SANS
SPONSORSHIP PROGRAM

SANS 2022 THREAT HUNTING SURVEY

Hunting for a Standard Methodology for Threat Hunting Teams

Authors: **Mathias Fuchs and Josh Lemon**

Publication Date: **July 20, 2022**

Analyst Program

MEET THE AUTHORS

Mathias Fuchs
SANS Certified Instructor

Mathias began his career teaching Linux administration and general IT security and quickly moved into penetration testing and red teaming. He moved over to digital forensics and incident response, a field where the attacker unintentionally sets the pace and partly controls what an investigator needs to do - rather than that being dictated by the customer or the investigator.

Josh Lemon
SANS Certified Instructor

Josh leads Ankura's APAC Digital Forensics and Incident Response practice where he assists government and commercial clients with sophisticated compromises, maturing their cyber defence and response programs, and threat hunting for malicious adversaries. In addition to his role at Ankura, Josh teaches two SANS courses: FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response.

OVERVIEW

Threat hunting has become a common process within organizations, for consultancies offering tailored services and for vendors when it comes to providing tooling. But how far have we come as a cybersecurity industry? Have we managed to land on a standard methodology, a common framework, or standardized skills for threat hunting teams?

This research paper looks back at how organizations have progressed over time and where our industry currently lies in finding a methodology to conduct, measure, and improve threat hunting. We also look back at the last two years to see if global economic impacts have caused any industry changes that give us cause to rethink our approach to threat hunting.

Key topics will include:

- Operationalizing threat hunting
- Innovative threat hunting tactics and techniques
- New tools that can help threat hunting for both endpoints and networks

SPONSOR

- Sponsors can associate with this industry-standard survey that the SANS community look to for guidance on tactical implementation and usage of threat hunting.
- Cobrand the survey results whitepaper and webcast.
- Collaborate with SANS' best cybersecurity experts who are at the forefront of the ever-changing war on cybersecurity.

View next page for sponsorship packages.

SANS
SPONSORSHIP PROGRAM

SANS 2022 THREAT HUNTING SURVEY

SPONSORSHIP PACKAGES	GOLD	PLATINUM
Survey and Paper		
Receive draft of the survey results for review and a final, branded survey results whitepaper	✓	✓
Survey Analysis & Discussion (100—150 minute virtual presentation) **July 20, 2022**		
Branding on the survey presentation registration page	✓	✓
15—20 minute speaking slot		✓
Included in 20—30 minute panel discussion with the survey author(s) and platinum sponsors		✓
Leads	300 leads no cap	500 leads no cap

LEAD SUBMISSION AND SURVEY PROMOTIONS

Lead Submission

The initial installment of leads will be provided within two business days of the live presentation. Additional leads will be provided on a regular basis for the first three months following the presentation. After three months, leads will be provided as requested.

Promotions

Survey: The survey will be promoted for five to six weeks to our SANS community.

Survey Presentation: The presentation will be promoted to the SANS community one week after the survey closes.

Whitepaper: The whitepaper will be available in the SANS Reading Room on the same day as the presentation and will be promoted to the SANS community.

ADDITIONAL SPONSORSHIP

Associated Paper or Product Review

Publish a custom paper based on a segment of the survey that is of interest to you or a product review that calls on the survey as an entry point to the review.

This associated paper also includes a webcast. Includes 200-lead guarantee with no cap and continued lead generation as a SANS archive webcast.

Contact your SANS representative today to learn more about sponsoring this SANS survey.