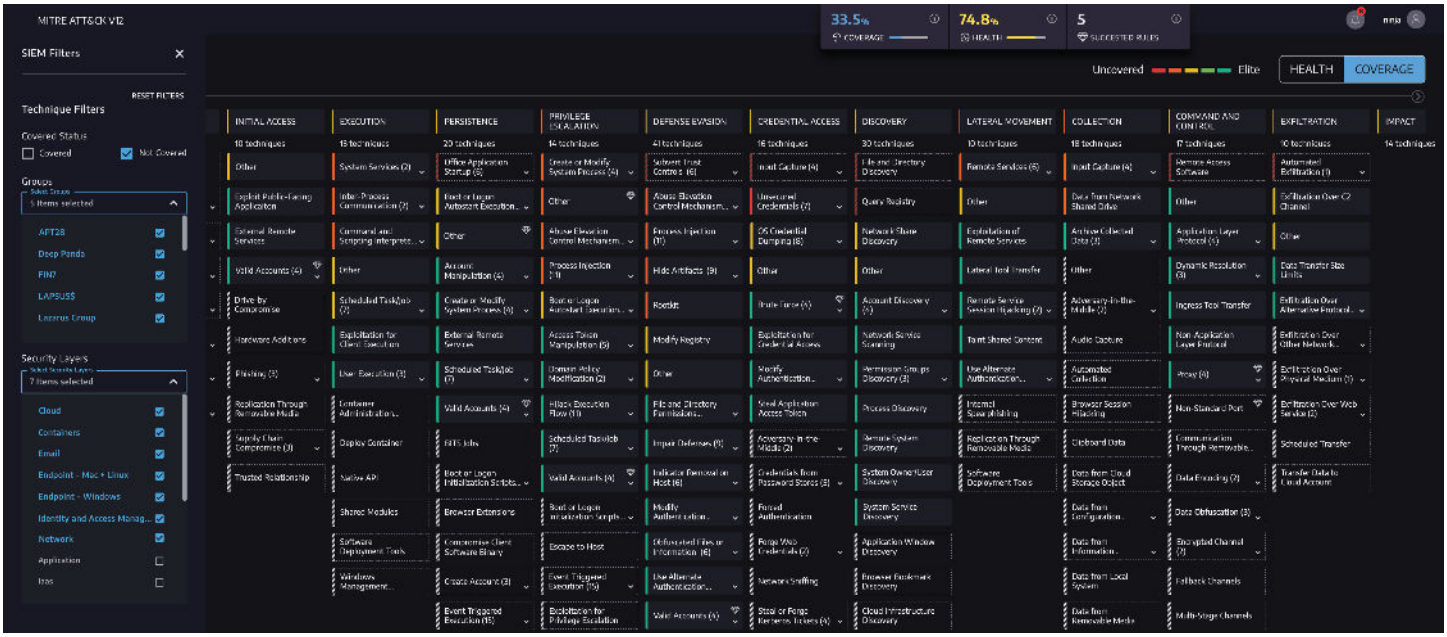
CARDINALOPS

Eliminate Detection Coverage Gaps with Automation and MITRE ATT&CK

Implement a Threat-Informed Defense for Your SIEM/XDR

SOC detection tools, such as SIEM/XDR and centralized log management systems, still serve as the operating system of most SOCs. And although they are capable of providing comprehensive threat coverage, they are typically undermanaged, misconfigured, highly dependent on tribal knowledge, and not optimized to cover the highest-priority MITRE ATT&CK techniques relevant to an organization. These implementation and maintenance gaps have remained difficult for detection engineers to manage and leave enterprises exposed to a large array of attacks without any visibility to their detection posture.

