

2018

Cybersecurity
INSIDERS

THREAT INTELLIGENCE REPORT

ANOMALI™

INTRODUCTION

Threat intelligence has become a significant weapon in the fight against cybersecurity threats, and a large majority of organizations have made it a key part of their security programs.

Among the key findings of the report are that organizations are leveraging threat intelligence data for a number of use cases, and many rate themselves fairly competent in their use of threat intelligence to identify and remediate cyber threats.

The most common benefits of threat intelligence platforms include better threat analysis, faster detection and response, more efficient security operations, and better visibility into threats.

Organizations are going to need these tools as they face cyber threats such as phishing, zero-day attacks, insider attacks, advanced persistent threats, and malware. Other challenges include threat detection, gaining full visibility into all assets and vulnerabilities, and lack of advanced security staff.

We would like to thank [Anomali](#) for supporting this unique research.

We hope you will enjoy the report.

Thank you,

Holger Schulze



Holger Schulze

CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

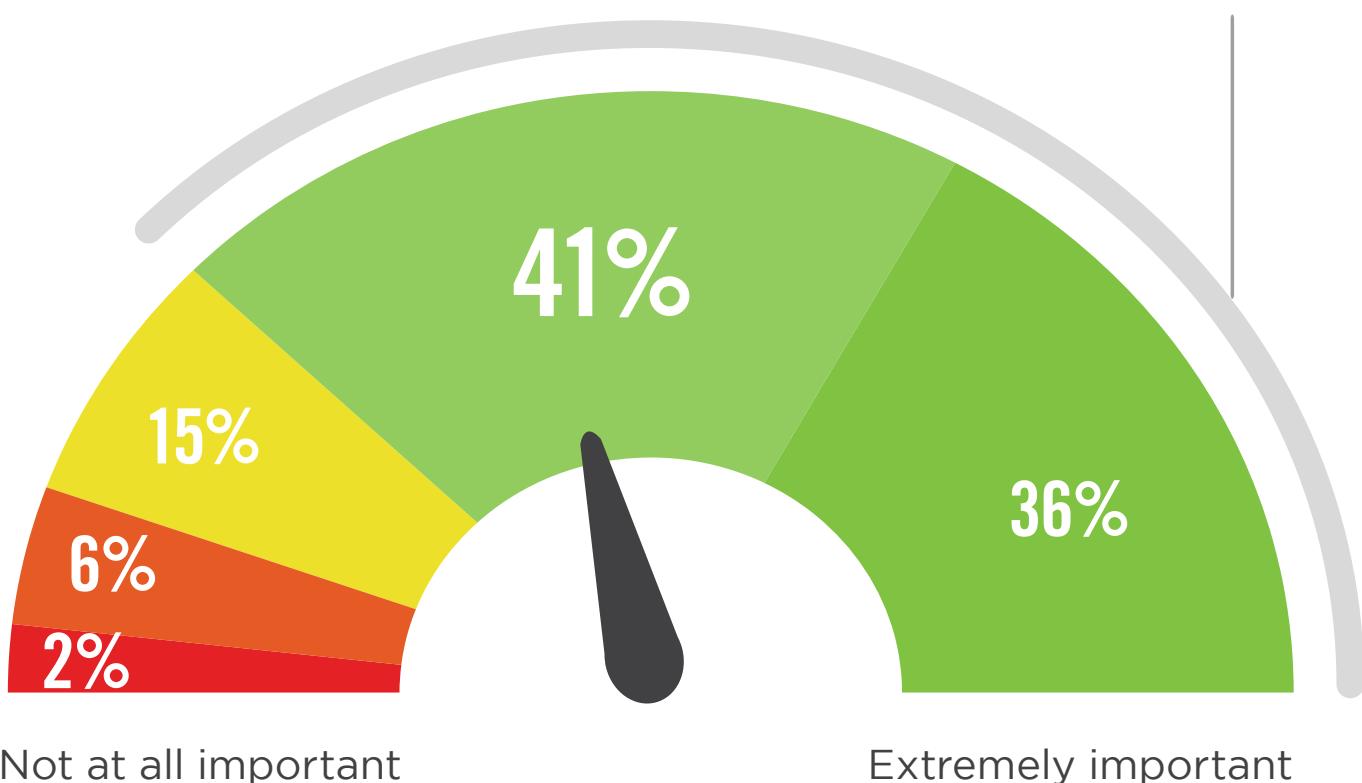
IMPORTANCE OF THREAT INTELLIGENCE

Threat intelligence is not just a “nice-to-have” capability at organizations anymore; it has become a vital part of robust cyber security programs. A large majority of respondents (77%) said threat intelligence is very to extremely important to their organizations’ security posture. Only 8% report threat intelligence as not important.

- ▶ How important is threat intelligence to your organization’s security posture?

Threat intelligence is very to extremely important to organizations’ overall security posture

77%



BIGGEST CYBER THREATS

Respondents are concerned about a plethora of cyber threats, with phishing attacks leading the way, cited by more than half (56%). Other threats they're concerned about include zero-day attacks against publicly unknown vulnerabilities (47%); insider attacks, including malicious or careless insiders (46%); advanced persistent threats/targeted attacks (45%); and malware, including viruses, worms, and trojans (44%).

