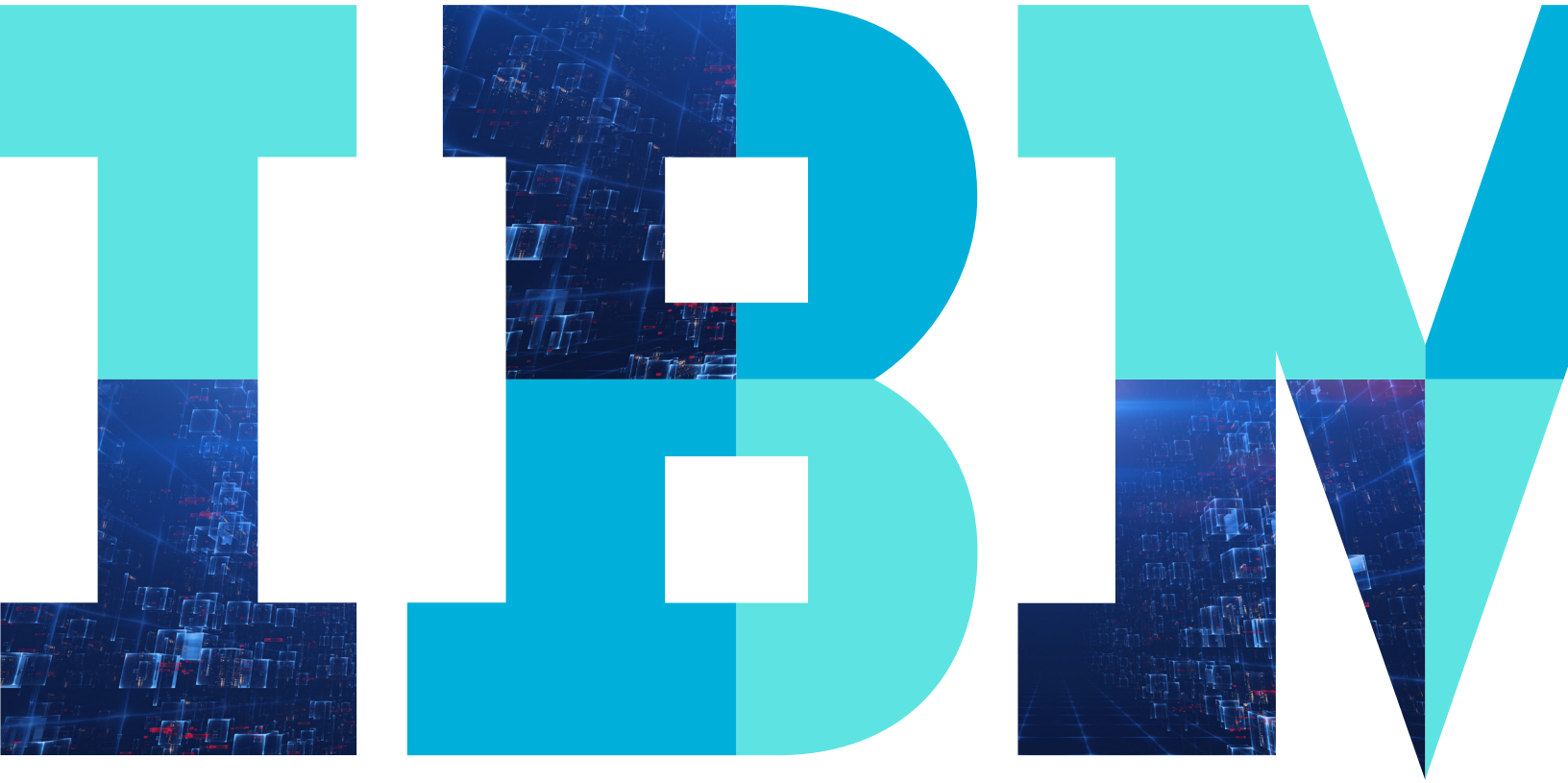
IBM Security
White paper

Master threat hunting

The creative science of threat hunting.



