THE STATE OF SECURITY OPERATIONS

Revealing the Big Picture

Start here

Contents

“What a waste”

We are all constantly trying to improve our cybersecurity defenses, but sometimes it feels like a losing battle, with too many alerts, lack of visibility and analysis, complex multiple systems and not enough staff.

Meanwhile, the attack continues.

Bad Actors

Bad actors are working around the clock developing new ways to make their way into our networks. They’re using AI to sniff out vulnerabilities, pitting their tools against a raft of detection schemes—triggering endless alerts, burning out dedicated security staff.

Old and New Methods

They’re still preying on people’s fears or generosity to compromise passwords. We’ve got a lot of work to do to protect our technology infrastructure from their attacks.

Protect and Defend

Because there is a mix of old and new methods for attack, we need a mix of old and new tools to thwart them. As cybercriminals become more sophisticated, so too must our strategy to defeat them.

Let’s look at the current state of cybersecurity and how we can plug some of the holes in our defense →

State of Play

Ideally, cybercriminals would be nice and friendly, writing their malicious code to some standard that our Security Information and Event Management (SIEM) system understands. Our Security Event Management (SEM) and Security Information Management (SIM) tools would see that carefully-crafted malware and send us nice, polite alerts describing what we should do about them.

That’s not the world we’re living in.

We asked a group of 1,200 security professionals, and they had some interesting things to tell us:

No SIEM solution

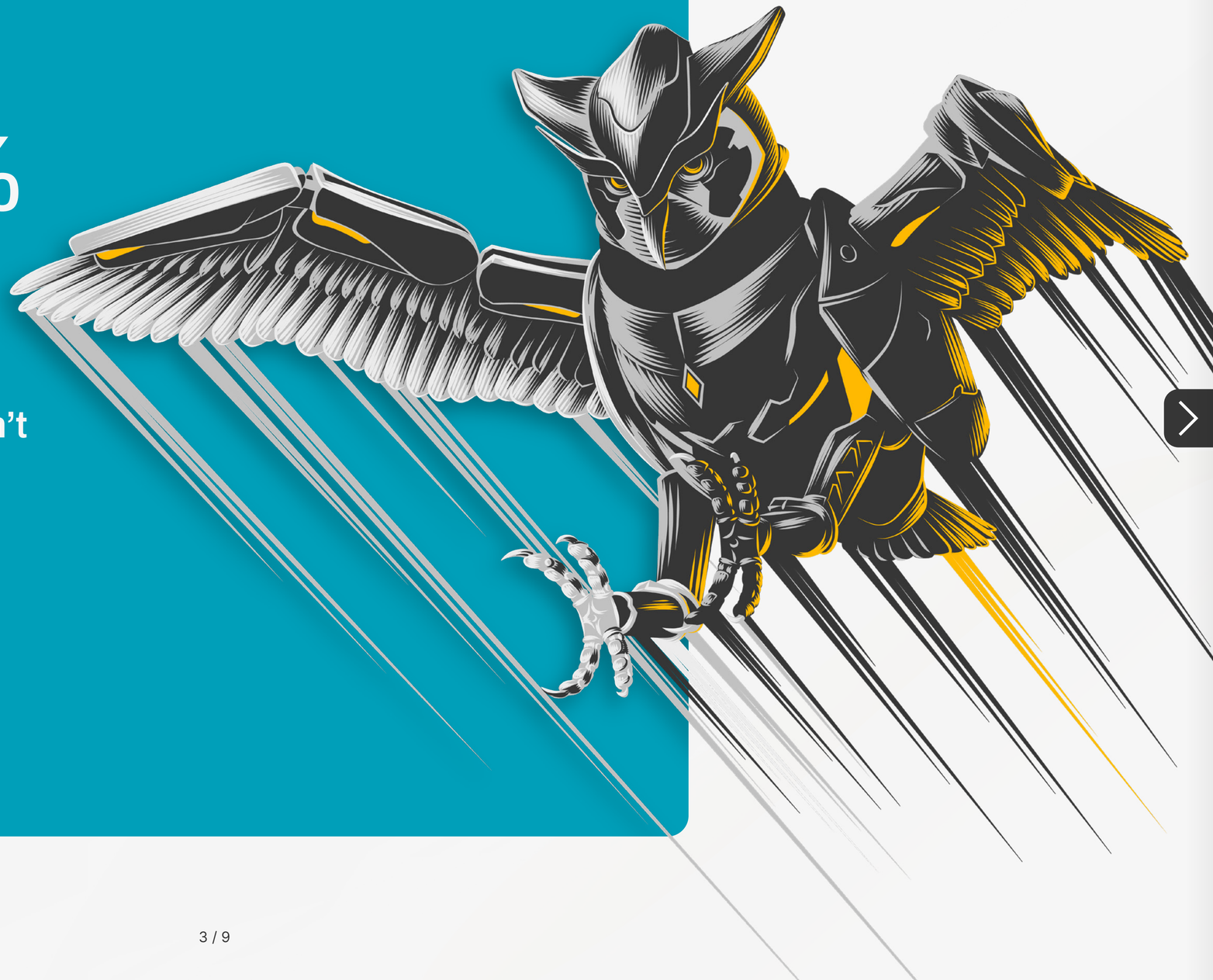
Time To Respond

Excessive alerts

17%

of respondents reported that they don't have a SIEM solution.

Of the rest, they need **two to three SIEM queries** just to triage an alert.