► Which cyber threats are you most concerned about?



56%

Phishing attacks



47%

Zero-day attacks
(against publicly
unknown vulnerabilities)



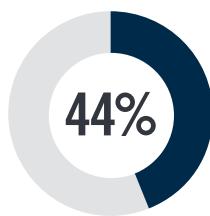
46%

Insider Attacks
(Malicious or
careless insiders)

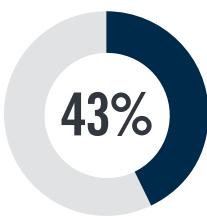


45%

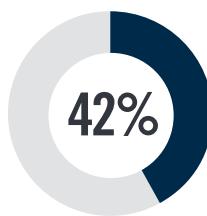
Advanced persistent
threats (APTs)
/targeted attacks



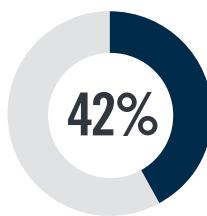
Malware
(viruses, worms,
trojans)



Unauthorized
access



Hijacking of accounts,
services or resources



Ransomware

Web application attacks (buffer overflows, SQL injections, cross-site scripting) 33% | Denial of service attacks (DoS/ DDoS) 22% | Cryptojacking 16% | Other 4%

THREAT MANAGEMENT PRIORITIES

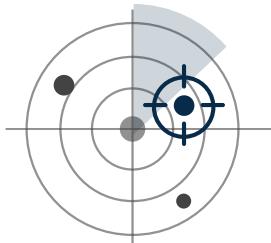
When asked to identify the most critical threat management priorities for their organization, 45% of respondents cited improving threat detection as a priority. Other priorities include proactive threat hunting (39%), improving investigating and analyzing threats (34%), and improving the blocking of threats (34%).

► What are the most critical threat management priorities for your organization over the next 12 months?



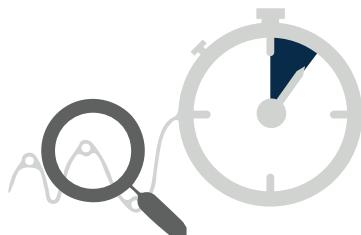
45%

Improve threat detection



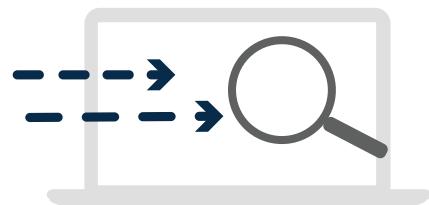
39%

Proactive threat hunting



34%

Improve investigating and analysing threats



34%

Improve lateral movement detection

Improve blocking threats 30% | Improve alerting 29% | Reduce false positive alerts 27% | Reduce unwanted / unauthorized traffic 23% | Automate incident response 21% | Improve enforcement of usage policies 19%
Aggregate security alerts 17% | Other 1%

THREAT MANAGEMENT FOCUS AREAS

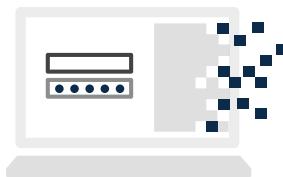
About two thirds of organizations (65%) focus their threat management efforts on denial (for example, firewall, threat intelligence gateway). Other areas of focus and investment include deterrence such as access controls, encryption, and policies (54%), detection such as user monitoring and intrusion detection (50%), incident response and mitigation (47%), analysis and post-breach forensics (45%), and deception such as honeypots (20%).

