2021

Cybersecurity
INSIDERS

THREAT HUNTING REPORT

LOOKINGGLASS

INTRODUCTION

Threat hunting continues to evolve as an innovative cybersecurity tactic that focuses on proactively detecting and isolating Advanced Persistent Threats (APTs) that might otherwise go undetected by traditional, reactive security technologies.

While many SOCs struggle to cope with the rising security threat workload, more organizations are adopting threat hunting as part of their security operations. They discover that proactive threat hunting can reduce the risk and impact of threats while improving defenses against new attacks.

The 2021 Threat Hunting Report explores the challenges, technology preferences, and benefits of threat hunting to gain deeper insights into the maturity and evolution of the security practice.

Key findings include:

- More than half of respondents (51%) identified reducing exposure to internal threats as their top threat hunting goal. This is followed by reducing the number of breaches and infections (45%) and reducing the attack surface (43%).
- The most common attacks that organizations proactively discover include malware (76%), phishing (71%), network intrusions (46%), and ransomware (41%).
- The top data sources that organizations collect and analyze for threat hunting purposes include endpoint activities (72%), system logs (71%), and firewall traffic (69%).
- 68% of organizations at least occasionally develop insights into adversary infrastructures as part of their threat hunting activities. However, only 21% of organizations are fully focused on gaining these insights.
- Organizations need to collect data from multiple sources to add context to their threat hunting activities. The most common data sources include external threat intelligence feeds (56%), user behavior data (56%), and file activity data.

We would like to thank LookingGlass for supporting this important research.

We hope you enjoy the report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

All Rights Reserved. ©2021 Cybersecurity Insiders

THREAT HUNTING GOALS

More than half of respondents (51%) identified reducing exposure to internal threats as their top threat hunting goal. This is followed by reducing the number of breaches and infections (45%) and reducing the attack surface (43%).

What are the primary goals of your organization's threat hunting program?

51%

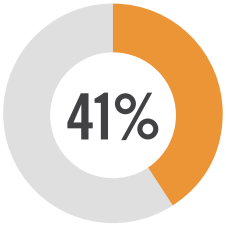
Reduce exposure to internal threats

45%

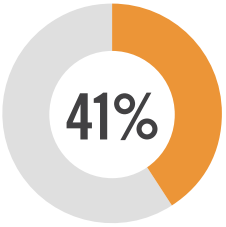
Reduce number of breaches and infections

43%

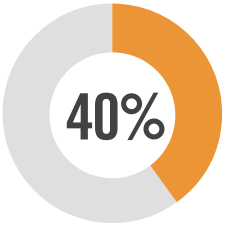
Reduce attack surface



Reduce time to containment (prevent spread)



Reduce exposure to external threats



Improve speed and accuracy of threat response

Reduce dwell time from infection to detection 39% | Optimize resources spent on threat response 31% | Other 7%

All Rights Reserved. ©2021 Cybersecurity Insiders

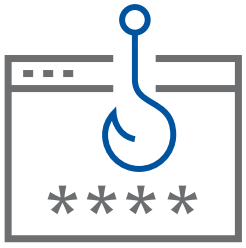
MOST COMMON ATTACKS

The most common attacks that organizations proactively discover include malware (76%), phishing (71%), network intrusions (46%), and ransomware (41%).

What are the most common attacks proactively discovered through threat hunting?

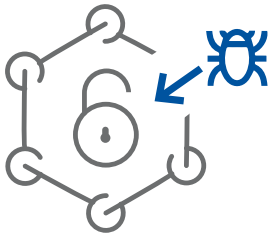
76%

Malware



71%

Phishing



46%

Network intrusion

41%

Ransomware

Supply chain compromise 2% | Other 2%

All Rights Reserved. ©2021 Cybersecurity Insiders

DATA COLLECTION SOURCES

The top data sources that organizations collect and analyze for threat hunting purposes include endpoint activities (72%), system logs (71%), and firewall traffic (69%).

