HOW TO REALLY REPORT RISK TO THE BOARD

VERITI

VERITI.AI

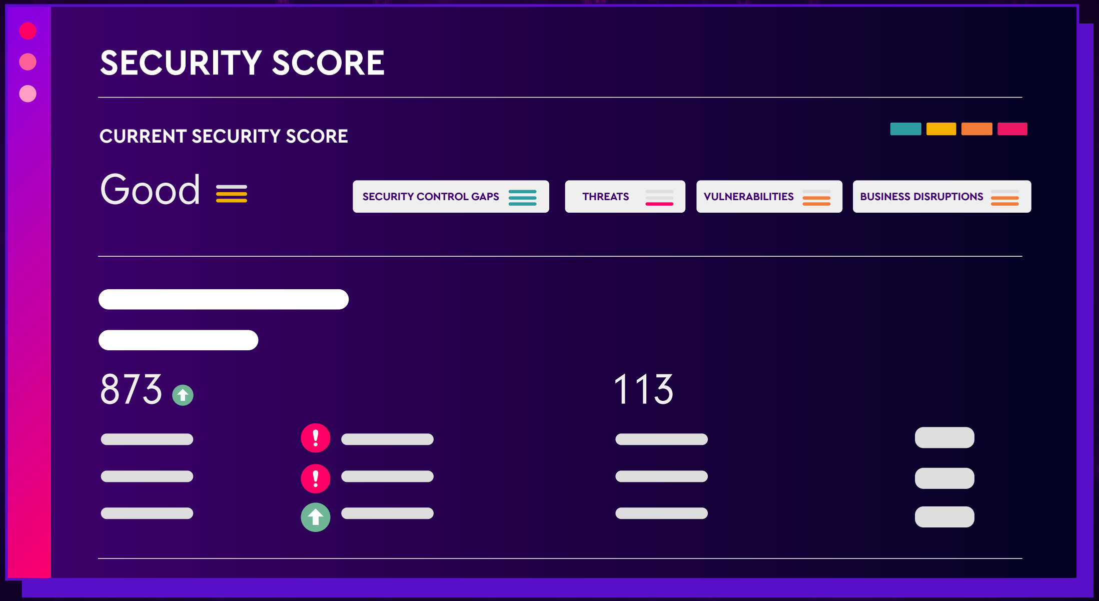
TABLE OF CONTENTS

INTRODUCTION

Reporting risk to the board is not just about identifying threats; it's about demonstrating the value of your security efforts. The key to effective communication lies in presenting not only the risks but also the impact of the remediations you've performed. This approach helps the board understand the true security posture of the organization, which includes both the challenges and the actions taken to address them.

START WITH THE BIG PICTURE

The first step in reporting risk to the board is to give an overview of the organization's current security posture. This should include a summary of the overall security score, which reflects the effectiveness of the security measures in place. However, rather than just stopping at what's wrong, also highlight what has been done to improve this score. Show the progression and the impact of these improvements over time.



