



VULCAN

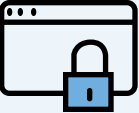



# **Enterprise Security and IT Teams Think Their Vulnerability Management Programs Are More Mature Than They Actually Are**



2020 is the worst. Already notorious for its epic struggles, 2020 is now on pace to deliver the most disclosed vulnerabilities ever. This combined with a rapidly shrinking window between vulnerability disclosure and vulnerability exploit, plus expanding, more-complex digital infrastructure, plus fewer resources to remediate vulnerabilities, and we have a perfect storm brewing for cyber security fail.

Vulcan Cyber commissioned research in collaboration with Pulse to determine the readiness of enterprise vulnerability management teams (cross-functional security and IT operations teams) to weather the approaching perfect storm. We wish we had positive findings to report at a time when it's more critical than ever for companies to have strong vulnerability management programs that deliver nothing short of remediation. However, while the vast majority think their programs are mature, there is a notable disconnect between perception and reality.

### The Vulnerability Remediation Maturity Model

			
Stage 1	Stage 2	Stage 3	Stage 4
<b>Reactive</b>	<b>Data-Driven</b>	<b>Orchestrated</b>	<b>Transformative</b>
Manage vulnerabilities on a case-by-case basis	Take customized, prioritized action on vulnerability, threat, and asset data	Remediate vulnerabilities at speed and scale	Rally the business and key stakeholders around cyber hygiene

[Click here](#) to download *The Vulnerability Remediation Maturity Model* eBook.

This survey of 100 IT and security leaders finds most companies' vulnerability management programs aren't as mature as they think they are, especially when it comes to end-to-end vulnerability remediation.

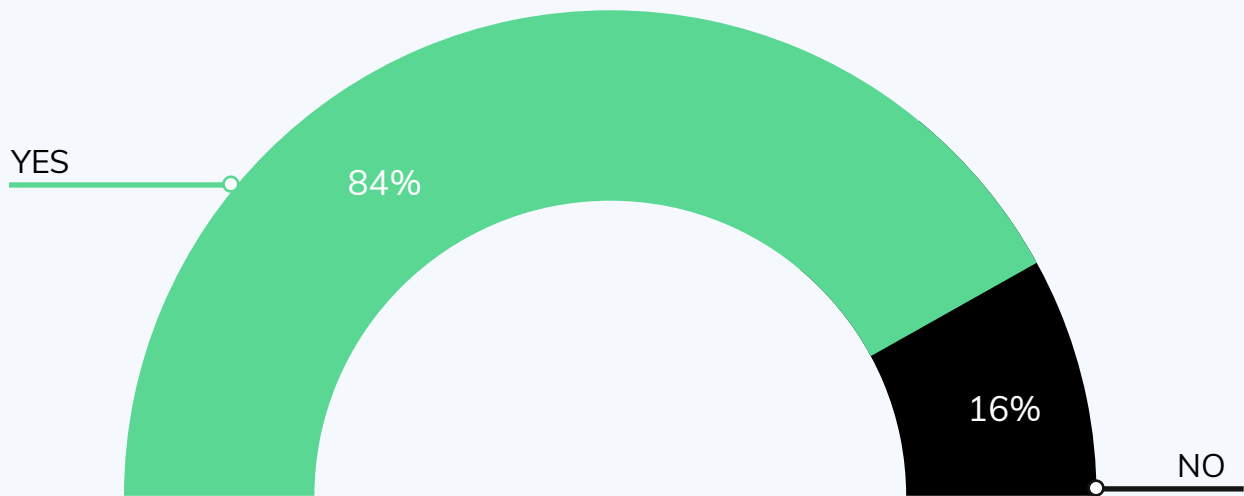
Data collected from June 26 - July 17, 2020

