)
Endpoint Security
Active Directory
Capture all Devices
Threat Discovery
Assess Controls
Understand Organizational Risk

Measure Program effectiveness

Asset Discovery & Prioritization

Improved Remediation Context
Asset Lifecycle Visibility

Repeatable

Measurable

Remediation

Full Org. Support
Asset database (CMDB)
Endpoint Security
Active Directory
Capture all Devices
Threat Discovery
Assess Controls
Understand Organizational Risk

Measure Program effectiveness

Asset Discovery & Prioritization

Improved Remediation Context
Asset Lifecycle Visibility

Repeatable

Measurable

Remediation
THANK YOU FOR YOUR TIME!

Questions or Comments?