COALFIRE

Coalfire Exposure Management Services for Tenable One

Find vulnerabilities and prioritize remediation to reduce your attack surface

Vulnerabilities exist in all organization's systems, whether in infrastructure, code, web applications, containers, or any new emerging technology. Identifying these vulnerabilities is a good starting point but insufficient to reduce the threat exposure and risk that adversaries pose to an organization. Coalfire® Exposure Management services focus on a holistic approach and process to help organizations go beyond vulnerability identification and manage vulnerabilities to ensure they reach a known accepted end-state, whether it be:

Determined as a false positive, remediated, mitigated, or classified into a specific risk bucket for review in the future.

Coalfire's exposure management services assess vulnerabilities to prioritize and address the highest risk areas, helping organizations strengthen their security posture and reduce their attack surface.

Comprehensive Exposure Management Solution to Reduce Your Attack Surface

Coalfire partners with Tenable, a leader in exposure management, to deliver expert services that enhance the Tenable One platform and empower organizations to manage their exposure effectively. With Coalfire's deep expertise in helping large enterprises identify risks and strengthen their security posture, combined with Tenable's cutting-edge vulnerability and exposure management capabilities, businesses benefit from a powerful solution that reduces their attack surface and defends against adversaries looking to exploit vulnerabilities.

The Coalfire Exposure Management services provide a programmatic approach to deliver all parts of the exposure management process that are relevant to your organization. The services build upon a process that focus on the following.

- **Attacker inventory:** A key element of an effective threat exposure management program is maintaining an asset inventory that mirrors the assets attackers are likely to target - this requires aligning various asset inventories, including:
  - Known-known assets from a configuration management database (CMDB)
  - Known-unknown assets from investigating disparities between scanners and their CMDB
  - Unknown-unknown assets, by proactively looking for new assets using tools such as Attack Surface Management (ASM)
- **Maximize scan scope:** Ensure a scanning strategy that clearly defines asset exclusion criteria and expected authentication requirements (such as using agents) to give high-accuracy results.
- **Remediate:** Identify remediation teams based on asset ownership and establish a regular cadence to ensure each team drives the vulnerability to an acceptable state within established timeframes.
- **Govern:** Ensure proper documentation and governance are in place at every step. As vulnerability management is a team effort, ensuring well-documented roles and responsibilities and gathering the necessary data is essential to driving the company's internal decision process.

To learn more about the Coalfire Exposure Management Services for Tenable One or get started, **contact us.**

Copyright © 2024 Coalfire Systems, Inc. All rights reserved. Coalfire, the Coalfire Logo, CoalfireOne, the Coalfire|Talks Logo, the Hexagon Logo, Hexeon, Neuralys, RAMP/pak, RAMP/pak+, RAMPcon, the RAMPcon Logo, and ThreadFix are trademarks or registered trademarks of Coalfire Systems, Inc. or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.