SANS 2023 Detection Engineering Survey: Detection Engineering Best Practices for Implementing a Threat-Informed Defense

Sponsored by CardinalOps

Today's Speakers

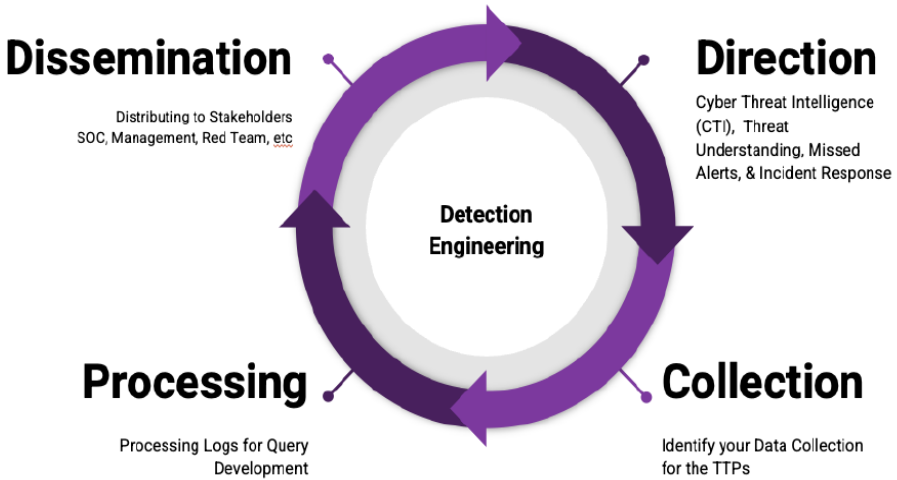
- Mark Orlando, *Certified Instructor, SANS*
- Kish Galappatti, *Senior Sales Engineer, CardinalOps*

Today's Agenda

- SANS 2023 Detection Engineering Survey introduction, concepts, and key insights
- Overview of survey results
- Conclusions
- Q&A/Discussion

What is Detection Engineering?

SANS defines Detection Engineering as a threat intelligence driven process (and discipline) for designing, testing, using, disseminating, and evaluating patterns, rules and signatures used to detect malicious activity.



What Is the SANS Detection Engineering Survey?

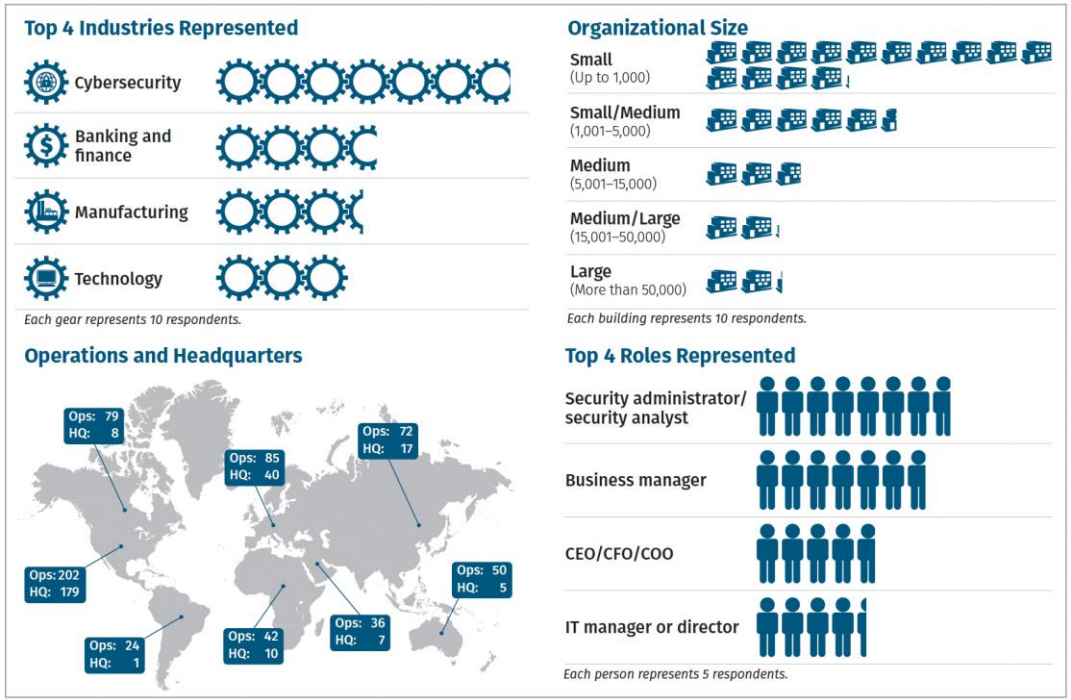
Analyst Program

- “State of practice” of Detection Engineering
- Open from July-October 2023
- Questions included multiple choice, multiple selection, ranking, free text
- Directed to professionals working directly with a SIEM or security leaders responsible for the SIEM

How Can I Use the Survey?

