CARDINALOPS

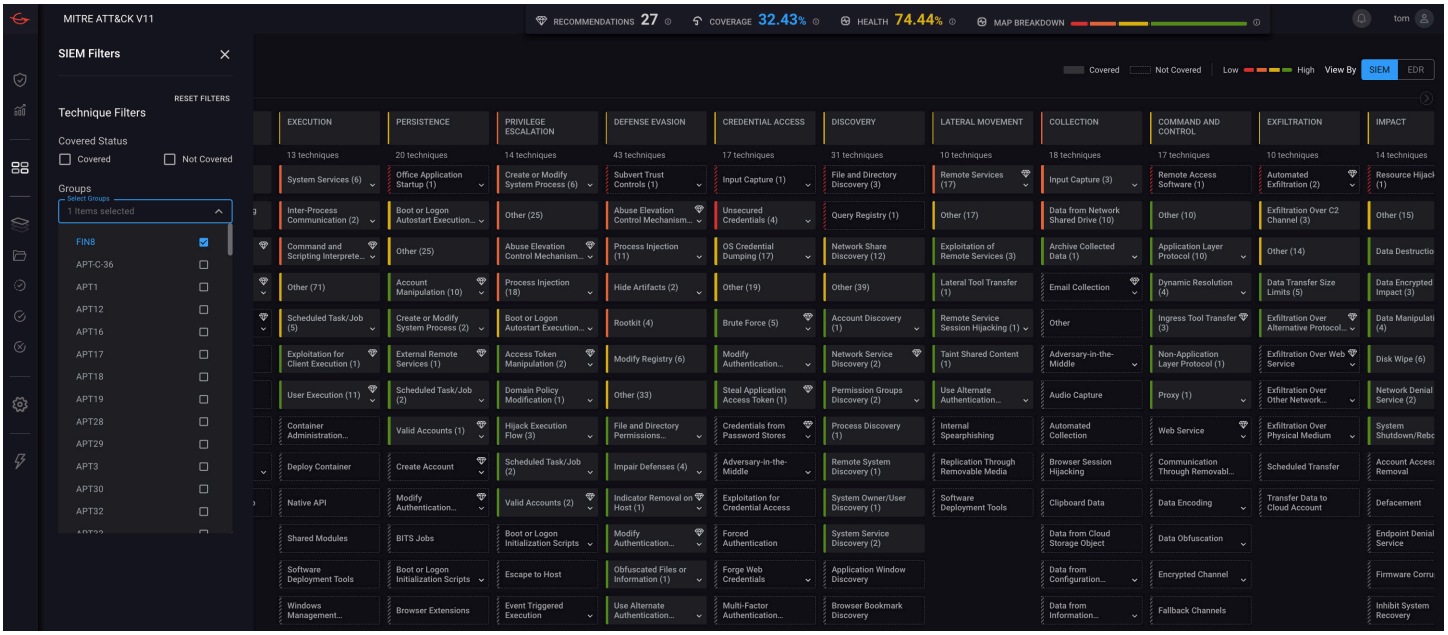
AI-Powered Detection Engineering

# Operationalize MITRE ATT&CK in Your SOC

## Eliminate Detection Coverage Gaps with AI and Automation

SOC detection tools, such as SIEM/EDR/XDRs 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/EDR/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

## Challenges CardinalOps Addresses

### For CISOs & SecOps Managers

Gain visibility & continuously improve your MITRE ATT&CK detection posture

- Are we missing detections for the MITRE ATT&CK techniques used by the specific APTs targeting our organization?
- How do we report our current posture to the board using an industry-standard framework and heatmap?
- Do we have those detections for all our crown jewel assets (Windows, Linux, containers, etc.)?
- How can we prioritize the development of new detections and onboarding of new log sources to match our business priorities?
- How can automation address our security talent shortage and reduce the time to deliver new detection use cases to production?
- Can we save on SIEM licensing costs by migrating unused or high-volume log sources to other platforms?

### For Security & Detection Engineers

Leverage AI and automation to manage your end-to-end detection engineering lifecycle

- Do we have detection rules that have become silently broken over time and will never fire due to misconfigurations or changes in our infrastructure (log format changes, RegEx typos, etc.)?
- Do we have misconfigured log sources that are no longer forwarding data to the SIEM/XDR?
- Which are our noisiest rules? What exclusions could we add to make them more effective?
- Can your platform automatically remediate broken, noisy, and missing detections with the push of a button?
- How do we quickly deliver new detections for high-profile vulnerabilities (Follina, Okta, Log4Shell, etc.)?

## Accelerate SOC Modernization

Quickly reduce risk via automation

Enable repeatable processes, metrics, and continuous improvement

Address talent and retention gaps

Accelerate strategic initiatives such as cloud transformation and SIEM migrations

**About CardinalOps**

Most security vendors pitch you on replacing your stack or adding new monitoring tools to it. CardinalOps has a more practical approach. The CardinalOps SaaS platform uses AI and automation to address some of the biggest complexity headaches that organizations have in managing their existing SOC detection solutions, without requiring you to walk away from the significant investments you've made in your current stack.

Our SOC detection posture management platform helps maximize your MITRE ATT&CK coverage for the latest threats and eliminate hidden detection gaps you may not even know you have. Setup takes less than an hour because there are no agents to deploy and it easily connects via the native APIs of your SIEM/EDR/XDR. 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

AI-Powered Detection Engineering