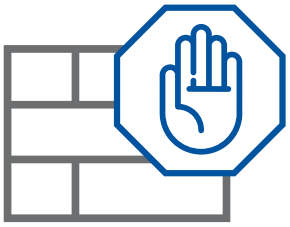
What kind(s) of data does your security organization collect and analyze?

72%

Endpoint activity

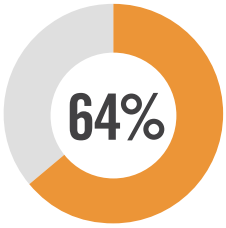
71%

System logs

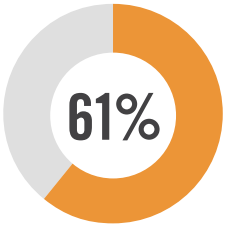


69%

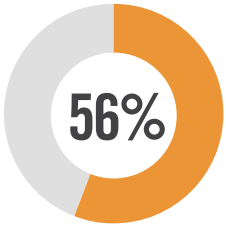
Firewall/IPS denied traffic



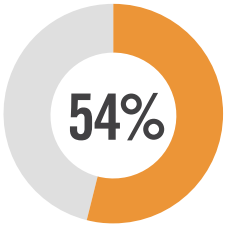
Firewall/IPS allowed traffic



Web and email filter traffic



Network traffic



Threat intelligence sources

Active directory 53% | DNS traffic 52% | Server traffic 47% | Web proxy logs 45% | User behavior 39% | File monitoring data 36% | Packet sniff/tcpdump 33% | Don't know/other 12%

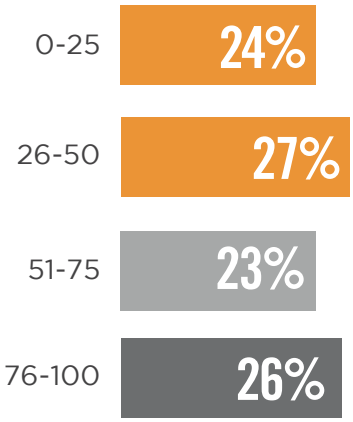
All Rights Reserved. ©2021 Cybersecurity Insiders

DETECTION METHODS

More than half of organizations (59%) spend less than 50% of their time proactively innovating to prevent a security threat, while 51% spend the same time in reactive response.

In a typical week, what percentage of your threat management time is spent with alert triage or reactive response to security threats versus engaging in proactive and innovative detection methods?

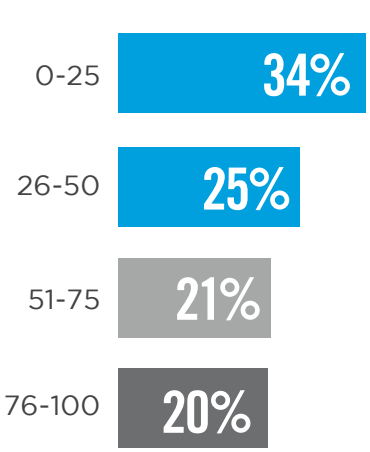
REACTIVE



51%

Are spending less than 50% of their time in **reactive response** of security threats

PROACTIVE



59%

Are spending less than 50% of their time in **proactive prevention** of security threats

All Rights Reserved. ©2021 Cybersecurity Insiders

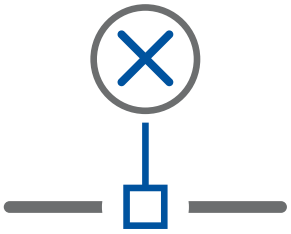
THREAT INDICATORS

Developing effective defense strategies requires understanding the indicators that compromise the organization's security posture. Research reveals that hunt teams most frequently investigate behavioral anomalies (71%), followed by denied/flagged connections (60%), suspicious IP addresses (56%), and suspicious domain names (51%).

What kinds of indicators are most frequently investigated by your hunt team?

