CARDINALOPS
Detection Posture Management

CASE STUDY

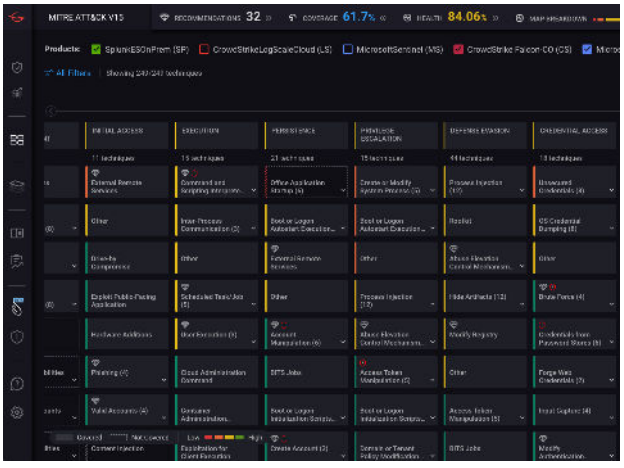
Global Bank Takes Control of their Detection Posture

Leveraging automation to assess their current coverage and continuously optimize over time

MULTINATIONAL FINANCIAL SERVICES ORGANIZATION

CHALLENGES

- Slowed by manual processes
- Difficulty keeping up with evolution of threat actor tactics and techniques
- Lack of visibility into multiple detection technologies (SIEM/EDR)
- Unable to quickly identify gaps in detection coverage



PROBLEM

Across 40+ business units and geographies with multiple deployed detection technologies, one of the world's largest financial services companies struggled to know where they had detection coverage in their SIEM – and where they didn't. In an effort to keep pace with sophisticated threat actors, their Global SOC was using manual processes to try and keep their hundreds of detections aligned to the MITRE ATT&CK® framework. Considerable daily resources were devoted to answer stakeholder concerns about how and where they were covered against specific threats.

SOLUTION

When the bank discovered they could automate much of their daily work with the CardinalOps Detection Posture Management platform, it proved to be a game-changer. Tasks that took hours, days, and weeks of time were now being handled continuously in the background – leaving SOC personnel free to focus on the highvalue portions of their work. When it stopped being about managing the data it became about the decisions they could make.

BENEFITS

Automated Mapping to MITRE ATT&CK

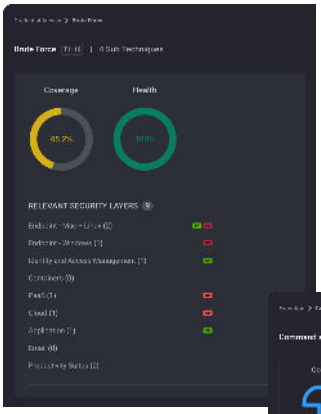
CardinalOps uses the detection telemetry type and associated rule logic to automate mapping. It also performs an integrity check to alert when a rule may not fire due to problems with the underlying log data. This data provides an organization-wide perspective with drill-down to see specific geographies or business units.

Seamless SIEM API Connection

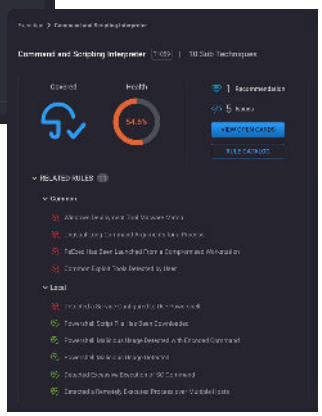
Connection to SIEM is effortless. Information about detection rules and related metadata is analyzed, processed, and updated directly in the CardinalOps portal.

CARDINALOPS

Maximize Your Detection Coverage and Fidelity



View detection coverage from SIEM and other detection tools in a single view – making it easier to find hidden gaps



See detections at a global scope and then drill down to find variations in local geographies and business units

RESULTS

Multiple Detection Technologies in Single View

The bank gained visibility into not just their Splunk SIEM, but also EDRs such as Crowdstrike Falcon® and Microsoft Defender for Endpoint®. Detection coverage from nearly any detection technology can now be seen side-by-side to help find both redundancy and hidden gaps that their SOC team would have previously missed.

Telemetry-Level Visibility

The security team can now understand how various log sources support (or don't!) their detection coverage within MITRE ATT&CK. They can now also identify under-performing (or missing) contributors and prioritize the addition of new telemetry.

CardinalOps continuously assesses and improves the detection coverage of your SIEM and other detection tools to enable a stronger, more resilient defense.

- Map your current detection coverage to MITRE ATT&CK® for continuous visibility
- Automatically detect and fix broken, misconfigured, and noisy rules
- Receive new, deployment-ready rules and recommendations for the threats relevant to you
- Automate manual tasks to free up team members to perform high-value work