- Learn about detection engineering staff, process, tools, and challenges in other organizations
- Consider different approaches or validate your own
- Make the case for more formalized detection engineering capabilities and measurement

Survey Respondents

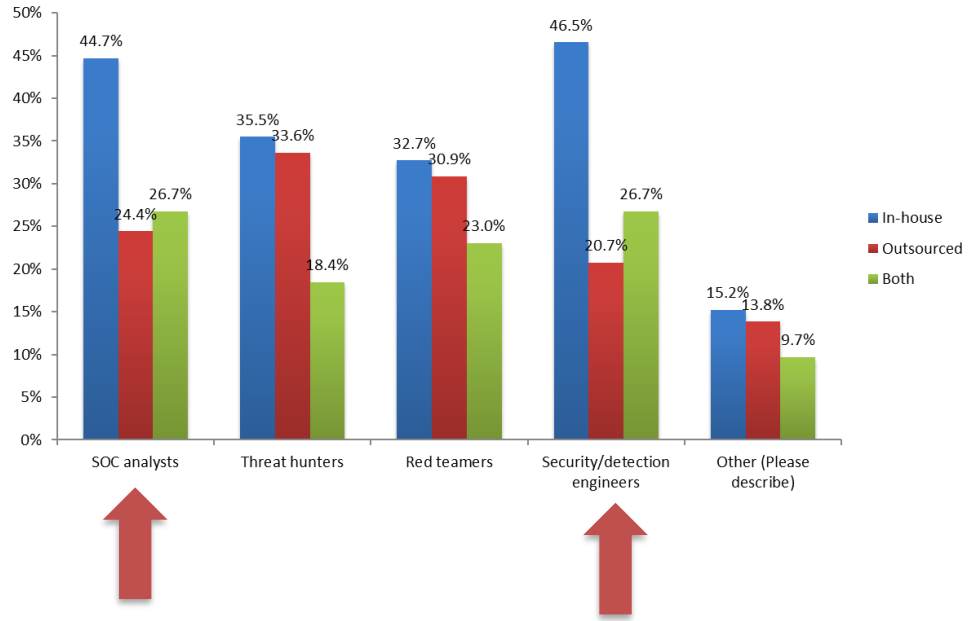


Key Insights

- SIEM continues to play foundational role, market shift indicates focus on threat detection versus compliance
- Hybrid staffing approach using internal teams and external partners is common
- Variety of testing and validation methods used, with heavy reliance on third-party assessments

Detection Engineering Roles

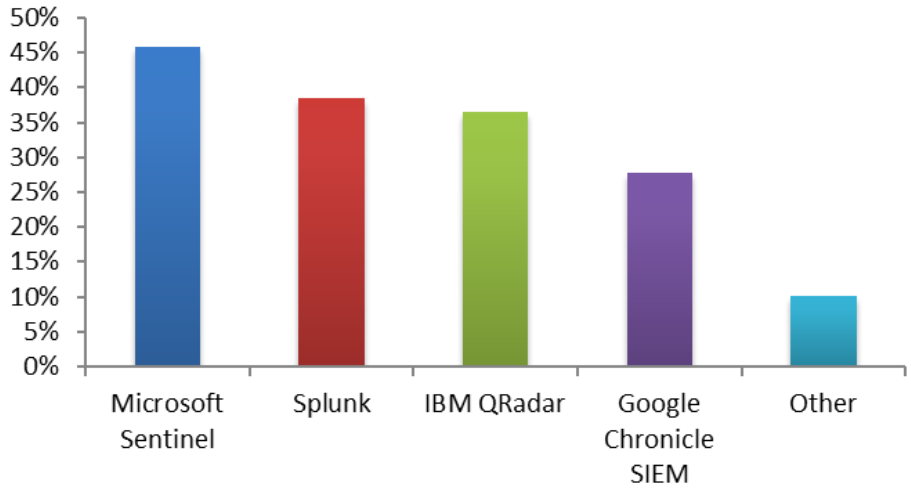
- Heaviest reliance on internal SOC Analysts and Engineers
- Outsourcing and/or hybrid approach is common across roles
- Other key staff includes Threat Hunters, Red Teamers