► What aspect(s) of threat management does your organization mostly focus on and invest in?



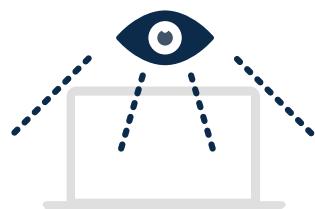
65%

Denial
(e.g. firewall, threat intelligence gateway)



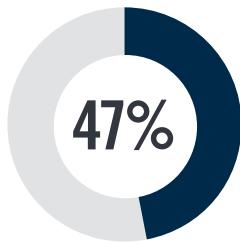
54%

Deterrence
(e.g., access controls, encryption, policies, etc.)

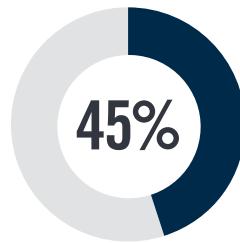


50%

Detection
(e.g., user monitoring, IDS, UEBA, etc.)



Incident Response & Mitigation



Analysis & Post Breach Forensics (e.g., SIEM, log analysis, etc.)



Deception
(e.g., honeypots, etc.)

None/Other 6%

USE CASES FOR THREAT DATA

Organizations are leveraging their cyber threat intelligence data for a number of use cases. Easily the most common use case is detecting threats and attacks, cited by 58% of the respondents. Other uses include incident response (49%), vulnerability management (45%), blocking threats (44%), and blocking malicious domains or IP addresses at egress points such as firewalls and threat intelligence gateways (43%).

► What are the top use cases for your cyber threat intelligence data?