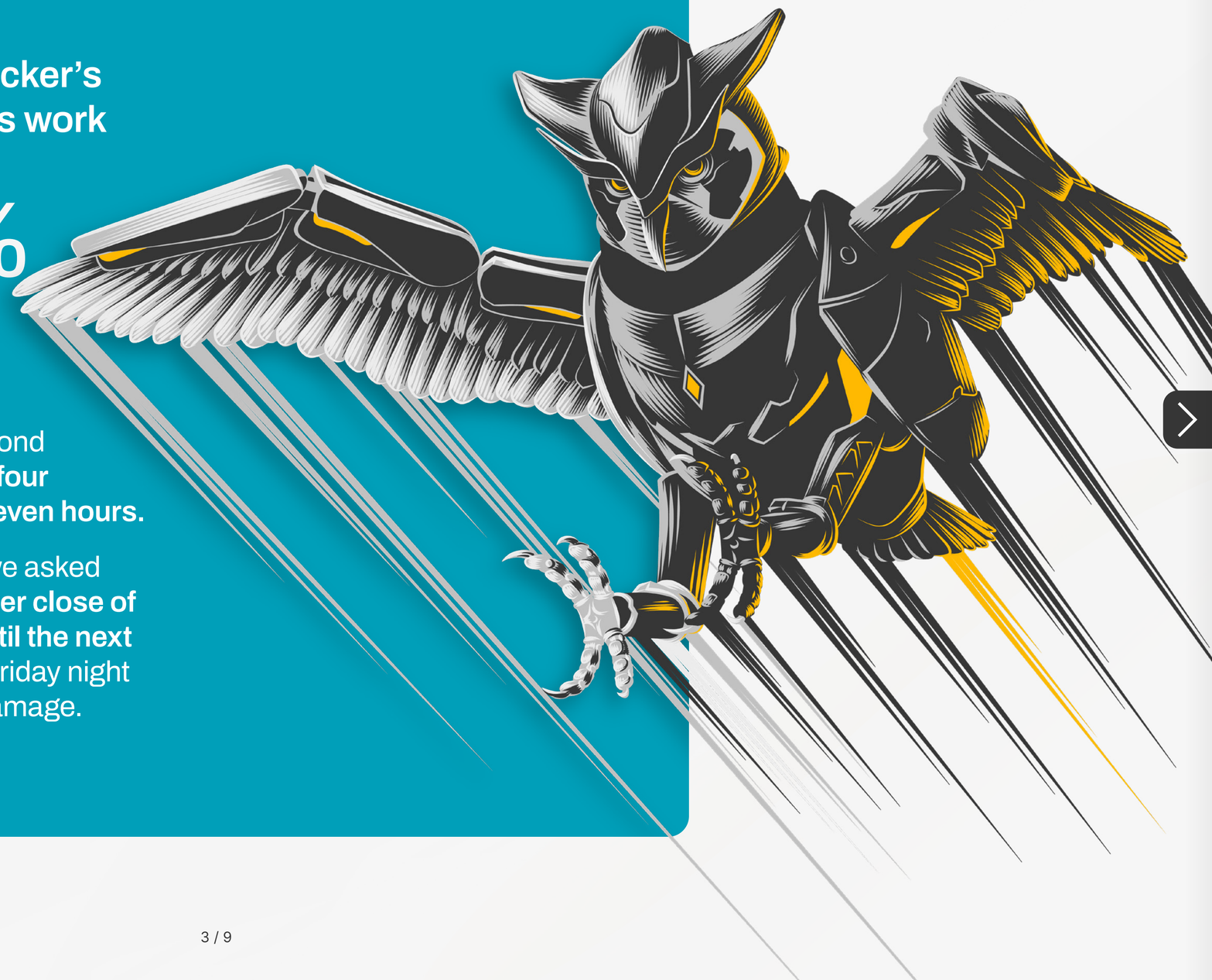


How long has the attacker's payload been doing its work inside your network?

55%

say their Mean Time to Respond (MTTR) is between **two and four hours, 19% say it's five to seven hours.**

Over half of the companies we asked say that **an alert received after close of business isn't even seen until the next business day.** That gives a Friday night attacker all weekend to do damage.



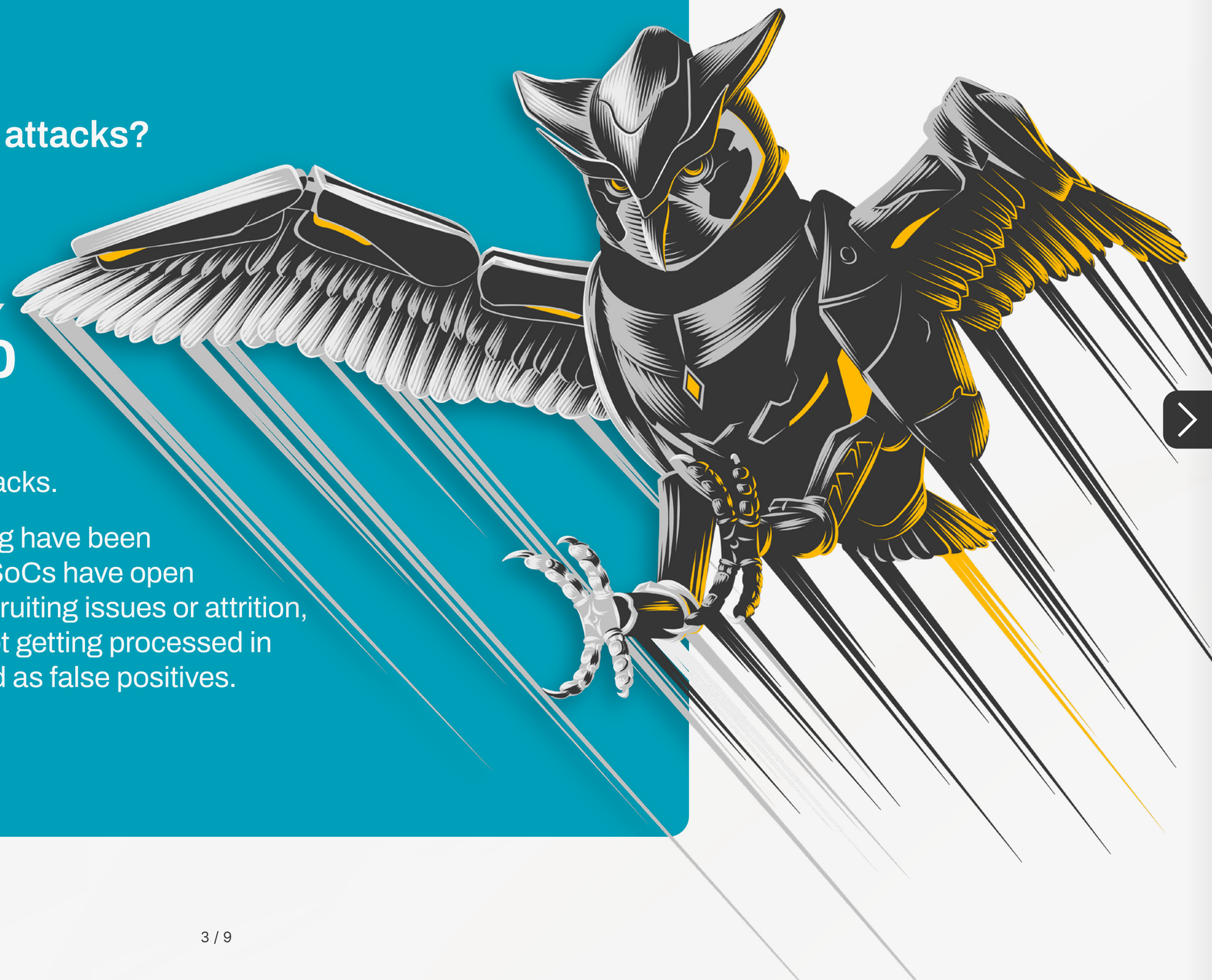
Are you seeing all the attacks?