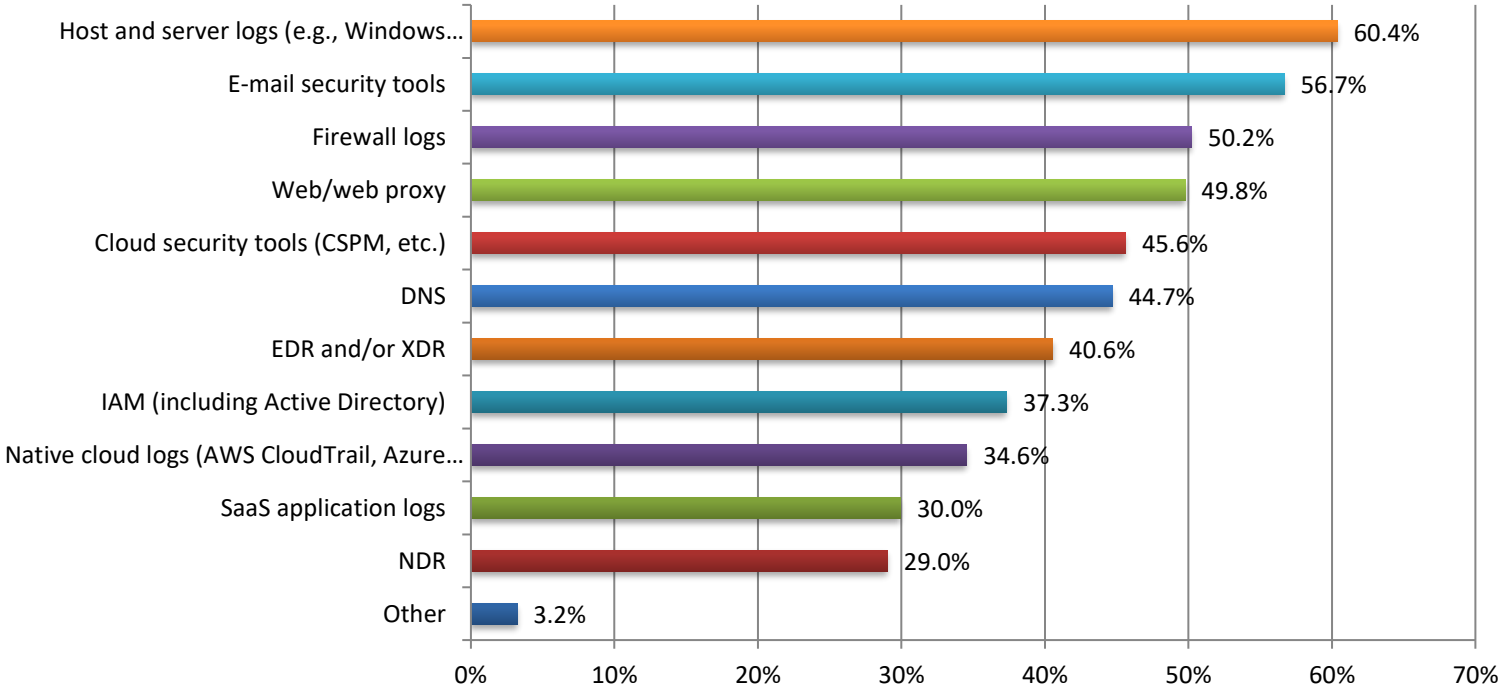
Toolsets Used (SIEM)

Analyst Program

- 45% Microsoft Sentinel
- 38.4% Splunk
- 36.6% IBM QRadar
- 27.8% Google Chronicle
- 10.2% Other