METRICS THAT MATTER

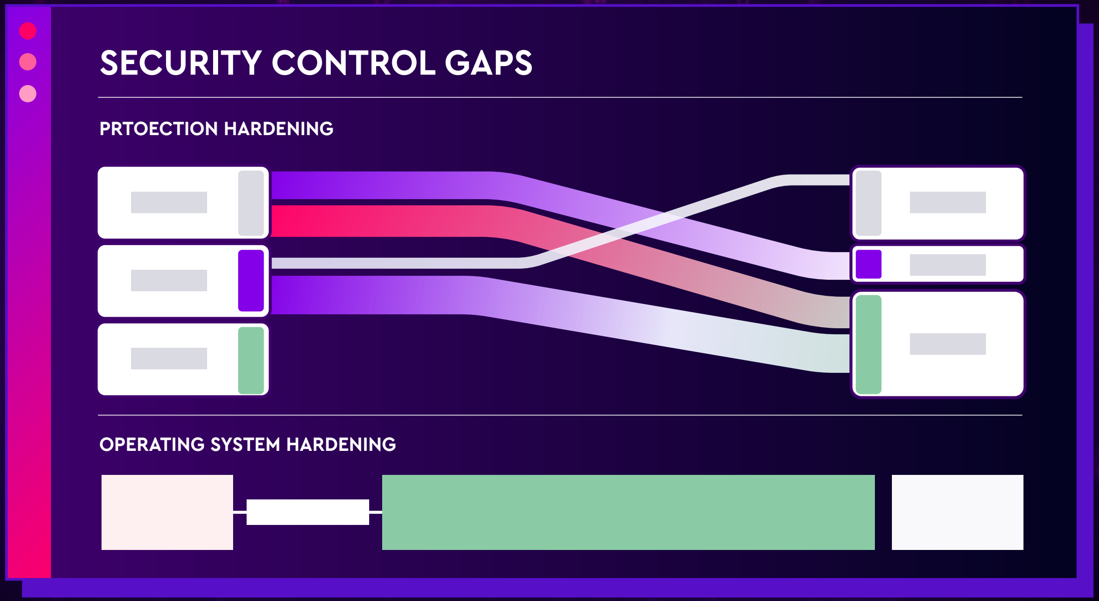
SECURITY CONTROL GAPS

Security control gaps represent the weaknesses in your security configurations that could be exploited by attackers. In this section, report on:

IDENTIFIED GAPS
The number and types of security control gaps discovered.

REMEDIATED GAPS
The specific actions taken to close these gaps.

IMPACT
How closing these gaps has improved the overall security posture, reduced potential attack vectors, and enhanced business continuity.



METRICS THAT MATTER

THREATS

Threats are potential incidents that could harm the organization if not mitigated. When reporting on threats, include:

DETECTED THREATS

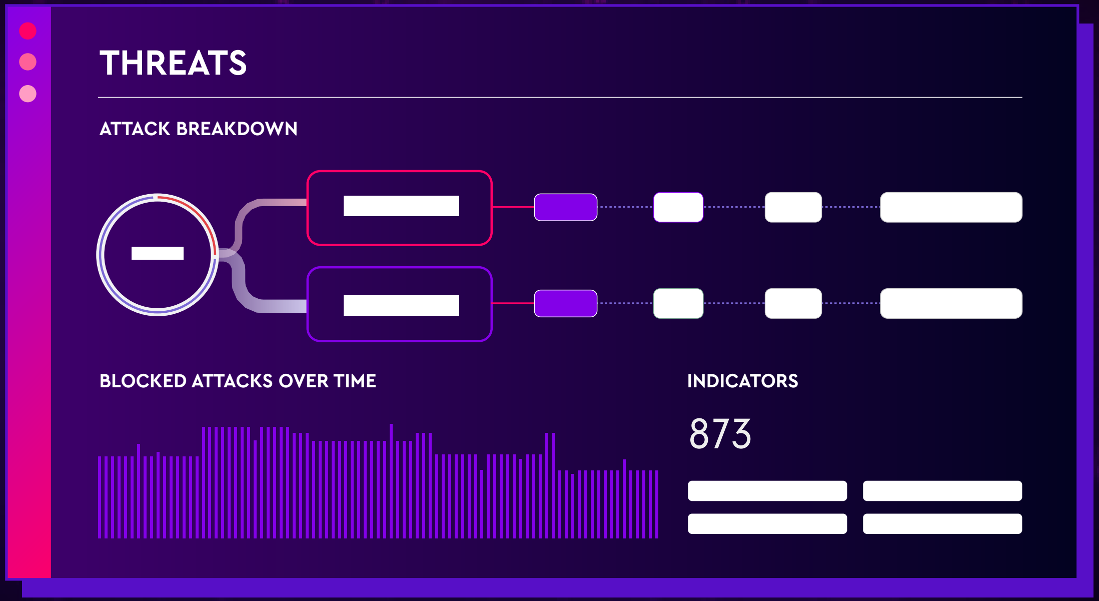
The total number of threats identified, broken down by type (e.g., malware, phishing, etc.).

NEUTRALIZED THREATS

Actions taken to prevent these threats from causing damage.

IMPACT

Highlight how these actions have reduced the risk of successful attacks, emphasizing the effectiveness of your threat detection and response strategies.



METRICS THAT MATTER

VULNERABILITIES

Vulnerabilities are weaknesses that could be exploited by attackers to gain unauthorized access to systems or data. This section should cover:

DISCOVERED VULNERABILITIES

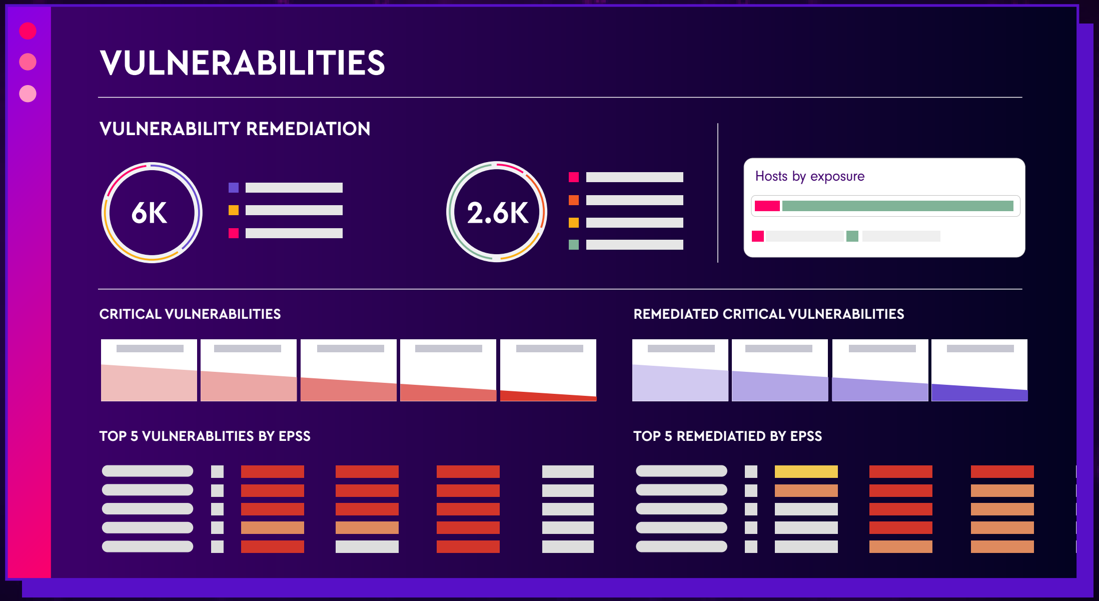
The number and severity of vulnerabilities found in the system.

REMEDIATED VULNERABILITIES

The specific steps taken to address these vulnerabilities, such as patching or applying compensating controls.

IMPACT

Show how these actions have reduced the organization's exposure to potential attacks, improving the security score and overall risk profile.


VULNERABILITIES
VULNERABILITY REMEDIATION
6K
2.6K
Hosts by exposure
CRITICAL VULNERABILITIES
REMEDIATED CRITICAL VULNERABILITIES
TOP 5 VULNERABLITIES BY EPSS
TOP 5 REMEDIATIED BY EPSS

METRICS THAT MATTER

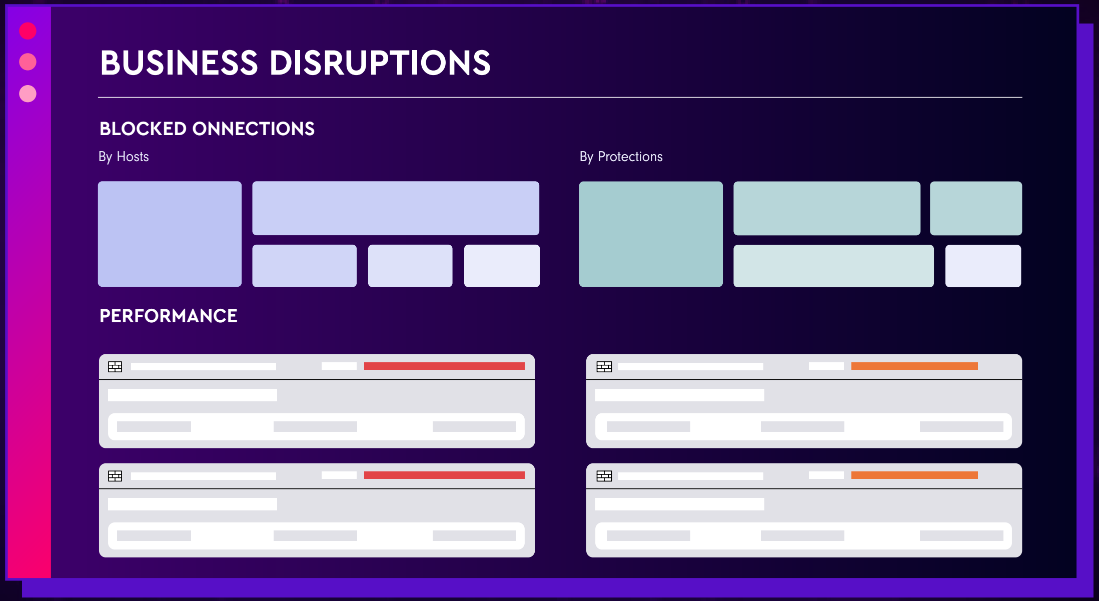
BUSINESS DISRUPTIONS

Business disruptions are events that can negatively impact operations, such as system downtime caused by security incidents. Report on:

IDENTIFIED DISRUPTIONS:
The number of disruptions that were linked to security issues.