58%

Detecting threats and attacks



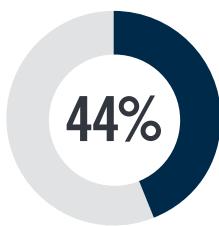
49%

Incident response

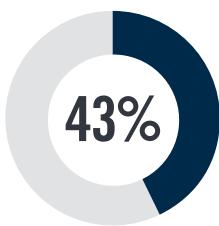


45%

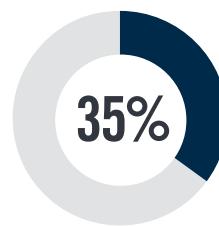
Vulnerability management



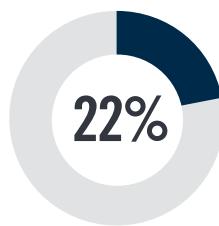
Blocking threats



Blocking malicious domains or IP addresses at egress points



Proactively hunting for indicators of compromise



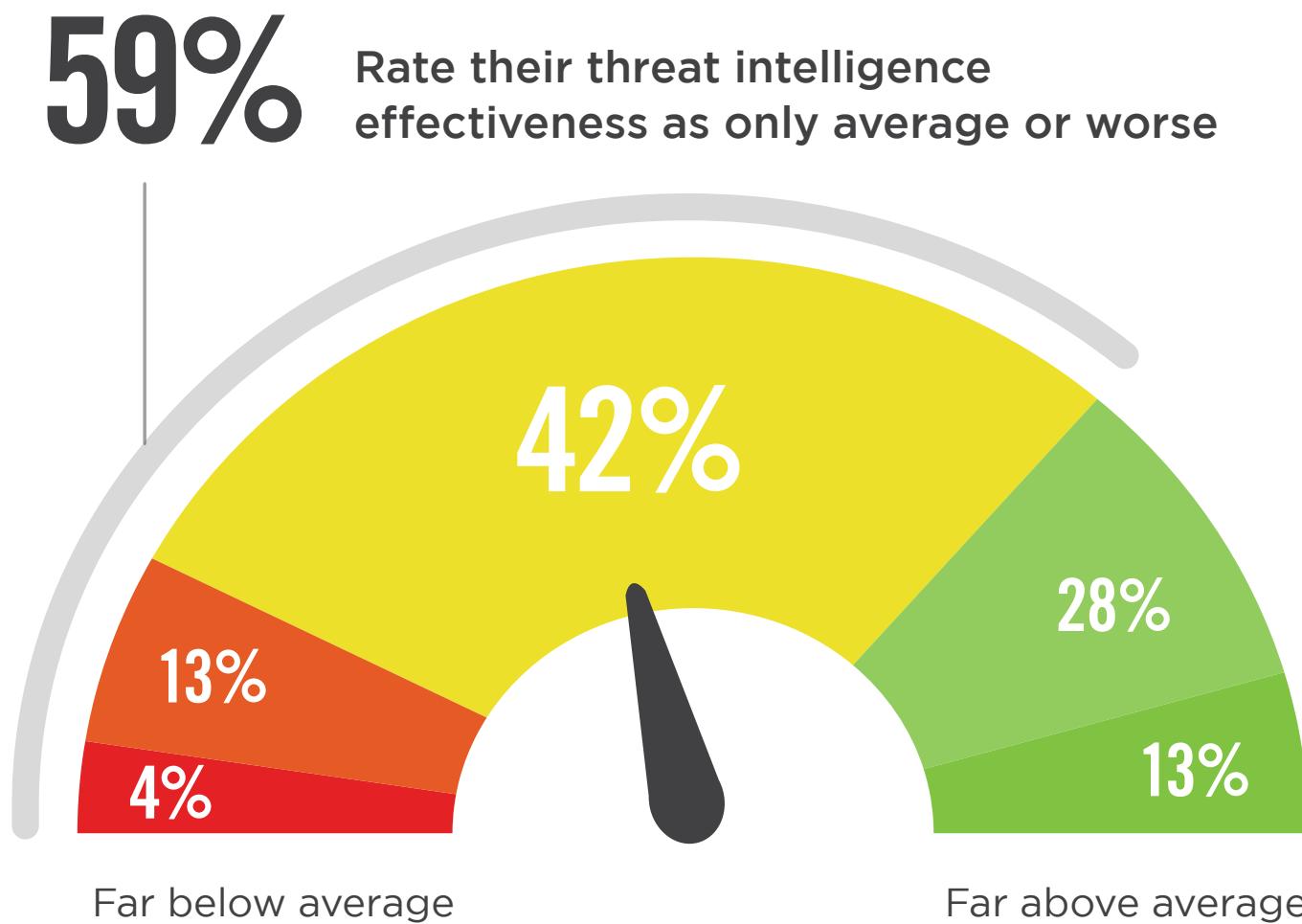
Adding context to investigations or compromise assessments

Providing trending data and reports to team and management 20% | Examining DNS server logs for malicious domains or IP addresses 18% | Building custom IDS signatures for malicious traffic 10% | Adding internally generated indicators to commercial indicators to track campaigns 10% | Other 3%

RATING THREAT INTELLIGENCE EFFECTIVENESS

A majority of respondents (59%) rate their organization's effectiveness in leveraging threat intelligence to identify and remediate cyber threats as only average or worse. Only a small group (13%) rate their organizations as far above average.

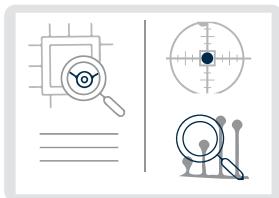
- ▶ How would you rate your organization's effectiveness in using threat intelligence to identify and remediate cyber threats?



BENEFITS OF THREAT INTELLIGENCE

The most common benefit of threat intelligence platforms is better threat analysis, cited by 20% of the respondents. Other benefits include faster detection and response (18%), more efficient security operations (12%), better visibility into threats (10%), and better prioritization of indicators of compromise (10%). Fewer respondents mentioned benefits such as better collection of threat data, reduced staff workload through automation, better threat remediation, and better reporting of threat management.