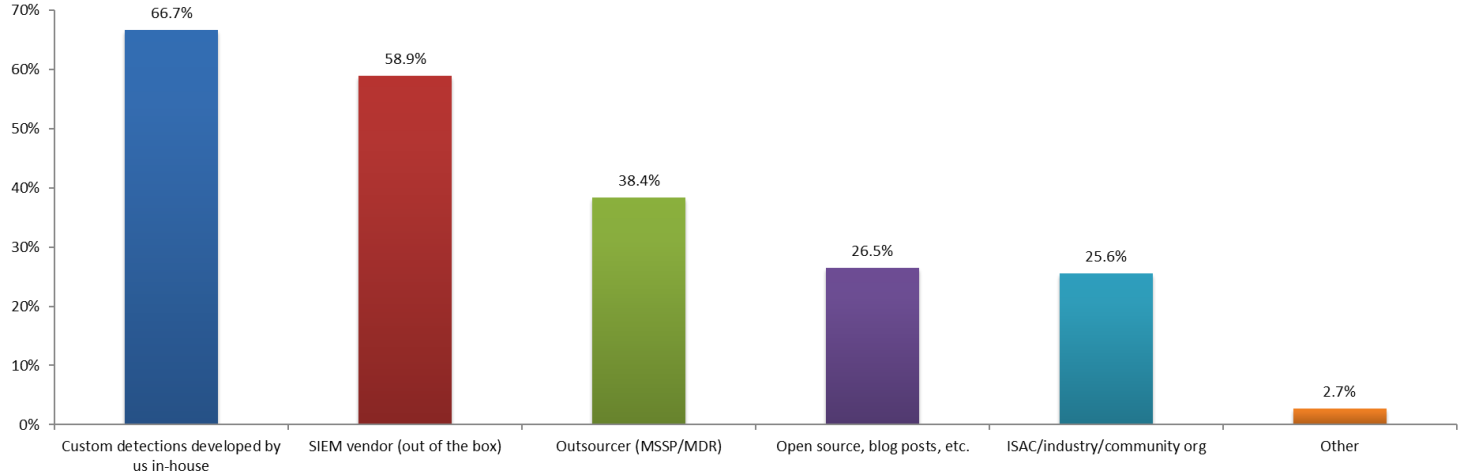


Detection Data Sources



Detection Use Cases

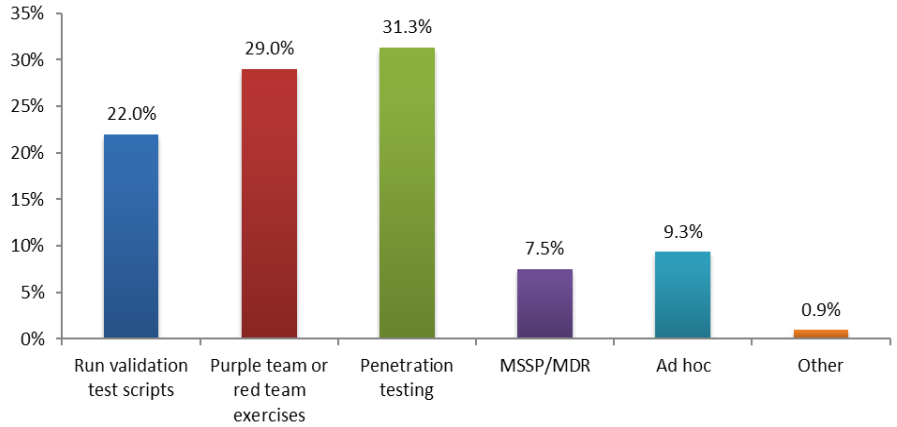
- **66.7%** develop detections in-house based on custom use cases
- **58.9%** rely on use cases provided by SIEM vendor
- **38.4%** rely on third party providers (MSSP or MDR)



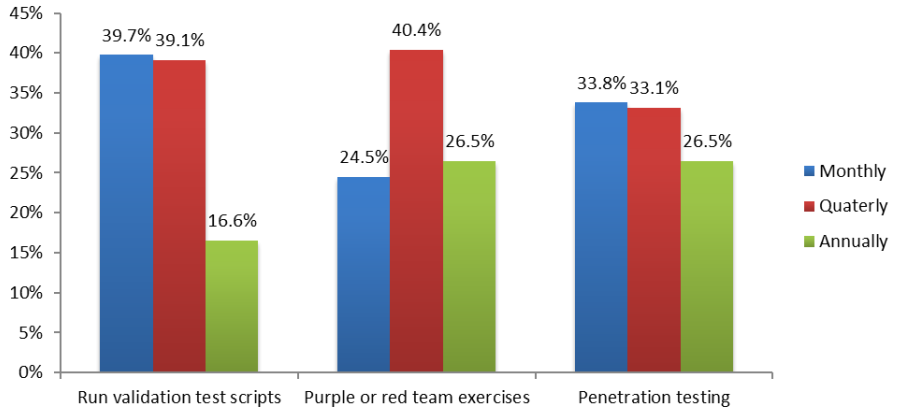
Testing and Validation

Analyst Program

Rule Testing and Validation

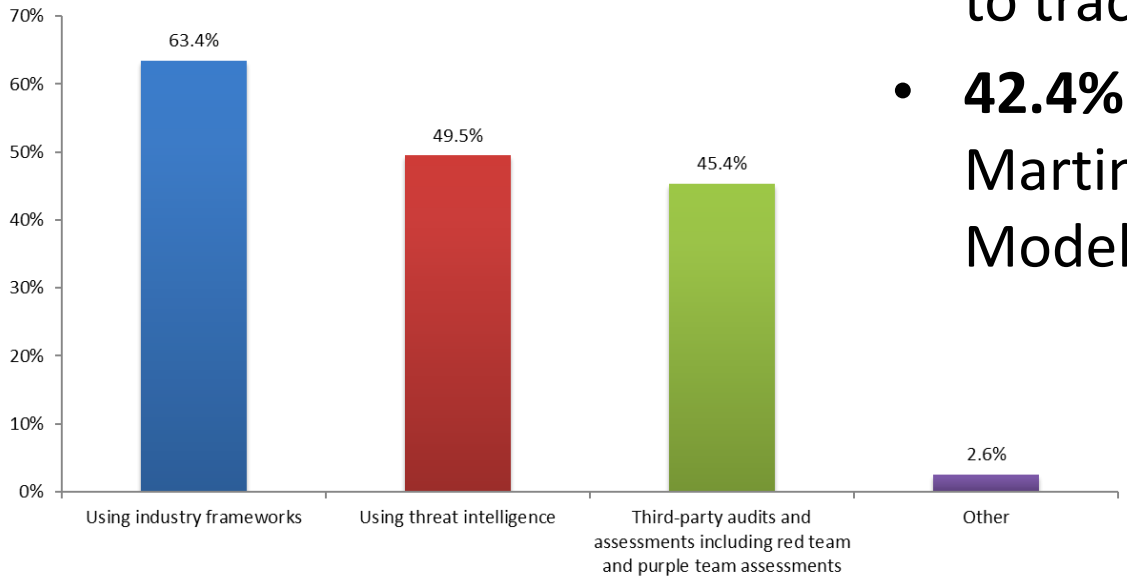


Testing and Validation Intervals



Third-party validation on a monthly or quarterly basis
is the most common testing method among respondents