The security professionals in our survey think they're missing up to

20%

of attacks.

And the alerts they are getting have been overwhelming staff. **25%** of SoCs have open positions, whether due to recruiting issues or attrition, so it follows that alerts are not getting processed in a timely manner or dismissed as false positives.



Data Analysis vs Cost

We talk about solving these problems with more data...

Alerts Retention Costs Analysis

The volume of false alerts and the lack of quality information available to analysts is adding stress to security teams, and causing burnout.

The experts on your staff become absorbed in low return investigative work and may not be able to get through a day's worth of alerts in a working day.

To get better, more accurate alerts, it follows that you need better, more accurate information about those alerts.

Data Analysis vs Cost

We talk about solving these problems with more data...

Alerts **Retention** Costs Analysis

If you're on the receiving end of threat alerts you know that they happen all the time and collecting data about each of them will be a huge and costly undertaking, particularly if you want to retain raw data and not just the alerts.

Most of our respondents only retain their data from one to six months.

Retention decisions are trying to strike a balance between costs, privacy, analytic capabilities, and data retention regulations across regions.

Data Analysis vs Cost

We talk about solving these problems with more data...

Alerts Retention **Costs** Analysis

Longer retention times and the ability to analyze a deeper data set, would be better from a threat analysis standpoint as well as for reporting, but collecting and storing more data is expensive.

Costs increase not only for housing the data, but also the required tools and expertise to analyze the complexity of structured and unstructured data can be prohibitive.

Conversely, working with the bare essential data will increase your costs over time, due to staff turnover or worse, the impact of an effective undetected breach.

Data Analysis vs Cost

We talk about solving these problems with more data...

Alerts Retention Costs **Analysis**

Your security team can be overwhelmed with alerts, not have the depth of data, or not have access to the right tool set, to enable them to complete their forensic investigations and remediate the impact of an incident, in a timely, effective and efficient manner.

36% of our respondents have resolved this by hiring an outside forensics firm, **but is there another way?**

The Job Ahead

These problems aren't going to be solved through technology alone.

For any successful defense against cybercrime, we need to focus on the people.

Recruiting

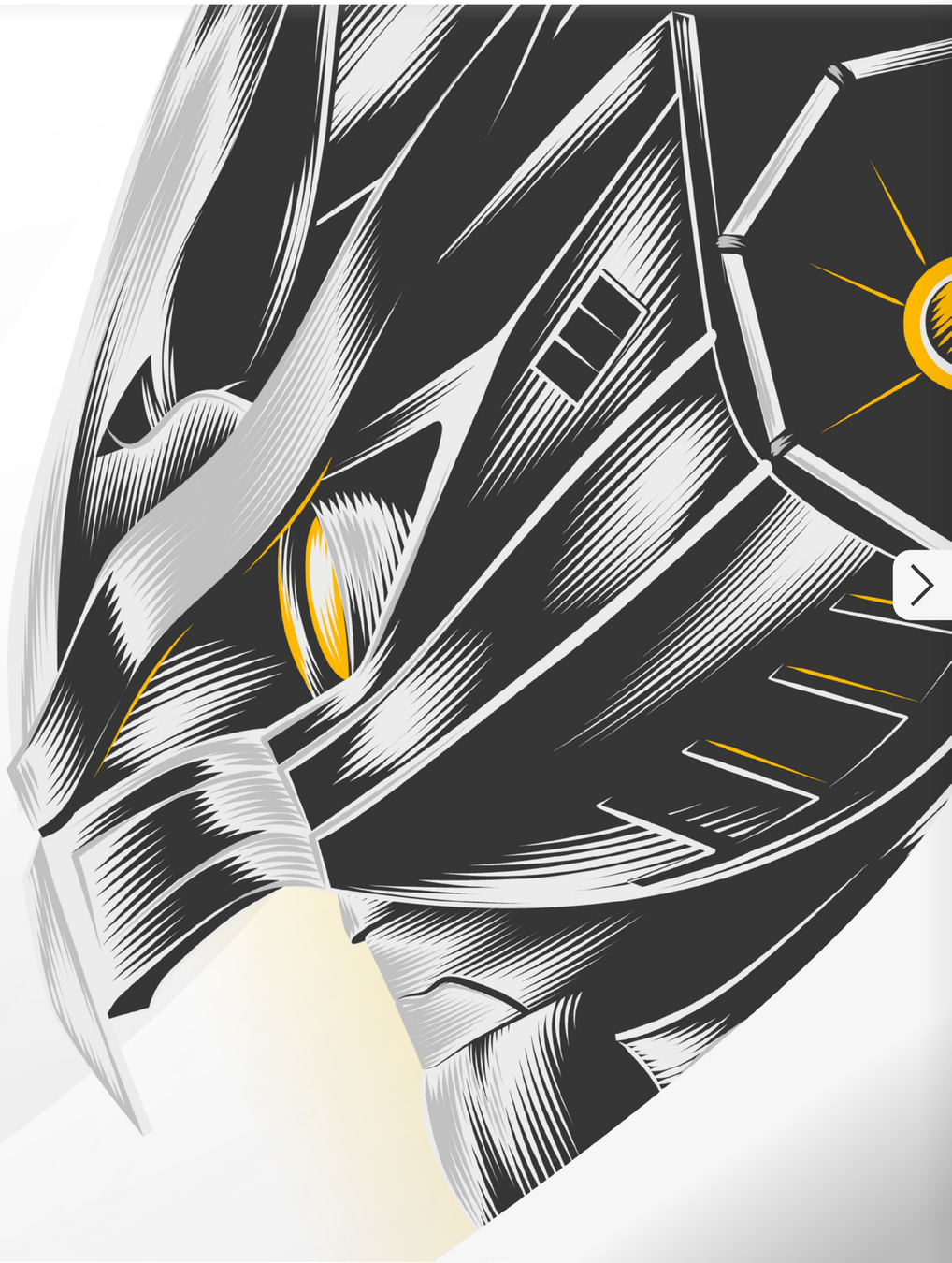
Recruiting security staff with more credentials fills the headcount gap, **but it is notoriously difficult and expensive.**