Contents

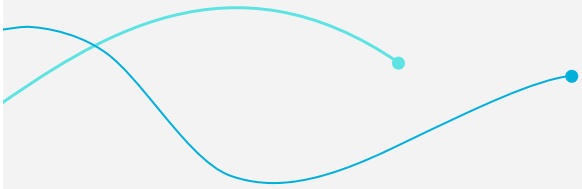
Key points

Threat hunting is an art *and* a science

The 20 percent of attacks you miss cause 80 percent of the damage

Master threat hunting to find threats sooner

The right technology and people find threats up to 60 times faster



The hunt is on

In a world where millions of new cyberthreat signatures and viruses are created each day, it might seem crazy to go looking for trouble. After all, trouble will find you soon enough. Yet even with the best tools, organizations only catch about 80 percent of all cyberthreats. It's the other 20 percent of cyberthreats — the minority of unknown and undetected threats — that cause the majority of damage.

It's the 20 percent of unknown/ undetected cyberthreats that are responsible for 80 percent of the damage caused by cyberattacks.

Smart organizations do more than react to security threats. They proactively hunt for threats in their networks, endpoints and systems. *Threat hunting* has become a security best practice in organizations around the world. As the name implies, threat hunting isn't a passive process, but a high-stakes hunt for enemies that involves a unique mix of technology, intelligence, skill and intuition.

The security analysts who perform threat hunting are after big game: data exfiltration schemes that sell private data to the highest bidder, the inception files of ransomware attacks that hijack data systems, viruses that can redirect online traffic to copycat phishing sites, and the list goes on. During the hunt, time is of the essence. The longer a threat stays lurking in your network, the more damage it causes.

69%

Of all data breaches are executed by state actors or advanced criminal organizations.[1]

90%

Of breaches caused by inside actors or privilege abuses took weeks, months or years to discover.[2]

197 days

Is the average time to identify data breach incidents by the security team.[3]

$3.86 million

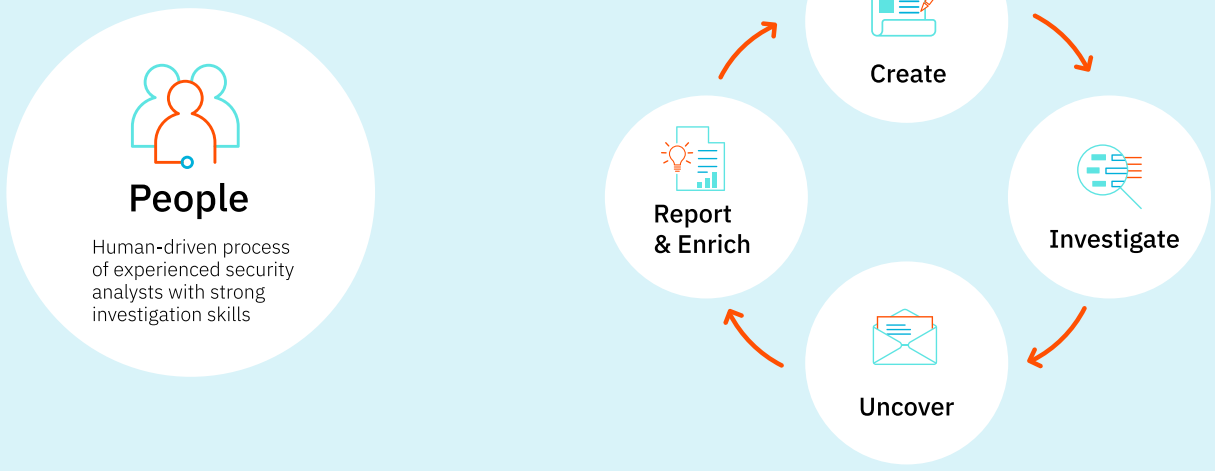
Is the average total global cost for a single data breach.[4]

The art and science of the hunt

Threat hunting isn't simply a person or a piece of software. It's a combination of person and machine, of art and science. Threat hunting requires a great deal of skill, concentration, collaboration and more than a little creativity. These are the areas where the human mind excels. But threat hunting also requires the right technology to sift intelligence from a vast sea of data, spot anomalies in system logs and automate the process using a global network of threat intelligence.