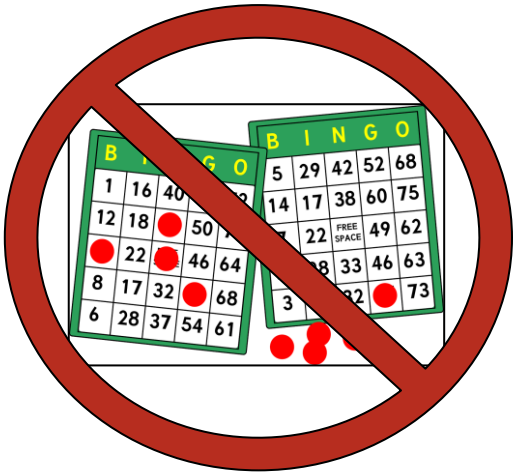
Alignment to Industry Frameworks (1)



- **85.6%** use MITRE ATT&CK to track coverage
- **42.4%** use Lockheed Martin Cyber Kill Chain Model

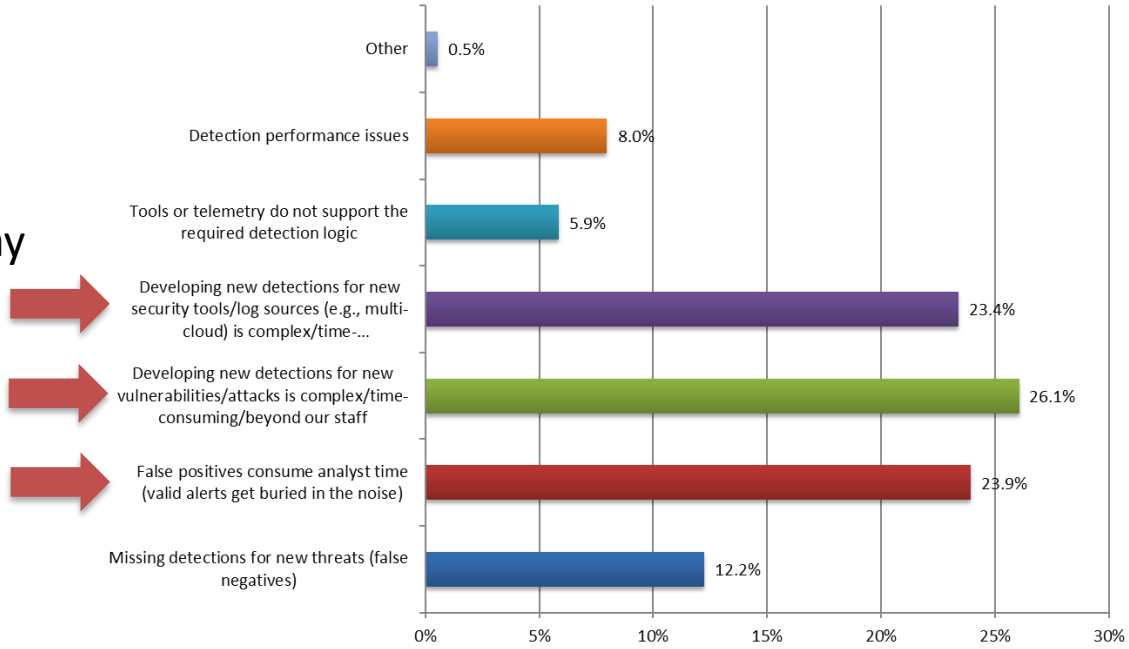
Alignment to Industry Frameworks (2)

- **97.5%** said alignment process is manual based on detection review or open-source information
- Others cited automated or semi-automated systems



Causes of Detection Gaps

- Complexity and cost to develop detections for new tools or new attacks
- False positives consume analyst time, take focus away from valid alerts
- Challenges result in false negatives



Conclusions

1. Consider how your intelligence, hunting, environment data inform new detections
2. Framework alignment improves maturity, but coverage must be *prioritized*
3. Tooling, testing, and validation should cover entire process, from data collection and processing to analytic development to continuous validation
4. Automation reduces cost, time and complexity