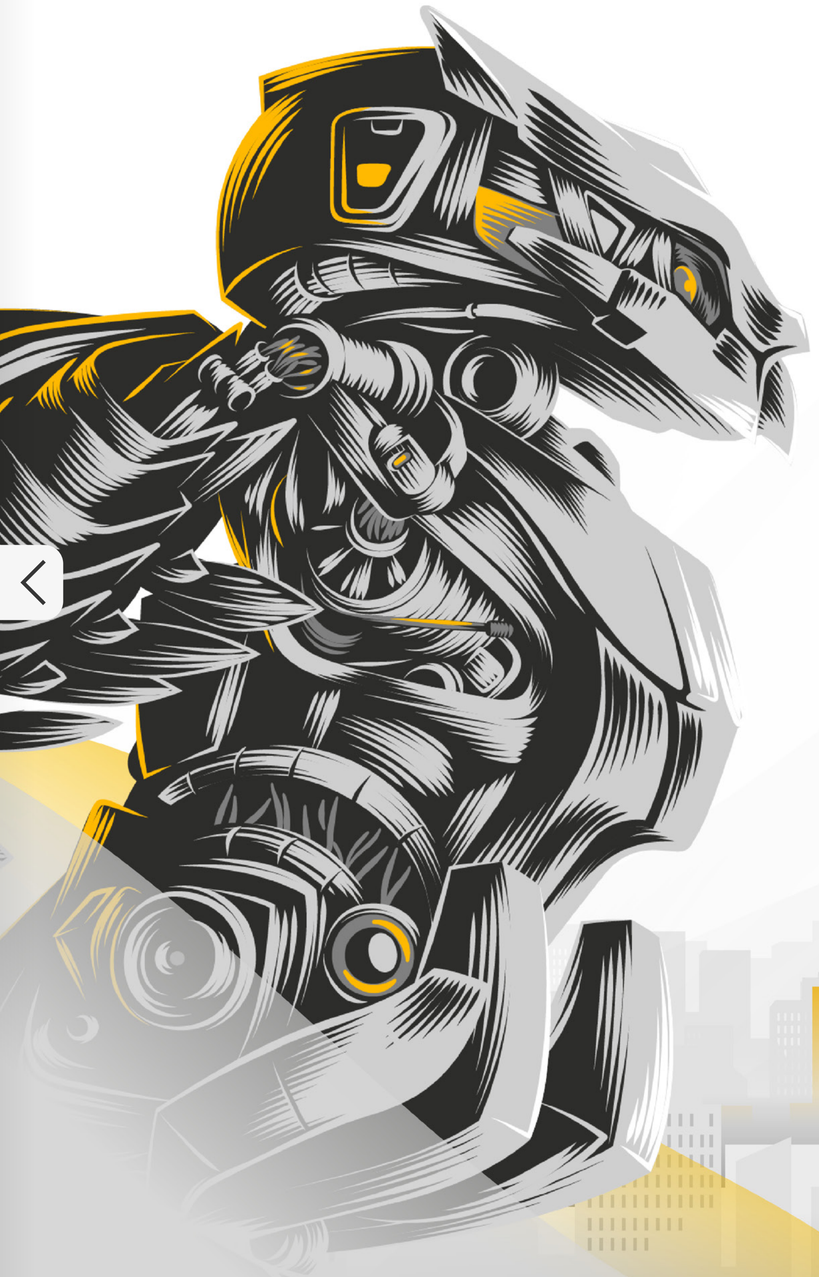
Outsourcing

You could outsource some of your security operations, **like 33% of our respondents have,** but lengthy onboarding and recurring costs could be a problem for the CISO.

Training

Training your existing staff on new tools and providing deeper analytics capabilities is more cost effective and it could aid retention too. **58% of our survey respondents are considering the use of AI and automation to fill their skills gap.**





Help Has Arrived

Security professionals are no stranger to the benefits of artificial intelligence.