PREVENTATIVE ACTIONS:
Measures taken to prevent these disruptions, including the use of AI to mitigate false positives.

IMPACT:
Demonstrate how these actions have maintained business continuity and minimized operational impact, contributing to a stronger security posture.
exposure to potential attacks, improving the security score and overall risk profile.



METRICS THAT MATTER

HIGHLIGHT COMPLETED REMEDIATIONS

Boards are often concerned with how risks are being mitigated. Instead of merely listing potential threats, showcase the remediation actions that have been completed. Break down the number of remediated vulnerabilities, configuration gaps closed, and threats neutralized. This demonstrates proactive management and the ongoing effort to reduce risk.

COMPLETED REMEDIATIONS

408 +20

ATTACKS BLOCKED

in the last week

25,300

DEMONSTRATE IMPACT WITH METRICS

Numbers speak volumes. Provide metrics that quantify the impact of your security efforts. Key metrics might include:

COST SAVINGS
Highlight the financial benefits of the remediations, such as reduced potential losses from breaches.

MTTR (MEAN TIME TO REMEDIATE):
Show how quickly the team responds to and fixes vulnerabilities, emphasizing the efficiency and effectiveness of your processes.

LABOR HOURS SAVED:
Quantify the time saved through automation or process improvements, which directly correlates to cost efficiency.

LABOR SAVED	20H	+1.2H
COST SAVINGS	$2350	+$307
MTTR	5H	+1H

SHOW THE RIPPLE EFFECT ON SECURITY POSTURE

Beyond individual remediations, it's crucial to show how these actions have improved the overall security posture of the organization. For example, how has closing a specific vulnerability reduced the attack surface? How has the automation of patch management contributed to consistent security across all endpoints? This section should focus on the broader impact of your remediations.

CVE-2023-38146

EPSS 90.52%
Windows Themes Remote Code Execution Vulnerability
2x Hosts are vulnerable
192.100.1.153 – XXX-DXXXX3
192.100.1.154 – XXX-XXXXX3

REMEDIATION:
Protection Activation -> Inactive to Detect mode

EXAMPLE

Attackers can exploit a known vulnerability in Microsoft Windows (CVE-2023-38146).

The attack goes unnoticed at the network layer, not initially detected.

Enhance the organizations existing system with threat intelligence by enabling protections.

INCLUDE FORWARD-LOOKING STATEMENTS

Boards need to know not only what has been done but also what is planned. Provide insights into upcoming remediations, the expected impact of these actions, and how they align with the organization's overall security strategy. This forward-looking approach reassures the board that security is not just reactive but proactive.