SANS

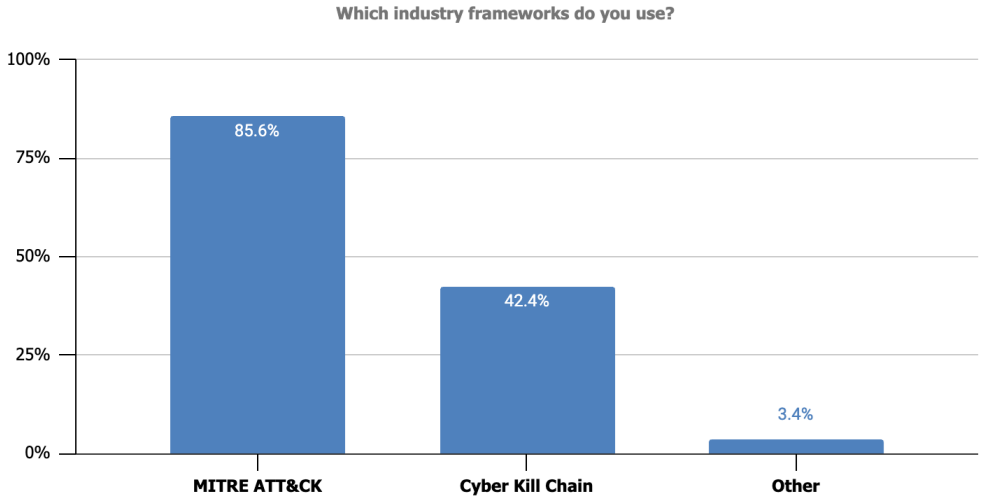
Detection Engineering Best Practices for Implementing a Threat-Informed Defense

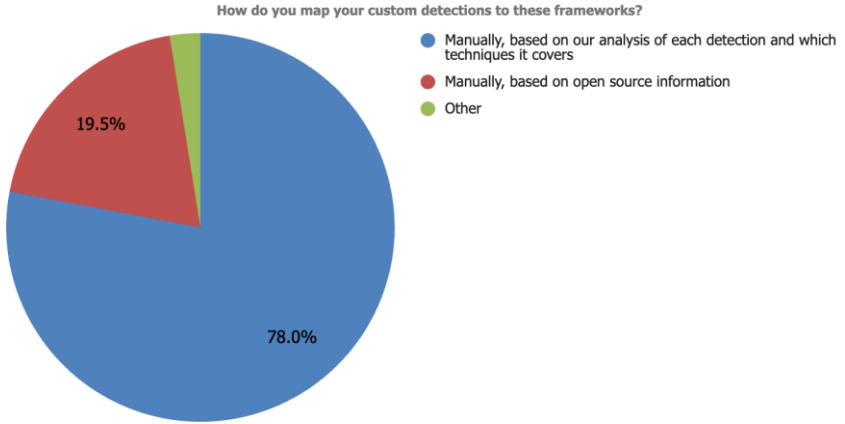
CardinalOps

Kish Galappatti

MITRE ATT&CK Used to Measure Detection Coverage… Manually

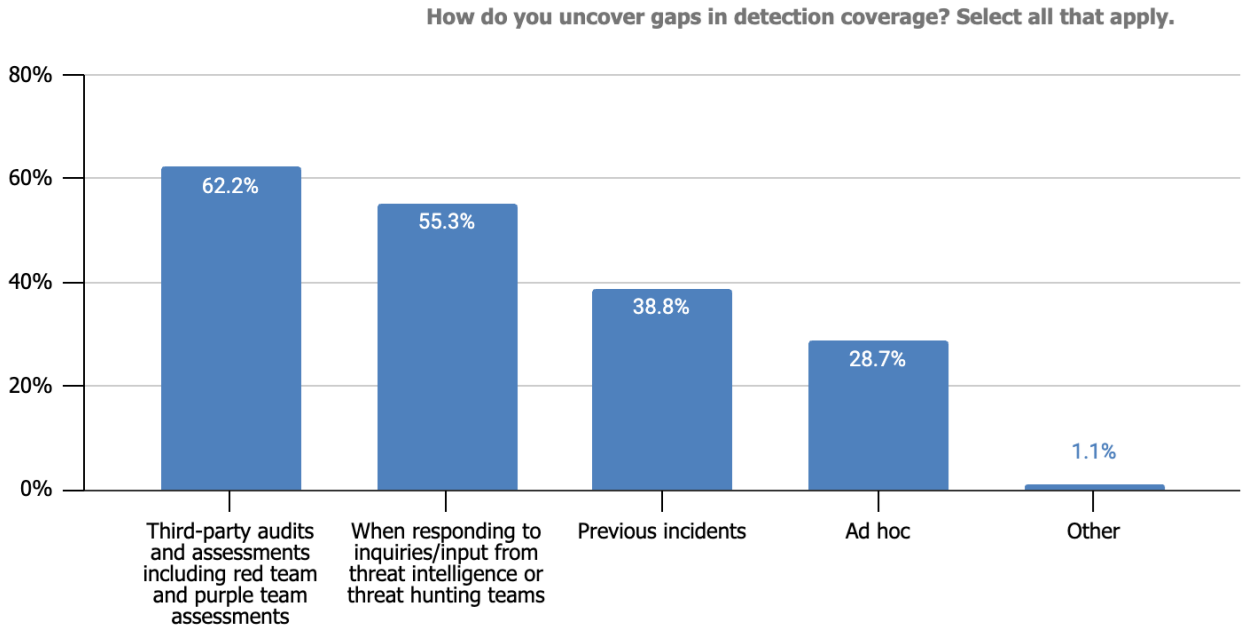
- 63% use industry frameworks to assess/measure their current level of detection coverage
- 86% use MITRE ATT&CK for this
- 78% manually map detections