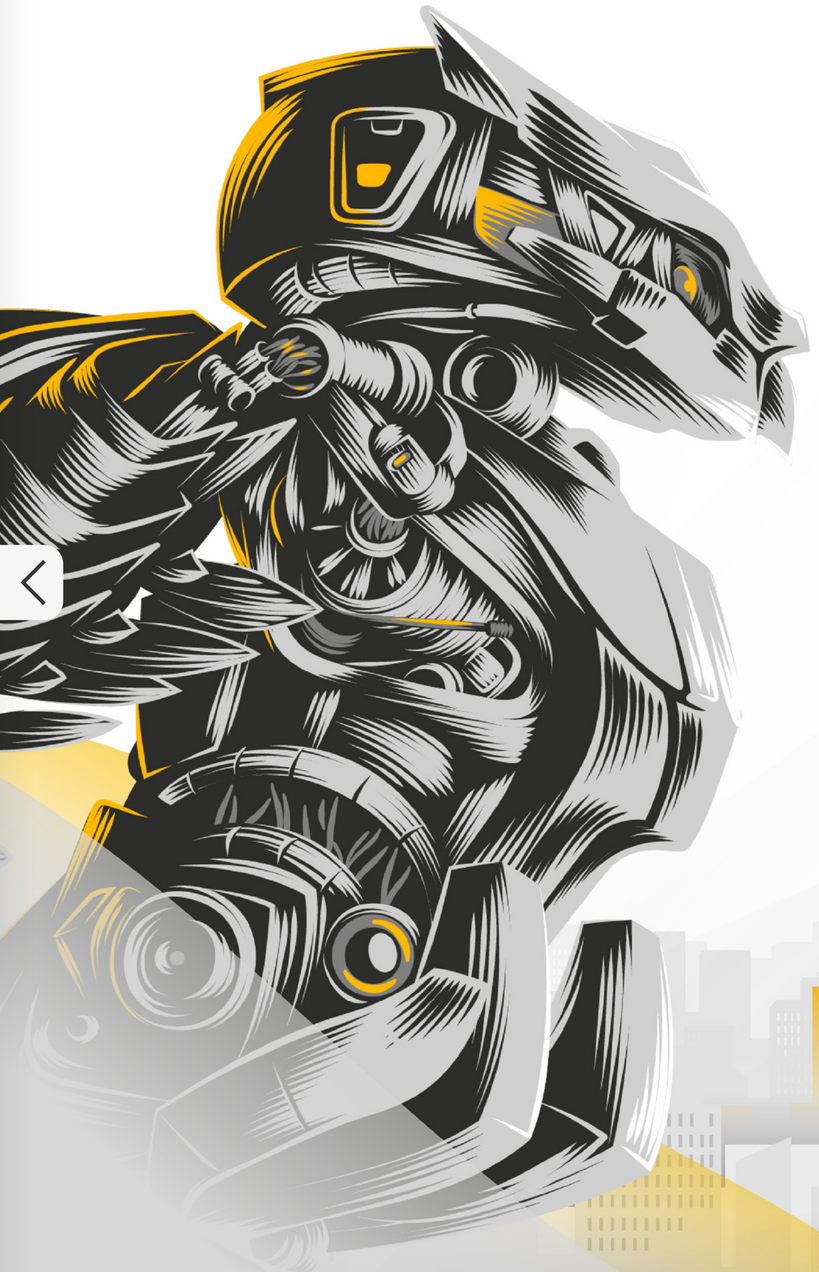
#01 Generative AI

#02 Hurdles

#03 Reaction

#04 Integration

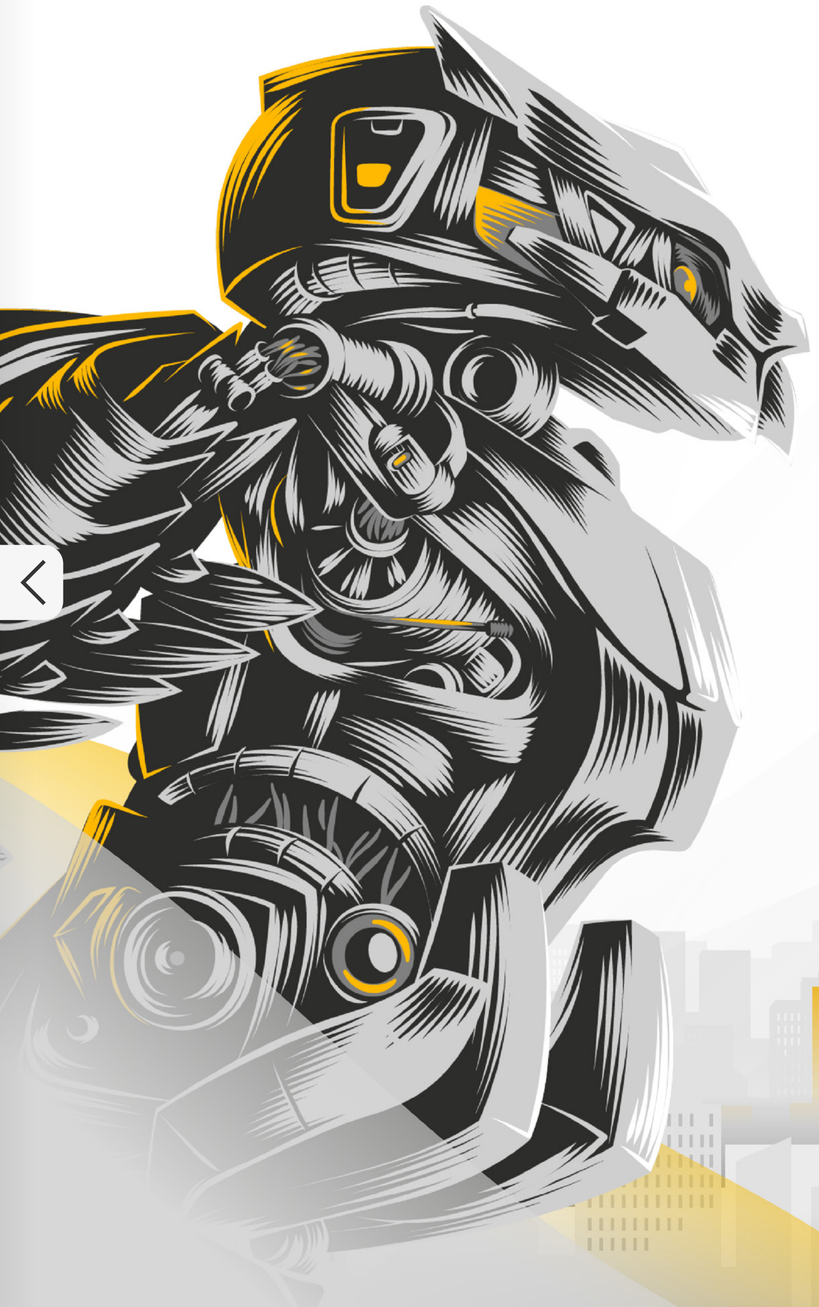
We know that generative AI can augment a team that's short staffed, supplement skills, provide coaching for junior staff members, and even take on some remediation tasks autonomously. But without the additional assistance that automation provides, security analysts are left to put the pieces of an incident together on their own. Their level of expertise is key here, and junior members may miss crucial clues during their investigations.



Help Has Arrived

Security professionals are no stranger to the benefits of artificial intelligence.

To get the latest AI models into your SoC, there can be hurdles to overcome to gain acceptance from sceptical decision makers. First, we need to get over the hype. AI and Machine Learning (ML) have been in the security space for years, much longer than the chatbots and hallucinatory AI images dominating the news. We also need to be able to assure organizations that their AI-discovered threat data is real and accurate.