AVAILABLE REMEDIATIONS

121

Expected Labor Saved	16 H
Projected Cost Savings	$ 1150

NEXT THREE MONTHS

SECURITY SCORE

Great

COMPLETED

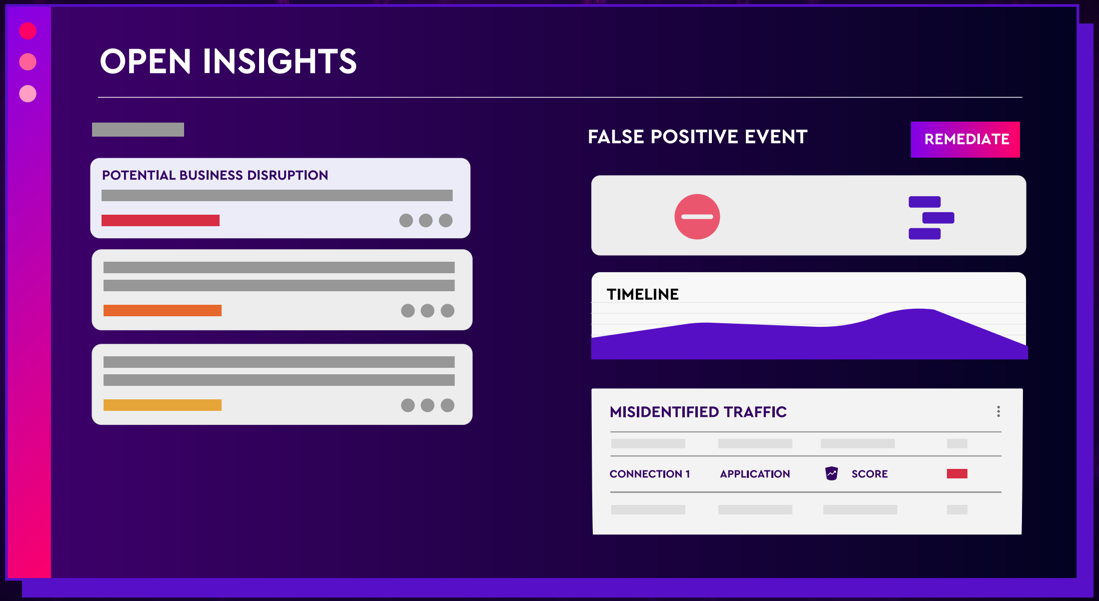
2,200	556% ↑

MTTR

6 Days	45% ↑

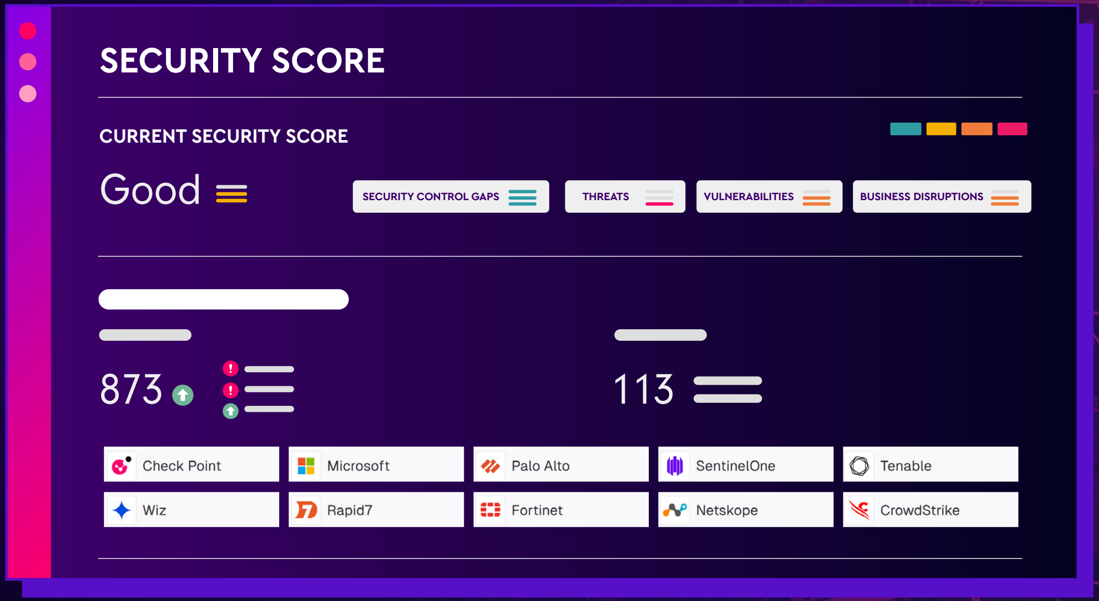
ALIGN SECURITY WITH BUSINESS OBJECTIVES

Finally, tie everything back to the business. The board needs to understand how your security efforts support the organization's goals. Whether it's ensuring business continuity, protecting intellectual property, or maintaining customer trust, make it clear that your security actions are designed to support and enable the business, not just protect it.



CONCLUSION

To really report risk to the board, focus on more than just the threats. Present a comprehensive view of the organization's security posture by highlighting the risks alongside the completed remediation actions and their tangible impacts. Demonstrate how these efforts have improved key metrics like cost savings, MTTR, and business continuity, clearly showing the board the value and effectiveness of your security strategy.



SECURITY SCORE

CURRENT SECURITY SCORE

Good

SECURITY CONTROL GAPS
THREATS
VULNERABILITIES
BUSINESS DISRUPTIONS

873

113

Check Point	Microsoft	Palo Alto	SentinelOne	Tenable
Wiz	Rapid7	Fortinet	Netskope	CrowdStrike

VERITI

Veriti’s agentless approach integrates with your entire security stack, continuously monitors for exposures from the OS-Level and upwards and ensures potential and actual threats are managed proactively without business disruption. It addresses every facet of your exposures and adjusts for the ripple effects of remediation actions to ensure business continuity.

VERITI.AI