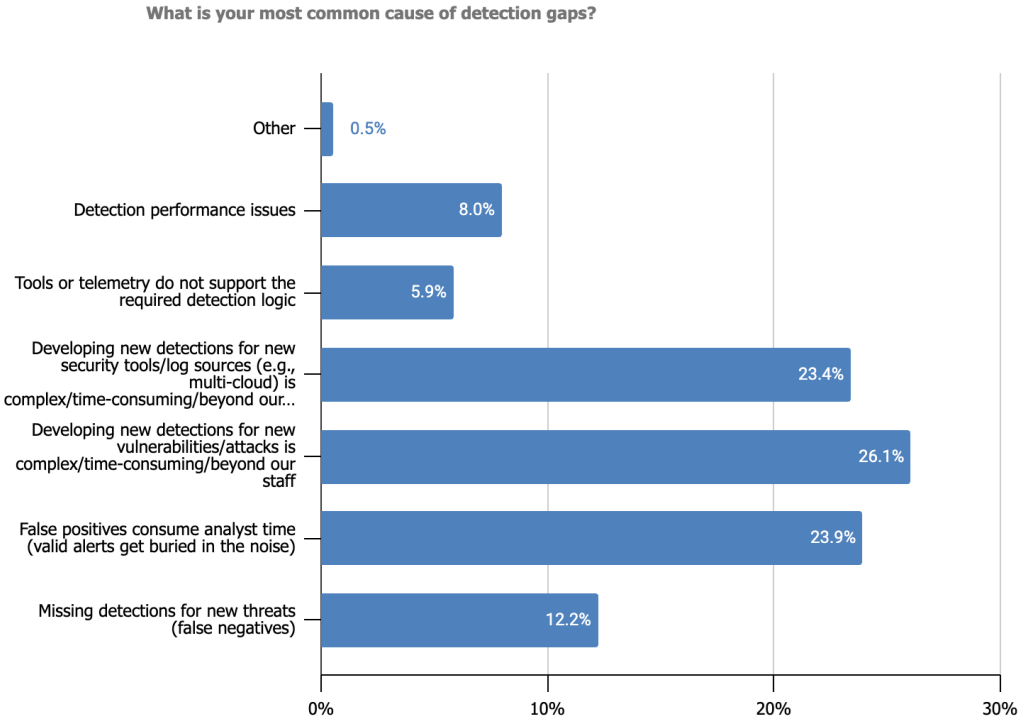
Identifying Gaps in Detection Coverage

- Ad hoc vs. continuous
- Systematic vs. reactive



Top Causes for Gaps in Detection Coverage

- Gaps in detection coverage being caused by both external (the need for new detections for new threats/log sources) and internal (false negatives, detection performance, etc.) forces