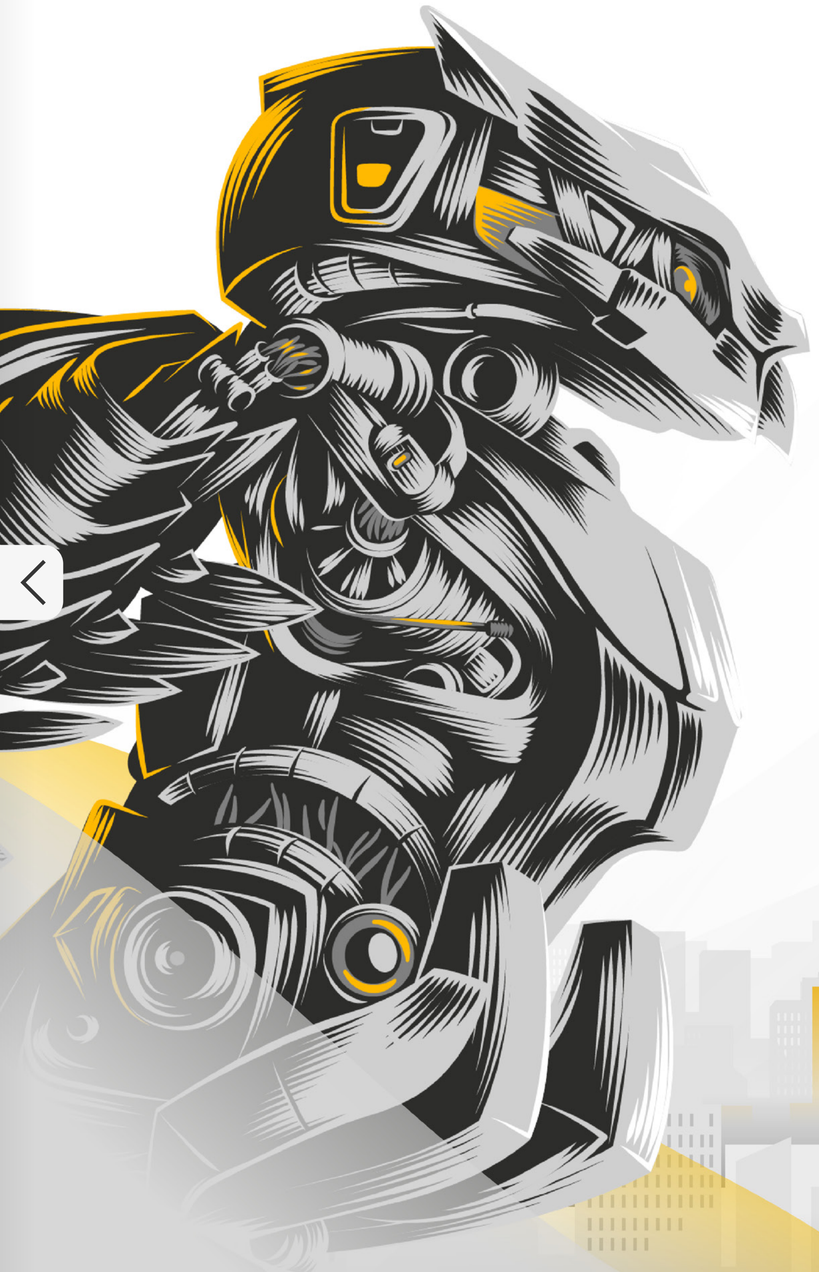


Help Has Arrived

Security professionals are no stranger to the benefits of artificial intelligence.

There's still work to do for AI to gain broader acceptance.

- How will network users react if they believe that AI is monitoring their activity?
- Will they see this as an unwelcome intrusion into their privacy?
- Will malware detection be triggered by activities specific to certain groups?
- Who can vouch for the safety of your AI implementation?



Help Has Arrived

Security professionals are no stranger to the benefits of artificial intelligence.

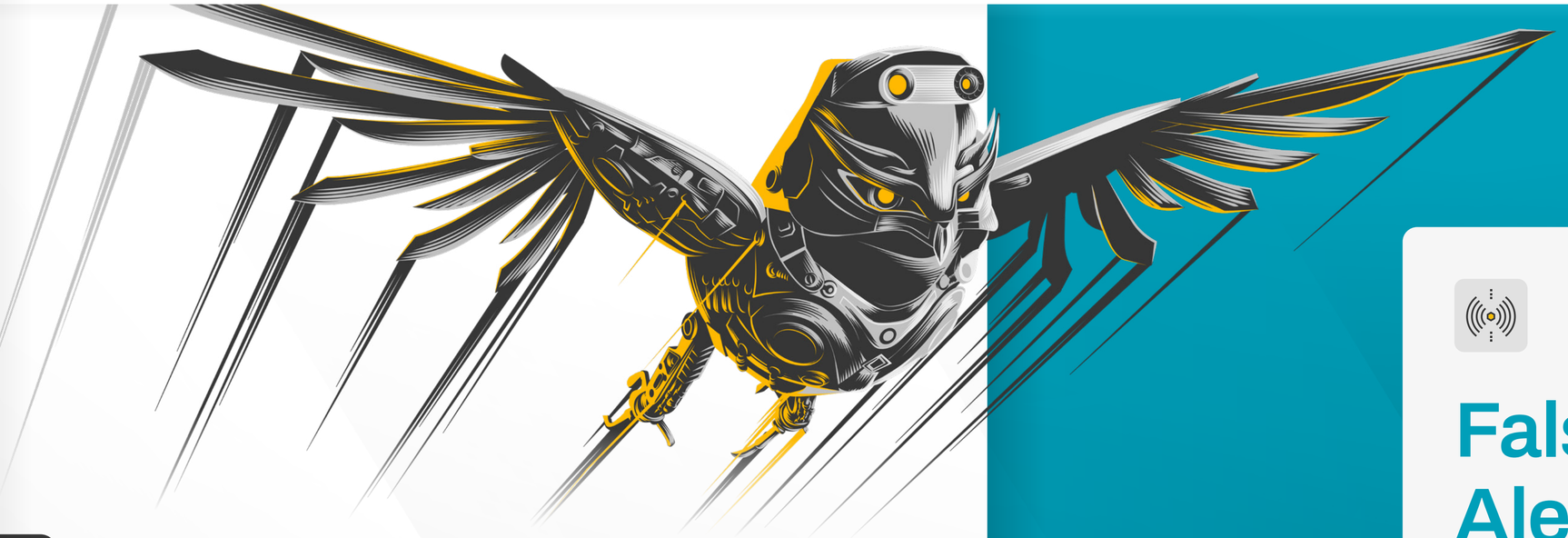
#01 Generative AI

#02 Hurdles

#03 Reaction

#04 Integration

Even after addressing the privacy and ethical concerns, as expressed by 45% of respondents, we're left with the need to fully integrate our existing systems into one effective whole. These are big tasks that require planning and foresight to get right.



Take Charge

Because cybersecurity threats are constantly evolving, security professionals need to take a holistic approach to securing network infrastructure.

To future-proof operations, **Generative AI automation** will be a key component to correctly identify novel as well as persistent threats.