Respondents: 100 IT and security leaders

- Respondents may claim their programs are mature, but the data says otherwise

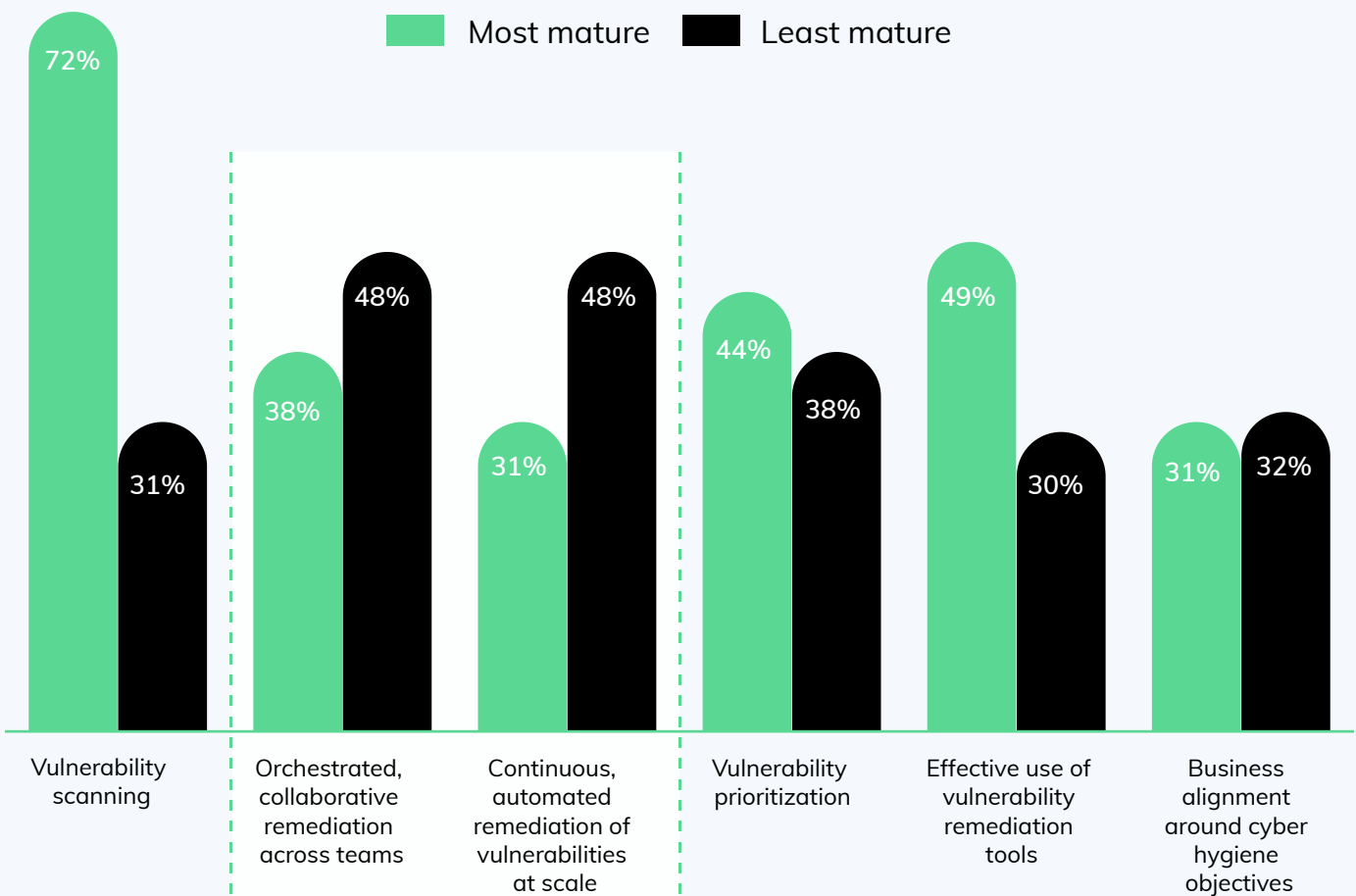
84% of IT and security leaders believe their security vulnerability remediation programs are mature.

DO YOU BELIEVE YOUR VULNERABILITY REMEDIATION PROGRAM IS MATURE?



However, most respondents said vulnerability scanning is the most mature element of their security vulnerability remediation strategy—which is only step #1 in a truly mature program.