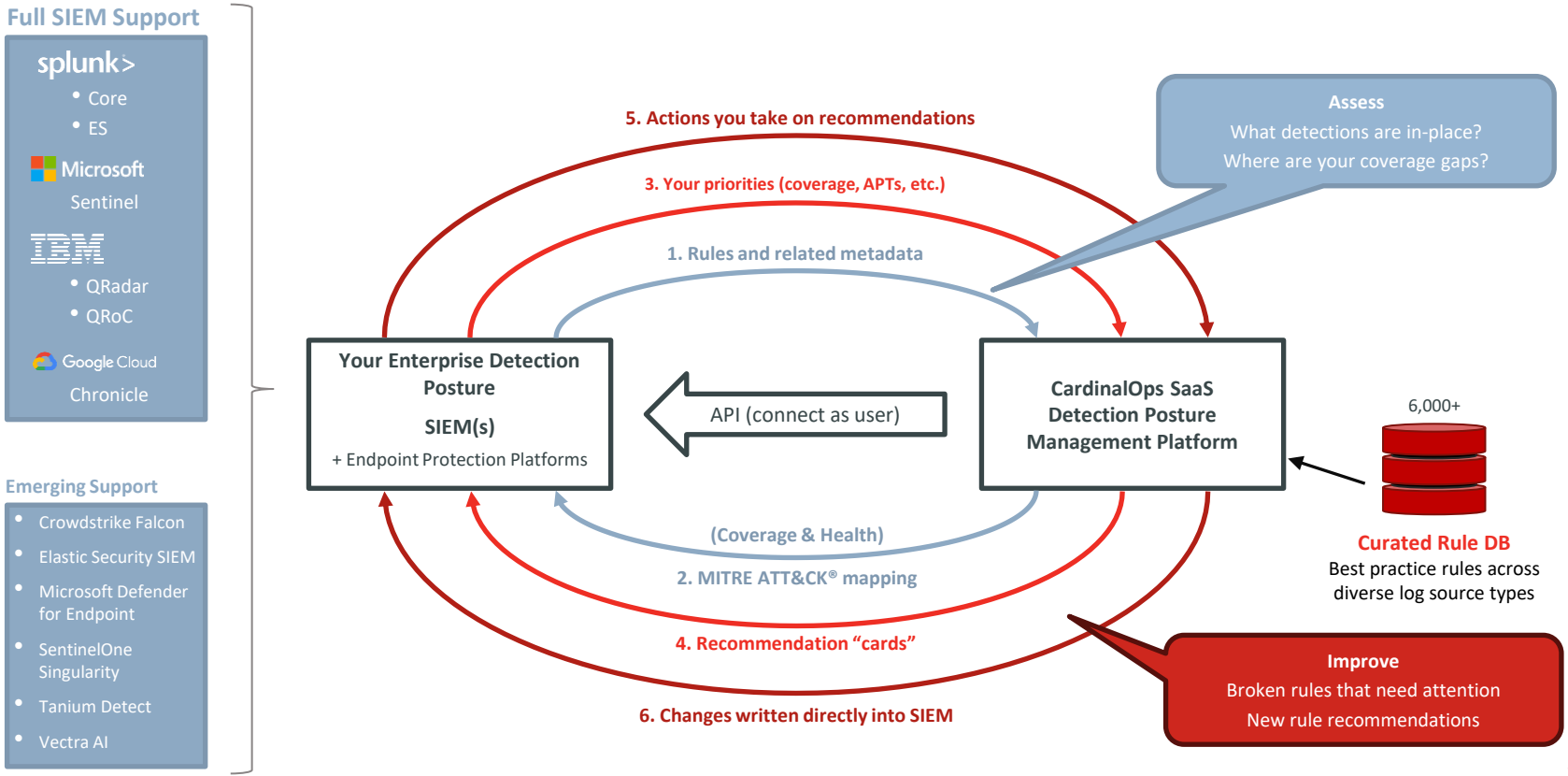


Detection Posture Management

CardinalOps continuously assesses and improves the detection coverage of your existing 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

Working with CardinalOps



Better detection posture management… by the numbers

Additional resources - www.cardinalops.com/whitepapers/

Category	Resource	Description
Technical Brief	Top 10 Ways that SIEM Rules (Silently) Break	Highlights how SIEM detections can go “offline” and create detection gaps.
	Top 3 Causes of Noisy SIEM Rules (and 5 Ways to Address Them)	Helpful tips for practitioners on dealing with excessive false positives.
	Addressing the Complexity Challenge of Multiple SIEMs	Provides considerations when an enterprise adds additional SIEMS.
Industry analyst report	Operationalizing MITRE ATT&CK with Detection Posture Management	Practical strategies for adopting the MITRE ATT&CK framework.
Original research	Third Annual Report on State of SIEM Detection Risk	Benchmarks for SIEM utilization and current trends in implementation.
Webinar	SOC, Meet Cloud. Cloud, Meet SOC. What Changes?	SANS webinar with Dr. Anton Chuvakin, Google Office of the CISO. He addresses the impact Cloud infrastructure has on the SOC.

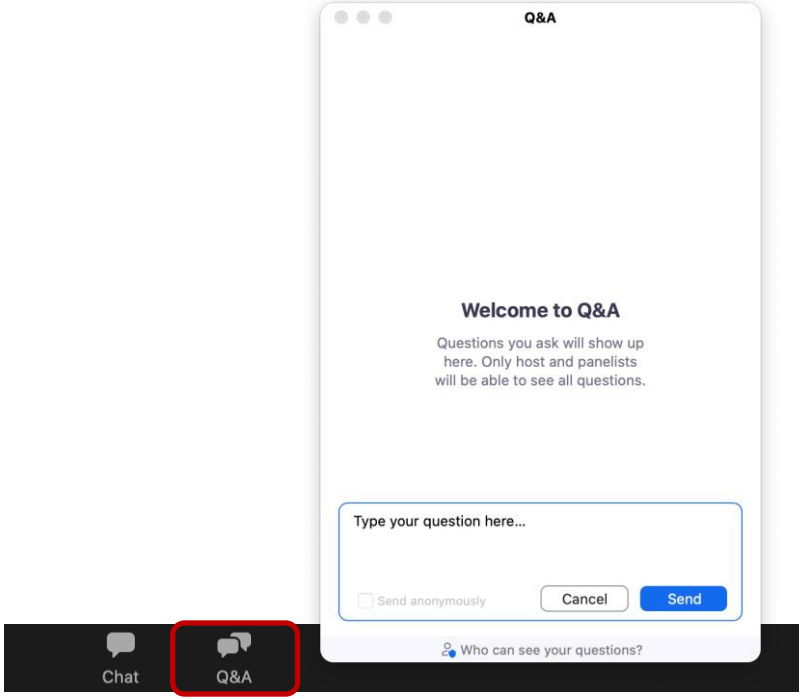
Thank you!

Kish.Galappatti@CardinalOps.com

Q&A

Please use **Zoom's** Q&A window to submit questions to our presenters.

Type your question, tell us if it's for a specific presenter, and then click Send.



Acknowledgments

Thanks to our sponsor:

To our special guest: Kish Galappatti

And to our attendees, thank you for joining us today!