► What main benefit is your threat intelligence platform providing?



20%

Better threat analysis



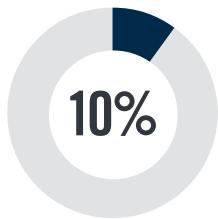
18%

Faster detection and response

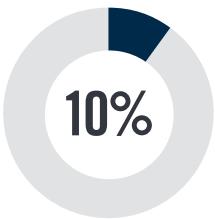


12%

More efficient security operations



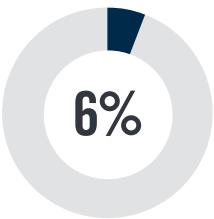
Better visibility into threats



Better prioritization of indicators of compromise (IOC)



No benefits



Better collection of threat data

Reduced staff workload through automation 5% | Better threat remediation 5% | Better reporting of threat management 3% | Other 3%

CHALLENGES FOR SECURITY TEAMS

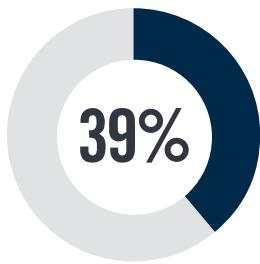
Detection of advanced threats, whether hidden, unknown, or emerging, is cited as the the most common challenge security teams face (43%). Other common challenges teams face include full visibility into assets and vulnerabilities across the entire environment (39%), lack of advanced security staff to oversee threat management (35%), detection and/or mitigation of insider threats (32%), lack of visibility into context around threats (30%), monitoring threats from mobile devices (30%), and too much time wasted on false positive alerts (29%).

► Which of the following do you consider to be top challenges facing your security team?

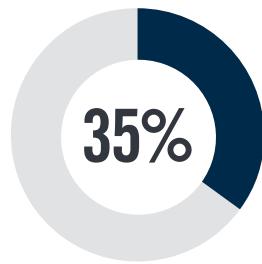


43%

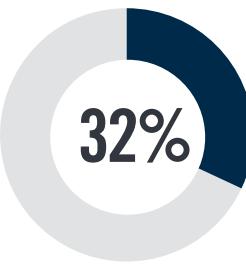
Detection of advanced threats
(hidden, unknown, and emerging)



Getting full visibility
to all assets and
vulnerabilities across
the entire environment



The lack of advanced
security staff to oversee
threat management



Detection
and/or mitigation
of insider threats

Lack of visibility into context around threats 30% | Monitoring threats from mobile devices 20% | Too much time wasted on false positive alerts 29% | Lack of confidence in automation tools catching all threats 26% | Monitoring security of cloud infrastructure 25% | Slow response time to advanced threats 25% | Working with outdated SIEM tools and SOC infrastructure 18% | Lack of proper reporting tools 16% | Other 6%

CYBERSECURITY BARRIERS

Lack of skilled/trained staff is the most common barrier inhibiting organizations from adequately defending against cyber threats, cited by just more than half of respondents. Other common barriers are lack of budget (41%), too many false positives (34%), lack of security awareness among employees (34%), lack of visibility into network traffic and other processes (25%), and poor integration/interoperability between security solutions (24%).

► Which of the following barriers inhibit your organization from adequately defending against cyberthreats?



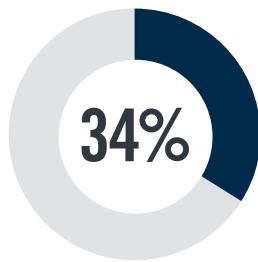
53%

Lack of skilled /trained staff

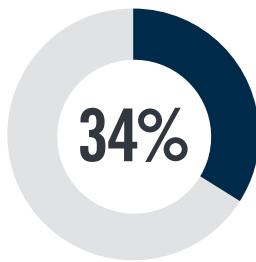


41%

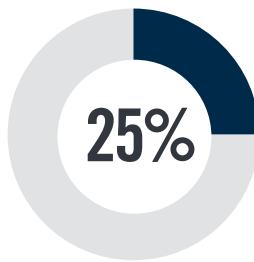
Lack of budget



Too many false positives



Lack of security awareness among employees



Lack of visibility into network traffic and other processes

Poor integration/interoperability between security solutions 24% | Lack of collaboration between separate departments 23% | Lack of management support/awareness/buy-in 23% | Inability to justify additional investment 22% | Insufficient or inadequate tools available in house 22% | Lack of contextual information from security tools 22% | Difficulty in implementing new security systems/tools 21% | Lack of effective security solutions available in the market 11% | Other 5%