Threat hunters use data, analytics and visualization tools the way an artist uses a palette, putting the pieces together until a clear picture emerges. Once they create that image, threat hunters then use their investigative skills to look for potential cyberthreats. As they uncover new threats, hunters rely on their expertise and close collaboration with their teams to quarantine and safely remove the threat. When the threat is over, that experience is reported and shared with security colleagues to enrich their joint threat intelligence and prevent future attacks of a similar nature.

The art of threat hunting

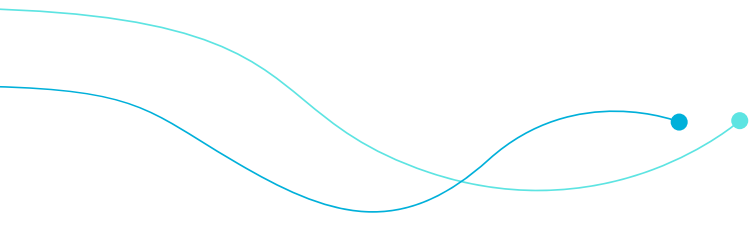


Meet an IBM Threat Hunter

Plan, prioritize and prepare

It's easy enough to spot a lion in a herd of zebras, but what do you do when everything looks like a lion? Security analysts know that a successful hunt starts with knowing your *prioritized intelligence requirements*. Start by asking the right questions (below), then discover what data is likely to hold the answer.

- What are the main security risks we face as an organization? Data exfiltration? Ransomware? Denial-of-service attacks?
- Who needs the most protection in our organization?
- Which of our data assets hold the most value to criminals: competitive data, customer data, financial data, etc.?
- Where are we most exposed: our network, our employees, our partners?
- What kind of technology is deployed in our network, how is it used and how can it be abused?



The problem is deeper than you think

Cyberattacks often seem to present themselves all of a sudden. In reality, the most dangerous attacks often lurk undetected in your network for months before they manifest. *Dwell time* — the period between a cyberattack's entry into the network and its eventual detection — is **more than six months on average**. It might seem that threat hunters have plenty of time to capture and kill cyberthreats before they activate, but the fact that detection takes so long underscores the difficulty of doing that.

The depth of the cyberthreat problem doesn't reflect a deficiency in security technology so much as it reflects the growing proficiency of the cybercriminal community. Fraud, ransomware and attacks-for-hire are a billion-dollar industry, and cybercrime organizations treat their operations like a profitable business. They innovate, they disrupt and they're constantly on the lookout for ways to increase their ROI. They also use multipronged attacks outside the view of traditional security systems to plant the seeds for their nefarious activities.

Organizations that master the art and science of threat hunting can reduce dwell time from months to minutes. Experience shows that, the more time a cyberattack spends in your systems, the more damage it does: to your customers, your business, your brand reputation and your bottom line.

91 percent of security leaders believe threat hunting increases the speed and accuracy of their response to cyberthreats.[5]

Better hunting through science

Standard security tools are great at detecting and blocking the known 80 percent of cyberattacks that come flooding into your network every day. But it's the perilous 20 percent you don't know about that present the biggest risk to your organization. How do you find what you don't know? By giving threat hunters better tools to hunt with, including data from different sources and advanced analytics to help them identify new patterns, models and behavior.

The science of threat hunting is a holistic discipline that integrates internal data, external data and intelligence, statistical analysis and intelligence analysis to give threat hunters better visibility into hidden threats. You can think of this technology as the threat hunter's night-vision goggles; without it, they're looking for a black hat in a dark forest.

Internal data and systems represent aggregated data from the entire organization, including data that might not typically appear as part of a Security Incident and Event Management (SIEM) tool, such as human resources information and emails. This data can help threat hunters create richer user profiles, set alerts and rules and correlate their hypotheses around *unknown* threats.

Statistical analysis tools help threat hunters detect anomalies, patterns and relationships in the data that could indicate the presence of a threat. It's here that you'll find next-generation security systems such as User and Entity Behavior Analytics (UEBA), which allow security analysts to quickly identify abnormal behavior by setting a baseline definition for what constitutes "normal" user behavior.