Eliminate ATT&CK Coverage Gaps that Leave Your Organization Exposed



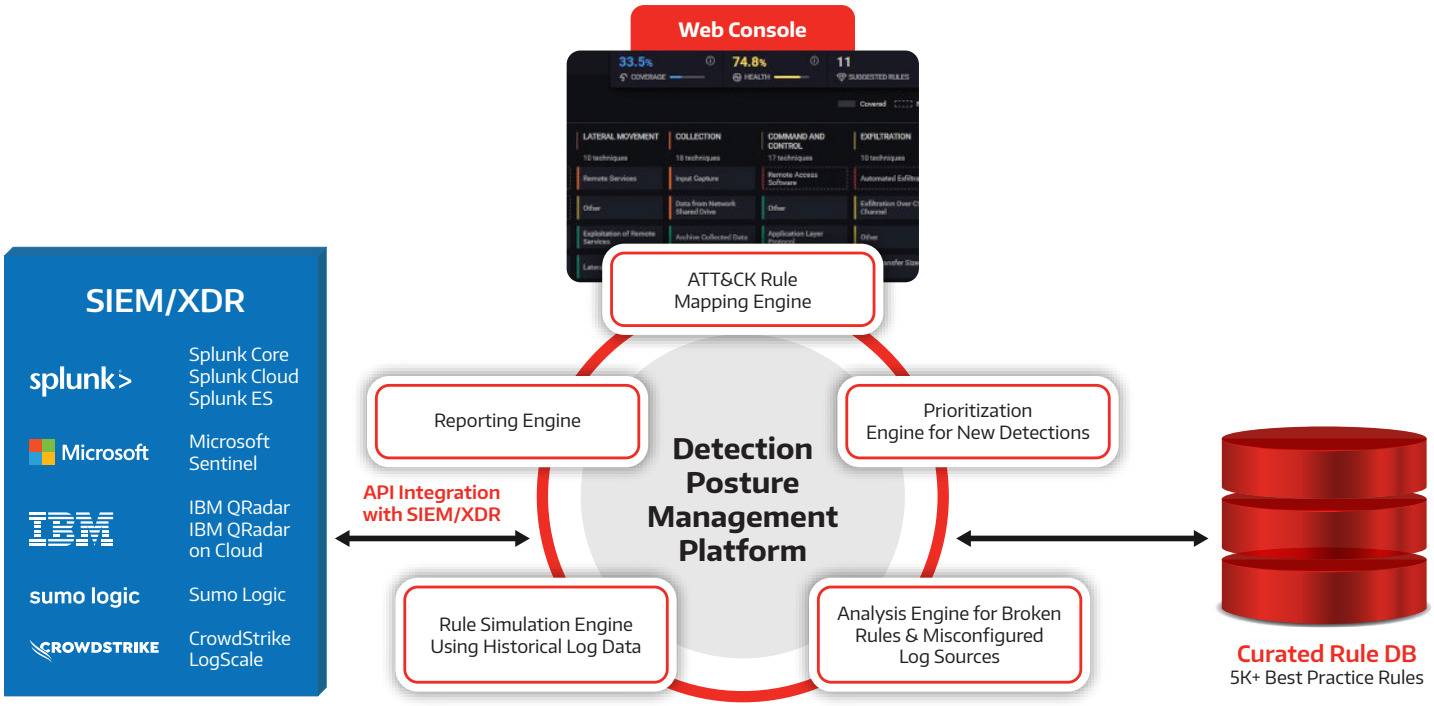
Increase the Effectiveness of Your Existing Security Stack and Your Team with the CardinalOps Platform

- Create MITRE ATT&CK coverage map and health metrics
- Continuously audit SIEM/XDR to identify and remediate broken, noisy, or missing detections
- Recommend new detections and log sources to increase ATT&CK coverage and address latest threats
- Identify SIEM cost savings from inefficient queries and unused or redundant logs

Integrations

splunk> CROWDSTRIKE vmware Carbon Black Microsoft Sentinel IBM Security Radar sumo logic

CardinalOps Architecture: API-Level Integration, Setup in Less than an Hour



Challenges CardinalOps Addresses

- How do we continuously improve our detection posture to reduce risk?
- Are we missing detections for the MITRE ATT&CK techniques and adversaries most relevant to our business?
- Do we have detection rules that are broken due to ongoing changes in our infrastructure – creating additional gaps for attackers?
- How can we leverage analytics and automation to reduce costs and rationalize our security stack while addressing hiring and retention gaps?
- How do we report our detection posture to the business and other teams using standard metrics and heatmaps?

About CardinalOps
Most security vendors pitch you on replacing your stack or adding new monitoring tools to it. CardinalOps has a more practical approach. Our detection posture management platform uses analytics and MITRE ATT&CK to maximize the effectiveness of your existing SIEM/XDR and security stack. It continuously identifies and remediates detection coverage gaps — based on your business priorities and the adversary techniques and APTs most relevant to your organization — so you can easily implement a proactive, threat-informed defense to reduce risk of breach. Importantly, it also allows you to keep the significant investments you've already made in your current security stack.

By providing continuous visibility into your current detection posture – with metrics and board-level reporting based on the standard MITRE ATT&CK framework – the platform enables you to programmatically answer the question "How exposed are we?". What's more, it helps boost your detection engineering team's productivity 10x compared to manual processes.

To learn more, visit www.cardinalops.com

CARDINALOPS
Detection Posture Management