THREAT INTELLIGENCE CHALLENGES

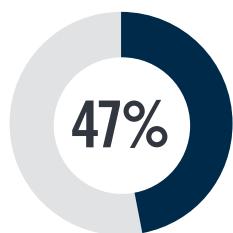
Organizations face several challenges in using threat intelligence. Respondents most commonly cited the greatest challenge as lack of security staff to make threat intelligence actionable (57%). Others: they lack the resources to access external threat intelligence (47%), have difficulty integrating threat intelligence into existing security controls (39%), are not able to effectively and efficiently take action using threat intelligence to prevent threats (39%), and struggle to manage and maintain multiple sources of threat intelligence (31%).

► What are the top challenges your organization faces in using threat intelligence?



57%

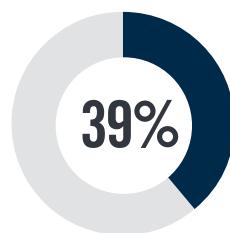
Lack the security staff
to make threat intelligence
actionable



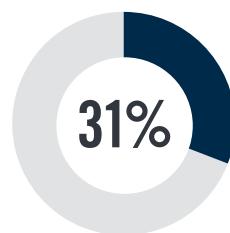
Lack the
resources to
access external
threat intelligence



Difficulty integrating
threat intelligence
into existing
security controls



Inability to
effectively and
efficiently take
action using threat
intelligence
to prevent threats

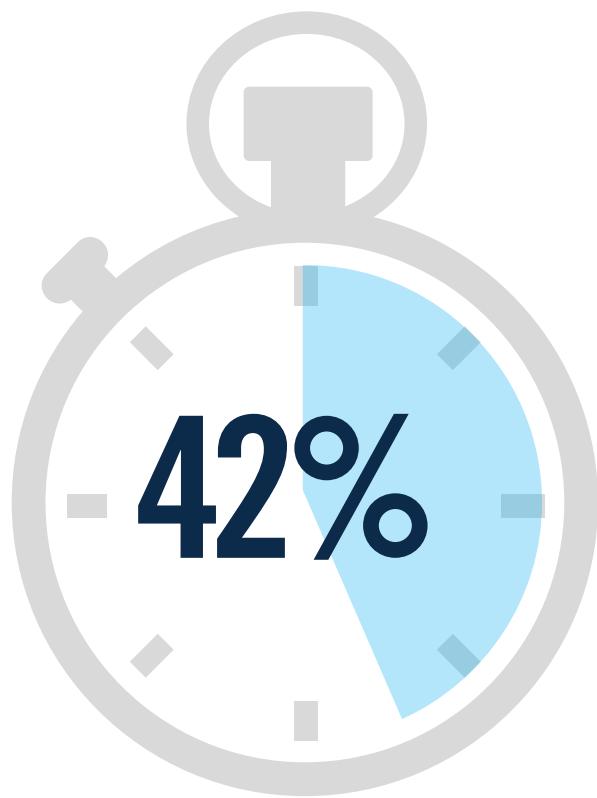


Managing and
maintaining
multiple sources
of threat intelligence

TIME SPENT RESEARCHING ALERTS

A majority of organizations spend over five hours a week manually researching alerts from threat intelligence feeds (58%). Thirty percent spend more than twice as much time.

- ▶ How much time per week is spent researching alarms from threat intelligence feeds?