71%

Behavioral anomalies
(unauthorized access attempts, etc.)

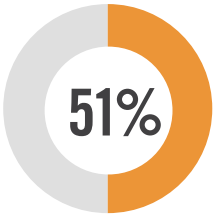


60%

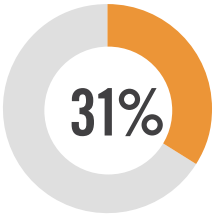
Denied/flagged connections

56%

Suspicious IP addresses



Domain names



File names

Not sure/other 13%

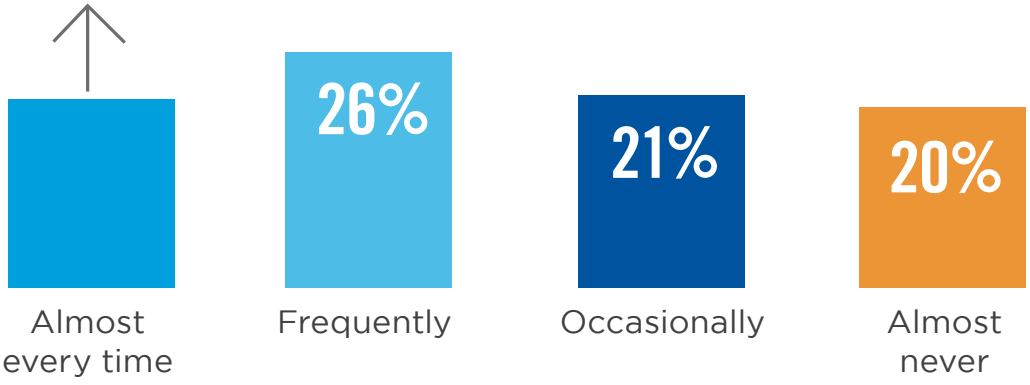
All Rights Reserved. ©2021 Cybersecurity Insiders

INSIGHTS INTO ADVERSARIES

68% of organizations, at least occasionally develop insights into adversary infrastructures as part of their threat hunting activities. However, only 21% of organizations are fully focused on gaining these insights.

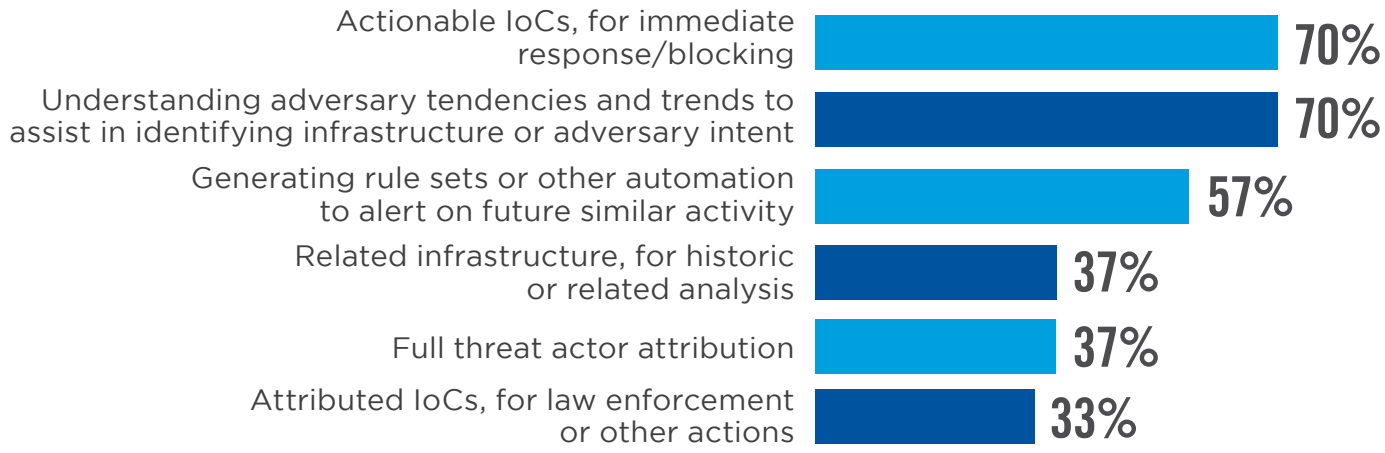
How often do you develop insights into adversary infrastructure (domains and IP addresses) as part of your hunt activities?