### WHICH 3 ASPECTS OF YOUR SECURITY VULNERABILITY REMEDIATION PROGRAM ARE MOST AND LEAST MATURE?

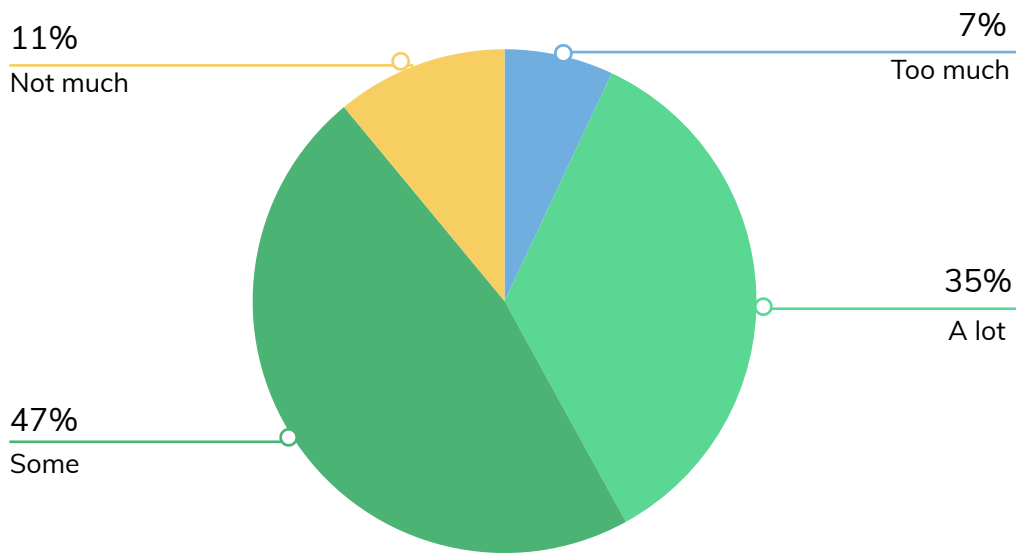


**Orchestrated, collaborative remediation and continuous, automated remediation are the least mature elements of most security vulnerability remediation strategies. These are vital elements of a mature, comprehensive program.**

- **Security vulnerability remediation processes are hindered by inefficient collaboration**

**89%** of security and IT teams spend at least some time collaborating with cross-functional teams. Efficiency is imperative, therefore boosting the maturity of orchestrated, collaborative remediation is vital for these companies.

**HOW MUCH TIME DO YOU SPEND WORKING WITH OTHER TEAMS ON VULNERABILITY REMEDIATION, FROM SCAN TO FIX?**



**HOW MANY COMPANIES IN THE FOLLOWING INDUSTRIES SPEND AN ABOVE AVERAGE AMOUNT OF TIME (i.e. a lot or too much) ON SECURITY VULNERABILITY REMEDIATION?**



**67%**

Transportation and Warehousing



**60%**

Software



**57%**

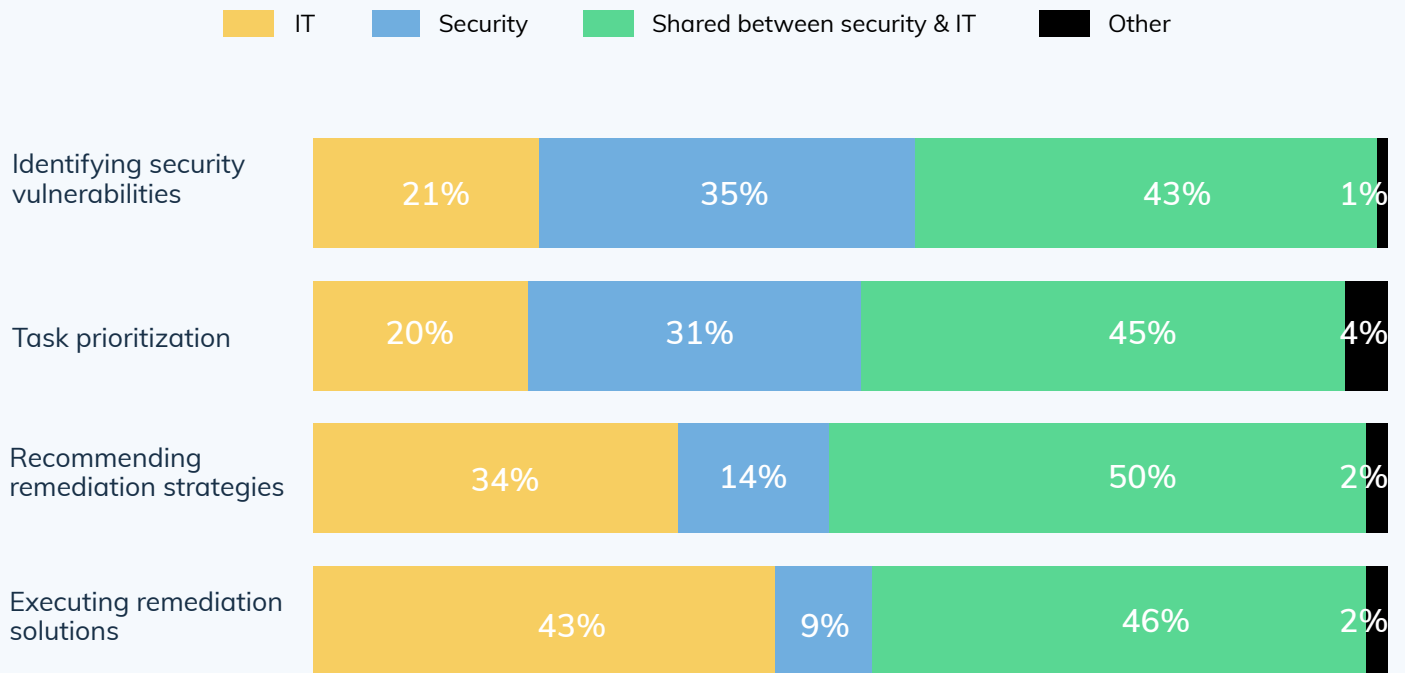
Finance and Insurance

**83%** of companies with 500-1,000 employees spend too much time collaborating on security vulnerability remediation activities.