<5 hours
per week



5-10 hours
per week



10-15 hours
per week



more than 15 hours
per week

58% spend more than 5 hours
a week researching alerts

CRITICAL FEATURES

When evaluating threat intelligence platforms, speed and continuous monitoring of threats are high priorities for organizations. When asked to identify the most important features of platforms, more than half of the respondents cited rapid identification and remediation of attacks (56%) and 24x7 threat intelligence, monitoring and analysis (54%). Also important are the ability to assess risk and prioritize threats (41%), integration with other platforms (40%), and management of indicators of compromise (38%).

► What are the most important features of a threat intelligence platform?



56%

Rapid identification and remediation of attacks



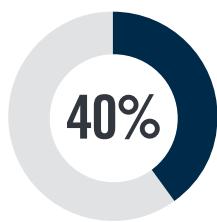
54%

24x7 threat intelligence, monitoring and analysis

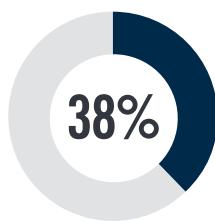


41%

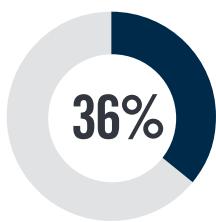
Ability to assess risk and prioritize threats



Integration with other platforms (SIEM, NGFW)



Management of indicators of compromise (IOC)



Continuously updated indicators



Threat assessment reports to identify vulnerabilities and risks

Easy incident investigation and threat research 30% | Security policy and controls management 23% |
Compliance oriented activities 14% | Other 5%

DATA SOURCES

Organizations are collecting data from a wide variety of systems, services, and applications. Leading the way are vulnerability management tools such as scanners, configuration and patch management, etc., mentioned by 61% of respondents. Other common data sources are network-based firewalls/threat intelligence gateways/intrusion prevention and detection systems (54%), applications including event logs and audit logs (52%), SIEM technologies and systems (50%), and host-based anti-malware software (48%).

► What systems, services and applications do you collect data from?



61%

Vulnerability management tools
(scanners, configuration and patch management, etc.)



54%

Network-based firewalls/threat intelligence gateways/IPS/IDS/UTM devices

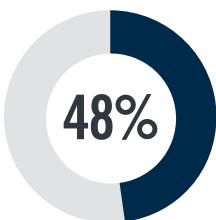


52%

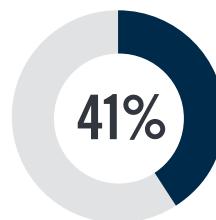
Applications (event logs, audit logs)



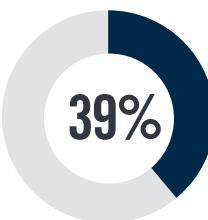
SIEM technologies and systems



Host-based anti-malware



Security intelligence feeds from third-party services



Network packet-based detection

Static Endpoints (PC, NAC, log collectors) 38% | Intelligence from your security vendors 36% | Whois/DNS/Dig and other Internet lookup tools 35% | Network-based malware sandbox platforms 35% | Dedicated log management platform 35% | Host-based IPS/IDS 35% | User behavior monitoring 33% | Mobile Endpoints (mobile devices, MDMs, mobile apps) 30% | ID/IAM (identity and access management) systems 27% | Relational Databases (transactions, event logs, audit logs) 27% | Cloud activity 27% | Netflow 22% | Social media applications (Facebook, Twitter) 19% | Management systems for unstructured data sources (NoSQL, Hadoop) 12% | Other 5%

METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of cybersecurity professionals to gain more insight into the latest trends, key challenges and solutions for cyber threat intelligence. 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.

CAREER LEVEL



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

DEPARTMENT



■ IT Security ■ IT Operations ■ Engineering ■ Compliance ■ Product Management ■ Sales ■ Other

COMPANY SIZE



■ Fewer than 10 ■ 10-99 ■ 100-499 ■ 500-999 ■ 1,000-4,999 ■ 5,000-10,000 ■ More than 10,000

INDUSTRY



■ Technology, Software & Internet ■ Government ■ Professional Services ■ Financial Services ■ Education & Research
■ Healthcare, Pharmaceuticals, & Biotech ■ Manufacturing ■ Computers & Electronics ■ Energy & Utilities ■ Other