21% Of organizations fully focus on developing insights into adversary infrastructures as part of their threat hunting activities



Don't know 12%

What are the most useful insights into adversary infrastructure that threat hunting produces?



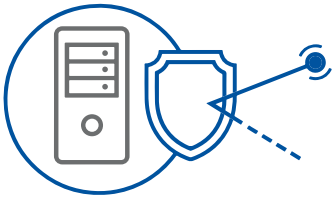
Other 3%

All Rights Reserved. ©2021 Cybersecurity Insiders

THREAT HUNTING TECHNOLOGIES

Many technologies are available to hunt threats. Endpoint detection and response is the clear leader with 63% of organizations integrating these tools into their threat hunting efforts, followed by SIEM (56%) and anti-phishing or other messaging security software (54%).

Which technologies do you use as part of your organization's threat hunting approach?

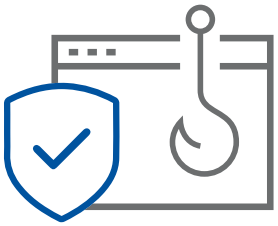


63%

Endpoint Detection & Response (EDR)

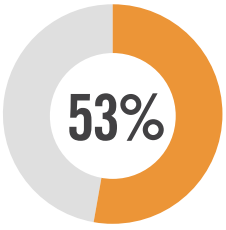
56%

SIEM

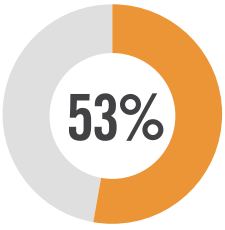


54%

Anti-phishing or other messaging security software

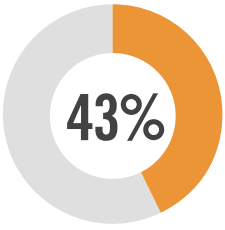


NGFW, IPS, AV, web application firewall, etc.



Network IDS/ Network Detection and Response (NDR)

Vulnerability management



Threat intelligence platform

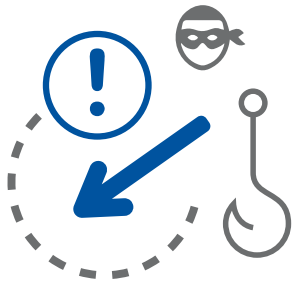
Enrichment and investigation tools 29% | Security Orchestration, Automation, and Response (SOAR) 19% | Not sure/ other 12%

All Rights Reserved. ©2021 Cybersecurity Insiders

THREAT HUNTING DATA

Organizations need to collect data from multiple sources to add context to their threat hunting activities. External threats intel feeds (56%), user behavior data (56%), and file activity data (46%) are the most common means for collecting this data.

Which contextual information do you use as part of your threat hunting data?