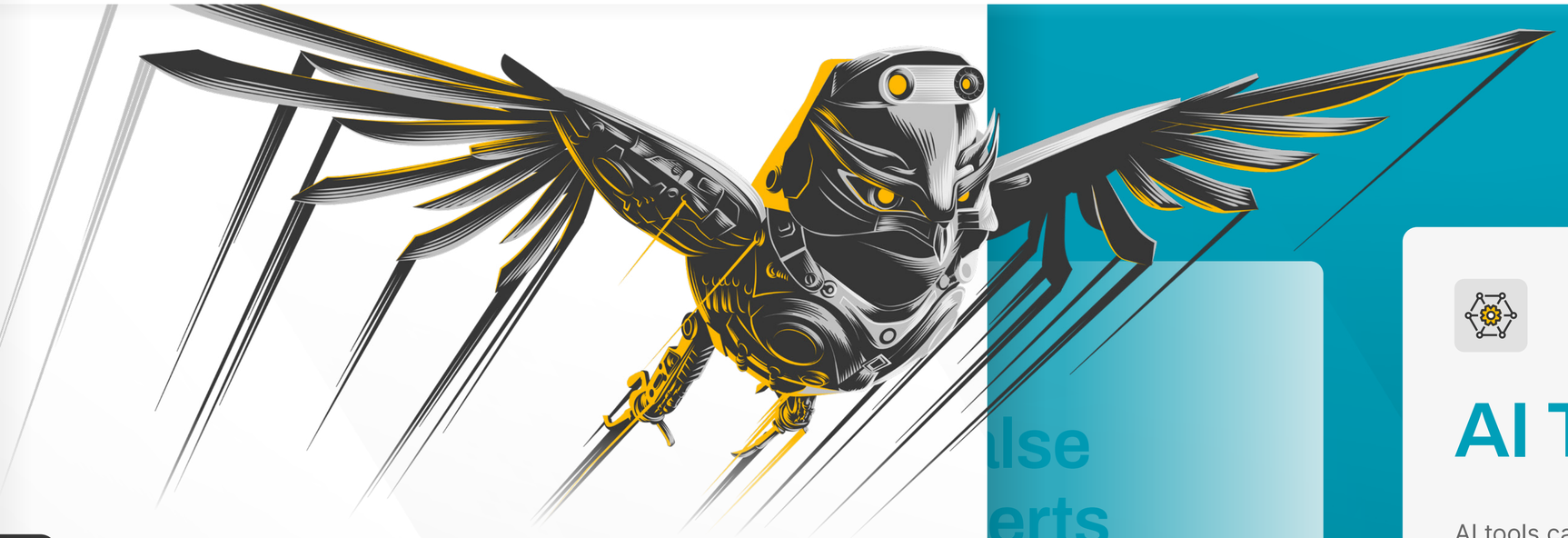
False Alerts

The importance of eliminating frequent false alerts by only surfacing actual, active threats cannot be overstated.

1 / 6

AI Tools

AI tools can handle elim
false alerts by recogni
malicious behavior, and
this information to operators
remediation faster than man
processes to provide real se



Take Charge

Because cybersecurity threats are constantly evolving, security professionals need to take a holistic approach to securing network infrastructure.

To future-proof operations, **Generative AI automation** will be a key component to correctly identify novel as well as persistent threats.

lse
erts

portance of eliminating
nt false alerts by only
ng actual, active threats
be overstated.

AI Tools

AI tools can handle elimination of false alerts by recognizing actual malicious behavior, and bring this information to operators for remediation faster than manual processes to provide real security.

Training

Training on a more com
of threat data, across
time period will allow
AI tools to better recognize
in the future, closing gaps in
network defenses.

2 / 6

Take Charge

Because cybersecurity threats are constantly evolving, security professionals need to take a holistic approach to securing network infrastructure.

To future-proof operations, **Generative AI automation** will be a key component to correctly identify novel as well as persistent threats.

Tools

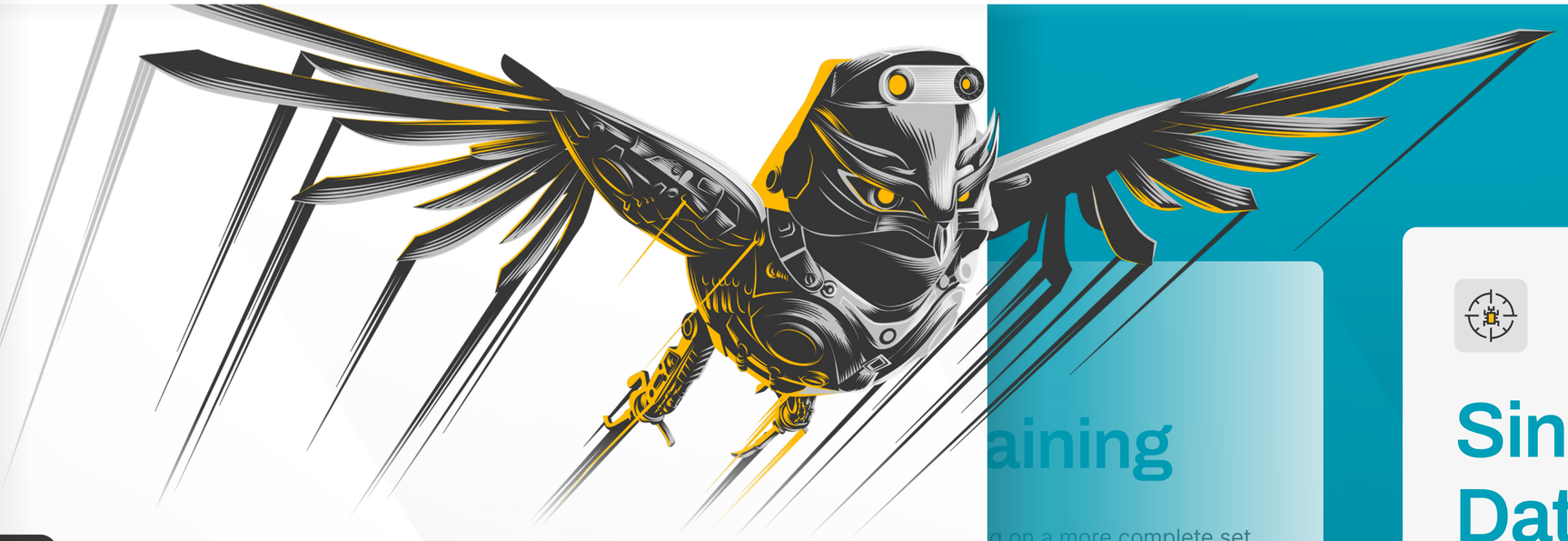
s can handle elimination of
lerts by recognizing actual
us behavior, and bring
ormation to operators for
iation faster than manual
ses to provide real security.

Training

Training on a more complete set of threat data, across a longer time period will allow Generative AI tools to better recognize threats in the future, closing gaps in network defenses.

Single Data Lak

Using AI tools to take in and make sense of structured a unstructured data from a sin data lake can provide holisti identification and also drama improve future security.



Take Charge

Because cybersecurity threats are constantly evolving, security professionals need to take a holistic approach to securing network infrastructure.

To future-proof operations, **Generative AI automation** will be a key component to correctly identify novel as well as persistent threats.

aining

g on a more complete set
at data, across a longer
eriod will allow Generative
s to better recognize threats
uture, closing gaps in
k defenses.