External data and intelligence bring in threat intelligence from the wild. With these tools, threat hunters can manually analyze where data points intersect, connect internal and external data to expose new risks, confirm events such as hijacked accounts and bring non-traditional, unstructured data (e.g., social media posts, news feeds, data on the dark web) into the light for deeper analysis.

Intelligence analysis includes advanced visualization tools that assist threat hunters in quickly investigating and researching correlations and links. These tools can be used to view a user's risk profile, track their activities over a timeline, identify trends, chart geospatial relationships and more.

Watch the Science of Threat Hunting

Elevate your security posture

Threat hunting is more than a security best practice. It's your best chance at stopping the most dangerous cyberthreats in the criminal's arsenal. When done with the right balance of art and science, threat hunting has a profoundly positive effect on your security posture:

- It exposes previously hidden security vulnerabilities
- It dramatically accelerates threat response times
- It detects hidden threats much sooner, reducing their dwell time and their potential for damage
- It helps you improve and automate countermeasures for continued security

Threat hunting sharpens your security skills

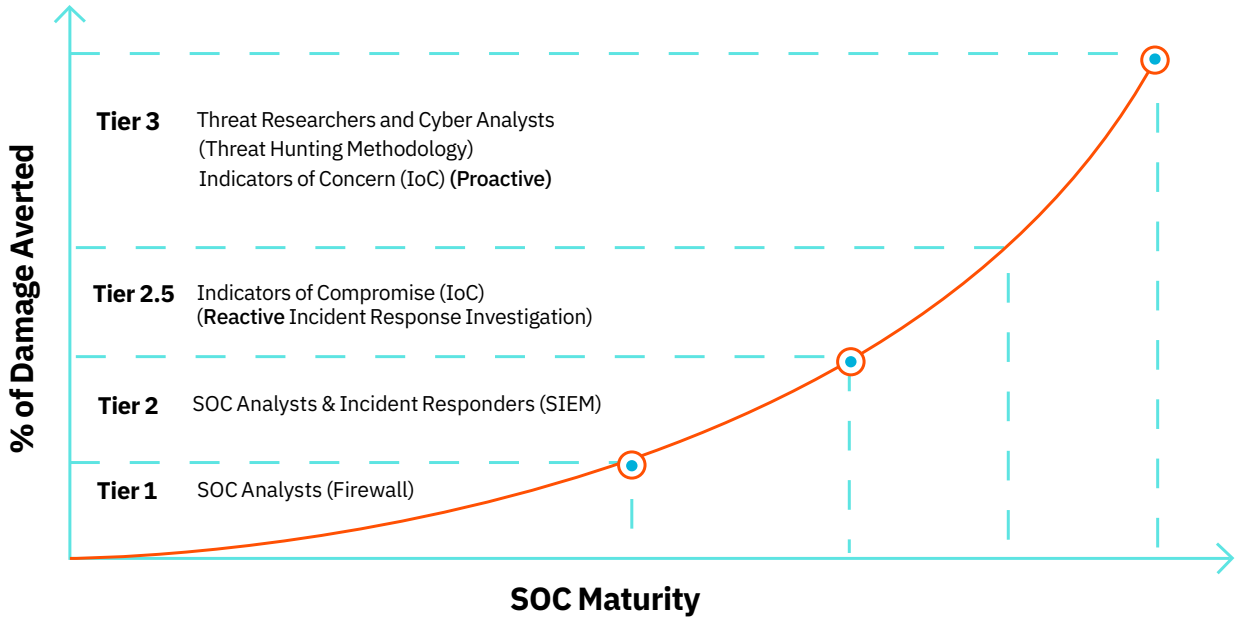
Threat hunting strengthens your security analysts, giving them a deeper understanding of the threats, risks and vulnerabilities that affect your organization. An empowered threat hunting team can supercharge your Security Operations Center (SOC), strengthening your organization at the highest tiers of its security efforts. Over time, threat hunting programs can even help organizations retrain Level 1 and Level 2 security analysts to become master threat hunters, while using automation, artificial intelligence (AI) and other tools to address L1/L2 security incidents.

Tier 1: This is where you'll find the high-volume, low-expertise attacks including common viruses, garden-variety attacks and amateur hackers.

