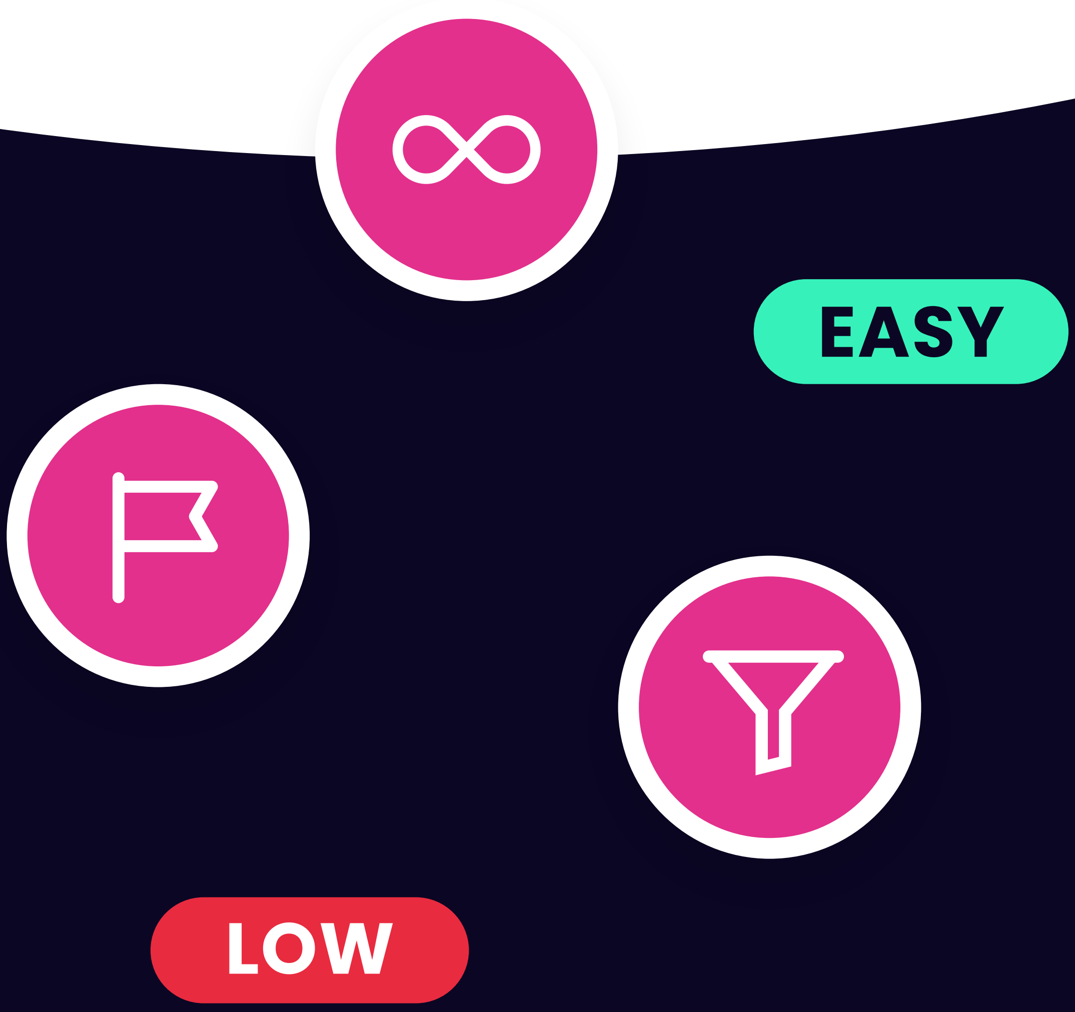
seemplicity

Fix More, Prioritize Less:

A comparison of two Approaches to Remediation



Enterprises face new security threats daily. Whilst keeping up with the influx of these threats has become a top priority for security teams, the average organization still finds itself with a backlog of more than 57,000 unfixed security issues within 6 months.

This ever-increasing security backlog is often owned by the security team, whilst the remediation (i.e. development and IT) teams who are the ones who can actually fix the backlog issues are often left in the dark. With security acting as the intermediator (i.e. “the good middleman”) between security findings and remediation, remediation scope is often determined by what the security team can prioritize rather than what the remediation team is capable of fixing. With this long-standing approach in place, risk-based vulnerability prioritization tools have come about with the aim to make the prioritization process smarter and automated.

But what if remediators received findings straight from the horse’s mouth, in other words, with security acting as a supporter rather than an intermediator? This approach can be referred to as Disintermediation.

Disintermediation is the "cutting out the middlemen" in connection with a transaction or a series of transactions. If we put disintermediation into the context of our daily life it’s like Uber or Netflix. Today, you no longer need to call a cab station to order a taxi, or go to Blockbusters to borrow a movie. Everything is now directly connected to the consumer. Bringing this back to remediation, disintermediation connects findings directly to the fixers, with the security team acting as the enabler rather than gatekeeper. As Jeff Bezos said, “Even well-meaning gatekeepers slow innovation.” If we want to continue to innovate at an accelerated rate, the gatekeepers must go.

Below we examine two approaches to driving remediation - prioritization and disintermediation to help you decide what path makes sense for your organization.

	PRIORITIZATION	DISINTERMEDIATION
Scope of discovered weaknesses	Dependent on the number of tools used and environments scanned	
Findings-to-Remediation Funnel	Distributed findings, centralized remediation	Centralized findings, distributed remediation
Determining factor of what gets remediated	Prioritization	Remediation capacity
Remediation scope	As wide as the security team **can prioritize**	As wide as the remediation team **can fix**
Visibility to weaknesses	Only the security team has visibility (and are mostly aware of just the prioritized weaknesses). Remediation teams have no ongoing visibility	Both security and remediation teams have full ongoing visibility of the weaknesses that are planned to be/in progress of being/have been remediated

Ownership of the security backlog	Solely owned by the security team	Shared ownership between security and Development/ IT Ops
Involvement of security team from identification to remediation	HIGH Operating the entire process	LOW Manage by exception, governing and supporting the process
Ability to identify team-level impediments and blindspots	HARD No clear picture of how weaknesses are distributed across the remediation organization	EASY Continuous visibility into how weaknesses are spread across the remediation organization
Remediation capacity utilized at any point in time	LOW UTILIZATION Only prioritized items are being remediated, even if a single team is responsible for all the items and all other teams are left with no security bugs	HIGH UTILIZATION Each remediation team handles as many security bugs as they can handle at any point in time
Ability to remediate longer-term weaknesses	LOW In a state of **reactive** firefighting	HIGH In a state of **proactive** prevention
Remediation methodology	Waterfall and post-hoc	Agile and continuous
Time-to-remediation	Time taken to process by the security team + Time taken to remediate by the remediation team	Time taken to remediate by the remediation team only

About Seemplicity

Seemplicity revolutionizes the way security teams drive risk down access the organization by orchestrating, automating and scaling all risk reduction workflows in one workspace. With their very own dedicated workflow platform, security teams are empowered to turn risk reduction into a self-service process that can be easily consumed by developers, DevOps and IT across the organization, in a simple, effective and collaborative manner that ultimately accelerates time-to-remediation and improves the overall security posture of the organization.

Learn more at seemplicity.io