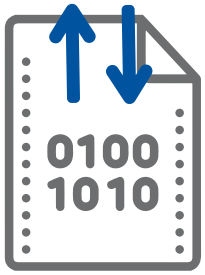


56%

External threat intel feeds

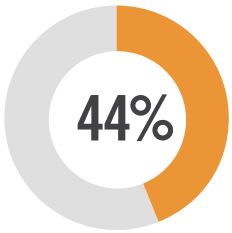
56%

User behavior data

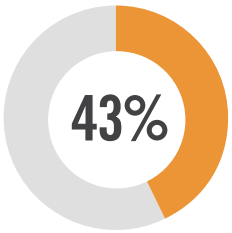


46%

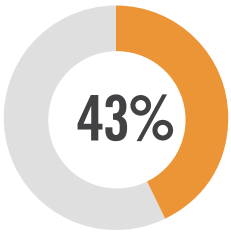
File activity data



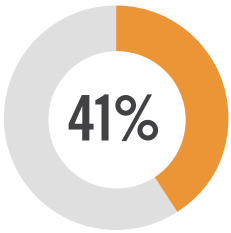
System patch status



User permission data



Network protocol data



Source blacklist

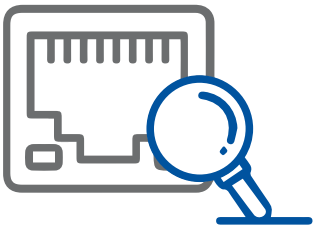
Asset inventory data 41% | Data classification 38% | File permission data 38% | Other 3%

All Rights Reserved. ©2021 Cybersecurity Insiders

POPULAR RECONNAISSANCE ACTIVITIES

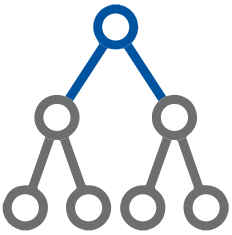
Port scanning is the most used activity for reconnaissance, with 73% of organizations including this technique in their threat hunting efforts. This is followed by active directory enumeration (54%) and host enumeration (44%).

Which of the following reconnaissance activities do you look for as part of your threat hunting activities?



73%

Port scanning

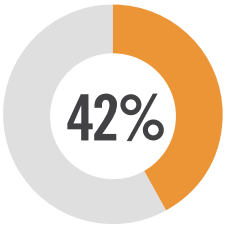


54%

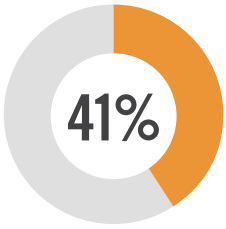
Active directory enumeration

44%

Host enumeration

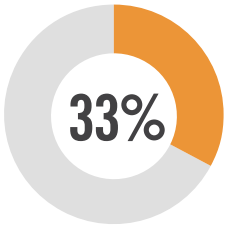


Remote system discovery



LDAP queries

Password policy discovery



Service enumeration

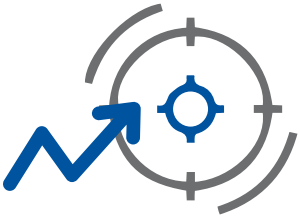
Open share enumeration 31% | None 10% | Other 4%

All Rights Reserved. ©2021 Cybersecurity Insiders

BENEFITS OF THREAT HUNTING

Threat hunting platforms provide security analysts with powerful tools to enable earlier detection, reduce dwell time, and improve defenses against future attacks. The top benefits organizations derive from threat hunting platforms include improved detection of advanced threats (68%) and tying at 55% are reduced investigation time, and saved time manually correlating events.

What are the main benefits of using a threat hunting platform for security analysts?



68%

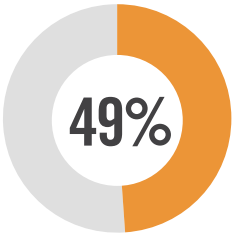
Improving detection of advanced threats

55%

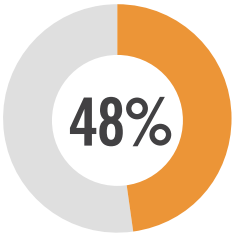
Reducing investigation time

55%

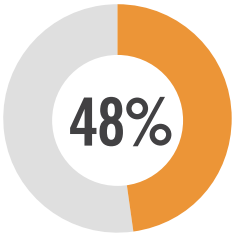
Saving time manually correlating events



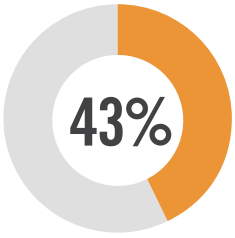
Discovering threats that could not be discovered otherwise