## ● Why is collaboration inefficient?

The majority of respondents say both IT and security teams share responsibility for security vulnerability remediation.

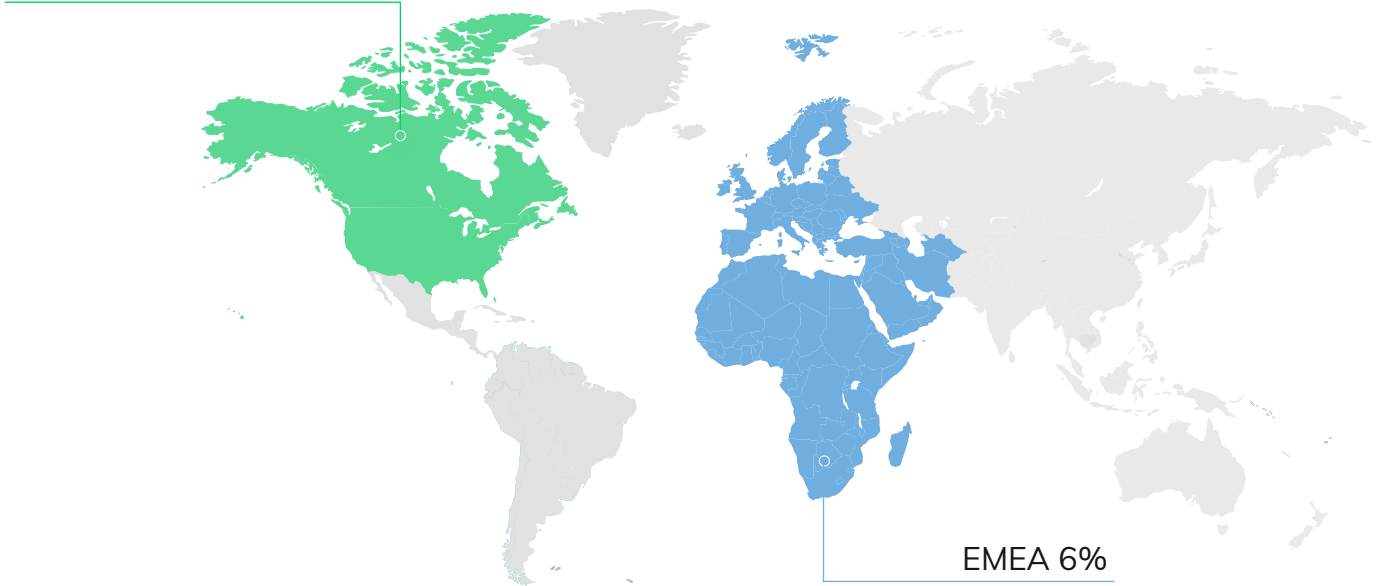
### WHICH TEAM IS RESPONSIBLE FOR EACH STAGE OF THE SECURITY VULNERABILITY REMEDIATION PROCESS?



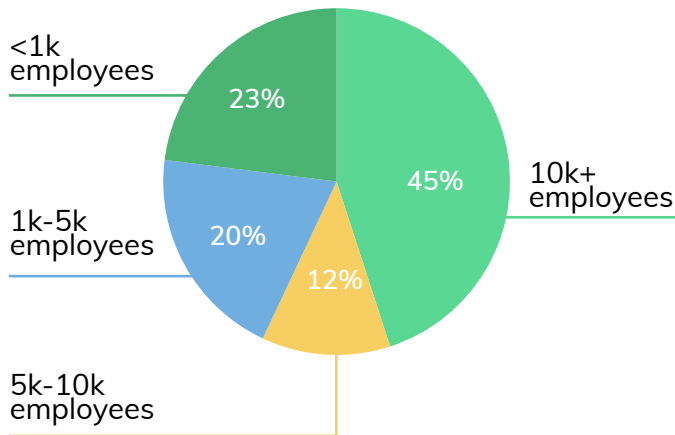
# Respondent Breakdown

## LOCATION

North America 94%



## COMPANY SIZE



## TITLES