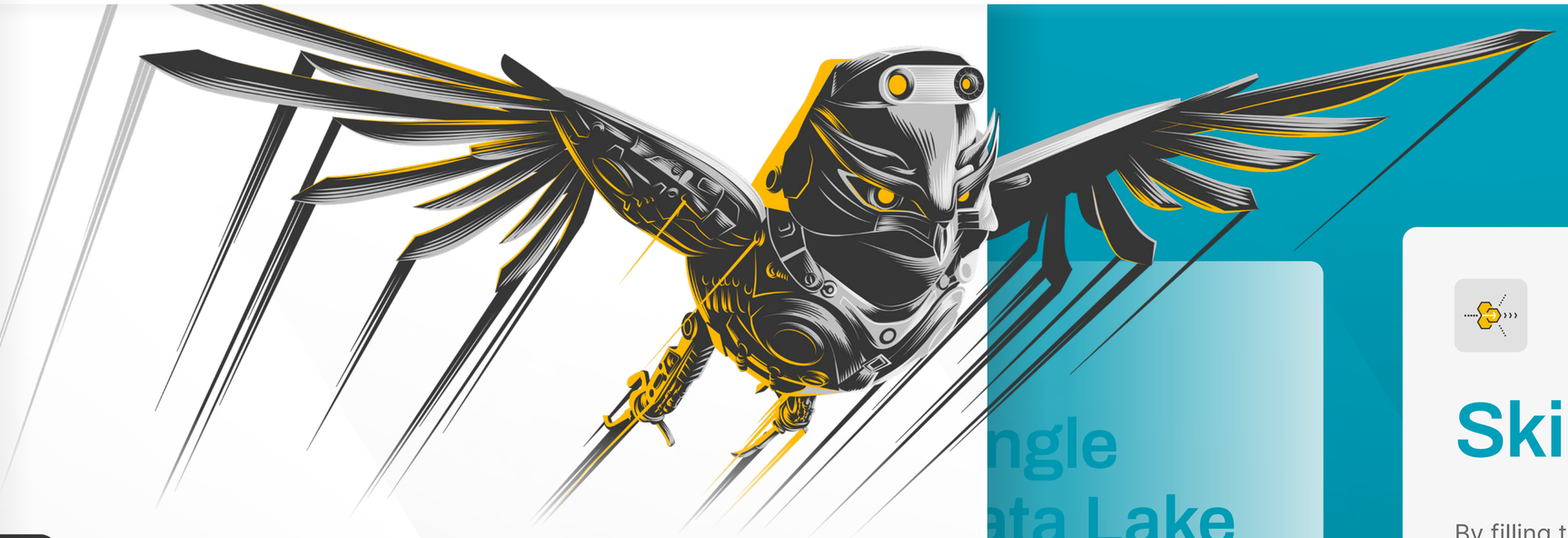
Single Data Lake

Using AI tools to take in and make sense of structured and unstructured data from a single data lake can provide holistic threat identification and also dramatically improve future security.

Skills Ga

By filling the skills gap in th
SoC, AI tools hold the
augmenting skills of the hu
operators to extract new val
from threat data, helping to
blind spots and remove freq
alert triggers.

4 / 6



Take Charge

Because cybersecurity threats are constantly evolving, security professionals need to take a holistic approach to securing network infrastructure.

To future-proof operations, **Generative AI automation** will be a key component to correctly identify novel as well as persistent threats.

ngle ata Lake

AI tools to take in and sense of structured and ctured data from a single ke can provide holistic threat ication and also dramatically e future security.

Skills Gap

By filling the skills gap in the SoC, AI tools hold the promise of augmenting skills of the human operators to extract new value from threat data, helping to identify blind spots and remove frequent alert triggers.

Visibility

Visibility into remediation st helps aid reporting for compliance. So no matter w you are in the world, you ca have the right data available reporting, law enforcement, other compliance needs.

5 / 6

Take Charge

Because cybersecurity threats are constantly evolving, security professionals need to take a holistic approach to securing network infrastructure.

To future-proof operations, **Generative AI automation** will be a key component to correctly identify novel as well as persistent threats.

kills Gap

g the skills gap in the
l tools hold the promise of
nting skills of the human
ors to extract new value
reat data, helping to identify
pots and remove frequent
iggers.

Visibility

Visibility into remediation steps helps aid reporting for regulatory compliance. So no matter where you are in the world, you can have the right data available for reporting, law enforcement, or other compliance needs.

How Cybereason Can Help

MalOp™ Engine

SDR (SIEM Detection and Response)

MDR (Managed Detection and Response)

IR (Incident Response)

Award-winning

Unique to Cybereason is the MalOp™ engine, which provides observability and context through extended use of AI-driven analytics and automation.

MalOp™ gathers threat information into a unified package and helps staff see your entire security picture, regardless of their experience level. This drives more efficient security operations by removing manual steps during triage and investigation.

How Cybereason Can Help

MalOp™ Engine

SDR (SIEM Detection and Response)

MDR (Managed Detection and Response)

IR (Incident Response)

Award-winning

Cybereason's SDR solution (SIEM Detection and Response) has been designed to address issues faced by global security professionals.

Based around the MalOp™ engine, SDR employs an open architecture so that enterprise customers can connect their existing investments and continue to derive value from their legacy tools.

One of the biggest improvements in SDR is reduced MTTR due to its use of a single, consolidated data lake for all security data. This minimizes the need to investigate across distributed data silos and consoles, cutting security data storage and processing costs in half.

How Cybereason Can Help

MalOp™ Engine

SDR (SIEM Detection and Response)

MDR (Managed Detection and Response)

IR (Incident Response)

Award-winning

For organizations requiring a robust response to cyberthreats, but needing a managed solution.

Cybereason's MDR (Managed Detection and Response) offers flexibility without compromising effectiveness by providing malware prevention, detection, and response as a service. Cybereason's own experts will defend your infrastructure against the most sophisticated attacks, so you don't have to. You can focus on other priorities, while Cybereason's team confronts the threat presented by bad actors across any endpoint, anywhere in the world.

How Cybereason Can Help

MalOp™ Engine

SDR (SIEM Detection and Response)

MDR (Managed Detection and Response)

IR (Incident Response)

Award-winning

If your organization is currently facing a cybersecurity incident, Cybereason's (IR) Incident Response is an end-to-end support service from initial detection to full remediation and recovery.

Utilizing industry-leading detection and threat-hunting tools and expertise, Cybereason provides a complete suite of digital forensics and incident response capabilities tailored to address any security threat, from malware intrusions to insider attacks.

How Cybereason Can Help

MalOp™ Engine

SDR (SIEM Detection and Response)

MDR (Managed Detection and Response)

IR (Incident Response)

Award-winning

Cybereason's award-winning technology and services are another step towards future-proofing cybersecurity operations.

They dramatically reduce the cost of centralizing security data and extend detection and response beyond the endpoint. With integrated observability and AI-driven automation, SoC analysts are now empowered to get more done with fewer distractions, freeing them up to focus on other business-critical initiatives.

Learn more at

Cybereason.com