Reducing time wasted on chasing false leads



Reducing attack surface



Creating new ways of finding threats

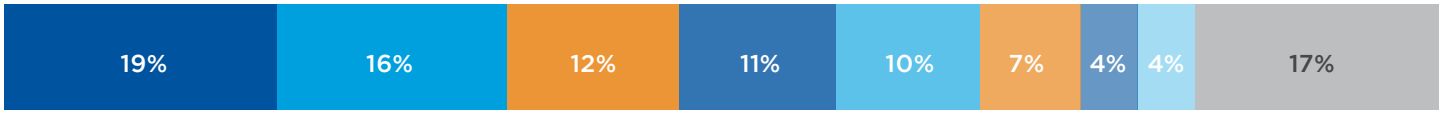
Connecting disparate sources of information 39% | Reducing extra and unnecessary noise in the system 38% | Saving time scripting and running queries 35% | Other 3%

All Rights Reserved. ©2021 Cybersecurity Insiders

METHODOLOGY & DEMOGRAPHICS

This Threat Hunting Report is based on the results of a comprehensive online survey of cybersecurity professionals, to gain deep insight into the latest trends, key challenges, and solutions for threat hunting management. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

PRIMARY ROLE



IT Manager, Director or CIO | CSO, CISO or VP of Security | Security Analyst | Security Manager or Director | Systems Administrator | Security Administrator | Threat Analyst | Auditor | Other

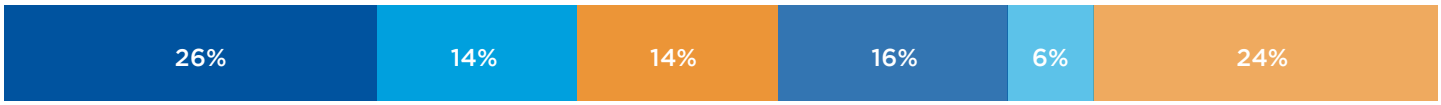
CAREER LEVEL

Director | Specialist | CTO,CIO,CISO,CMO,CFO,COO | Manager/Supervisor | Consultant | Administrator | Owner | CEO/President | Other

DEPARTMENT

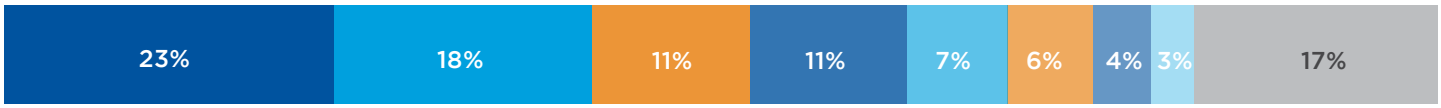
IT Security | IT Operations | Security Operations Center (SOC) | Engineering | Sales/Marketing | Product Management | Other

COMPANY SIZE



Less than 100 | 100-499 | 500-999 | 1,000-4,999 | 5,000-9,999 | Over 10,000

INDUSTRY



Technology | Financial Services, Banking or Insurance | Government | Healthcare | Manufacturing | Telecommunications or ISP | Retail or Ecommerce | Energy or Utilities | Other

All Rights Reserved. ©2021 Cybersecurity Insiders

LOOKINGGLASS

LookingGlass develops cybersecurity solutions that empower organizations to meet their missions with tailored, actionable threat intelligence and threat mitigation capabilities that move at machine speed. For more than a decade, the most advanced organizations in the world have trusted LookingGlass to help them protect financial systems, ensure telecommunications are cyber-resilient and safeguard economic and national security interests.

Rooted in operationalizing threat intelligence, LookingGlass solutions help reduce the time to detect and respond to incidents, enable cyber investigations, optimize threat hunt operations, and improve analyst productivity and efficiency. By linking the risks and vulnerabilities from an organization's external attack surface to customized threat actor models, LookingGlass provides a more complete view of cyber risk and enables systematic definition and deployment of mitigations to defend against the threats that matter.

Learn more at lookingglasscyber.com