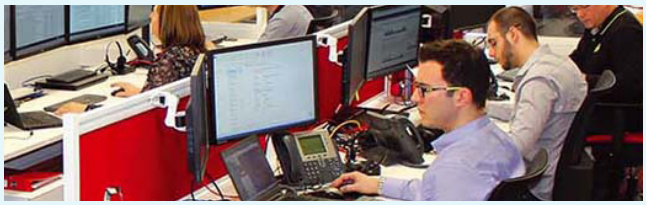
Tier 2: This is where your SIEM system comes into play as you respond to known threats and attacks.

Tier 2.5: This is where threat hunters first enter the picture, tracking plausible threats using Indicators of Compromise.

Tier 3: And this is where threat hunters shine, using a mix of creativity and technology to capture and kill hidden threats before they cause damage.



Artificial Intelligence, in combination with Security Operations Centers, can help security analysts investigate threats up to 60 times faster and uncover 10 times more actionable threat indicators.



Case study: Reducing threat investigation and root cause determination from three hours to three minutes

Learn how security analysts at Sogeti Luxembourg were able to investigate threats faster, protect their reputation and prevent millions of dollars in damages with cognitive technology from IBM.

→ **Read the full case study**

Master threat hunting, and you master much more

Security Ops teams have seen it all at one time or another, and they have the processes in place to stop most of it. But there are many types of threats that can slip through your SOC. In these scenarios, threat hunting can uncover and address pernicious cyberthreats before they can impact your organization as well as other operational points of concern, from HR to marketing:

- Advanced persistent threat (APT) discovery
- Insider threat identification and investigation
- Disgruntled employee identification
- Employee sensitive data caching
- Asset vulnerability vs.criticality comparison
- Threat campaign tracking
- Strategic report production for leadership
- Host-based intrusion prevention system (HIPS) and intrusion detection system (IDS) correlation
- External scanning pattern analysis
- Spear-phishing identification and impact analysis
- Pirated software use identification
- Threat intelligence integration into incidents
- Big data analysis search across large data sets
- Fraud detection and investigation
- Retrace trades for compliance
- Insider trading identification and investigation
- Executive information security protection
- Reputation and brand awareness
- Integration of state-level threat reporting
- Vendor risk management compliance tracking
- Identify employees with competitive “side jobs”
- Identify individuals leaking info to media
- Discover customer data leaked online
- Discover leaked sensitive documents online
- Dark web data aggregation and discovery
- Social media monitoring and investigation

What does it take to be a master threat hunter?

Master threat hunters aren't born. They're made from a mix of experience, intelligence and technology. Here's what it takes to be a master threat hunter in your organization:

- The ability to tap into a deluge of data from disparate (and often disconnected) sources
- The tools and training to turn data into actionable security intelligence
- Access to the latest threat intelligence to sharpen your hunting skills
- An orchestrated and repeatable approach to threat hunting

It's survival of the smartest

Cyberthreats are evolving at a frightening pace. For every known attack signature, there are thousands more being spawned each second. Cybercrime is no longer the hobby of disgruntled engineers or bored teenagers, but a sophisticated billion-dollar industry with advanced technology and highly skilled personnel spread across the globe. It doesn't just *feel* like you against the world. It is you against the world.

Fortunately, organizations can fight back. With advanced technology, powerful partners and, most importantly, the right people, security teams can turn the tables on cybercriminals and become the hunter instead of the hunted. For more information on how you can master threat hunting with IBM products and services, visit us online at ibm.com.

Master threat hunting with IBM Security products and services

Internal data and systems

IBM QRadar Security Intelligence Platform

Intelligence analysis

IBM i2 Enterprise Insight Analysis

External data and intelligence

IBM QRadar Advisor with Watson

People

IBM Managed Detection and Response Services

IBM Managed SIEM Services

IBM X-Force Incident Response and Intelligence Services (IRIS)

Statistical analysis

IBM QRadar User Behavior Analytics

Sources

1. Ponemon Institute 2018 Cost of Data Breach Survey.

2. 2017 Verizon Data Breach Investigations Report, 10th Edition.

3. Ponemon Institute.

4. Ponemon Institute.

5. The Hunter Strikes Back: The SANS 2017 Threat Hunter Survey.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
November 2018

170-21717-USEN