IBM **Security**

Beyond the Hype: AI in your SOC

Ask yourself these 7 questions before adopting an AI security solution

IBM

1

Am I confident in our risk and security balance?

Consider these three items on your punch list:

You're Low on Talent

Tier 1 or front-line analysts are often new to the industry. It takes time for them to truly develop the skills, confidence and maturity in their investigation skills that you need across your SOC. Replace with the content below: According to EMSI, a national labor analytics firm[1], the "US has less than half of the cybersecurity candidates it needs to keep up with ever intensifying demand. For every 100 cybersecurity roles needed, there are a mere 48 qualified candidates, many of whom are already gainfully employed".

Dwell Times Are Too Long — and It's Costing You

Key findings of the Cost of Data Breach Report 2020, include

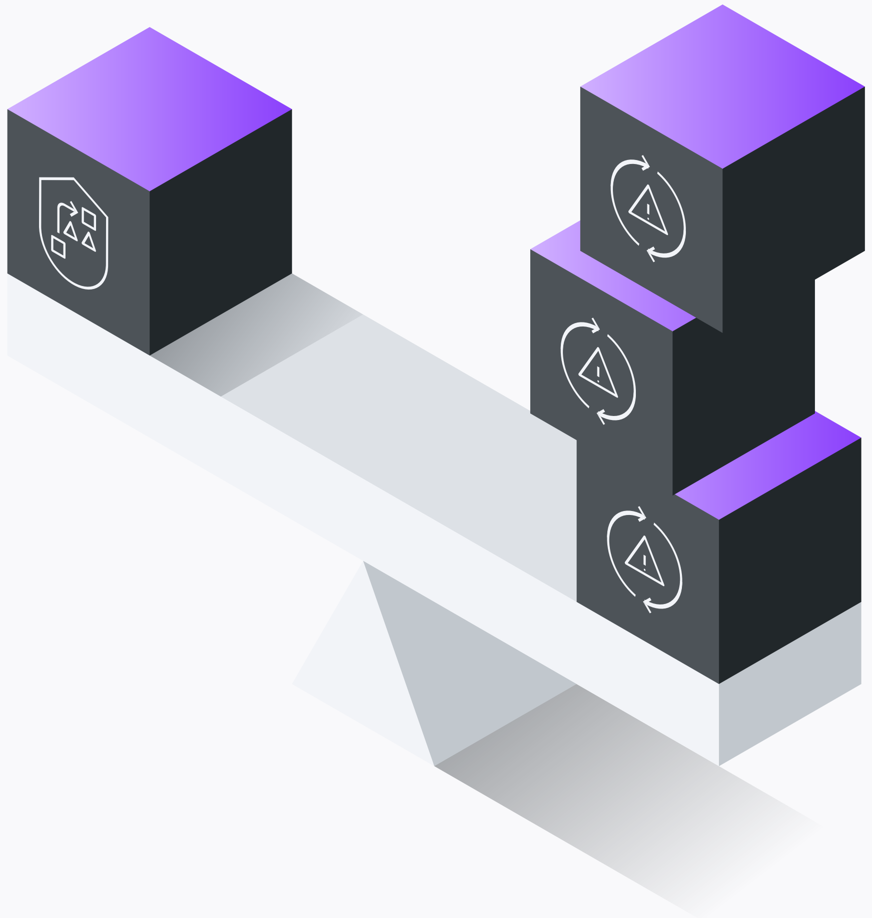
— 280 days – average time to detect and contain a breach

— 315 days - Average time to detect and contain a data breach caused by a malicious attack

— $1.12 million - Average cost savings of containing a breach in less than 200 days vs. more than 200 days

Your Team Has Insights-Overload — and You're Not Helping

Your organization probably has cybersecurity job fatigue (don't worry, you're not alone). It's overwhelmed by repetitive work and there's a breakdown of defined processes. All of this adds up to a higher probability that an important Indicator of Compromise (IoC) has been missed. And when you add new point solutions to address the latest, advanced threats, you're only making things worse: You're creating more data silos, adding integration complexity and increasing the number of insights your analysts must analyze.



A SIEM is necessary for your operation, but what about AI?

What part is hype and what part is real?

CISOs have the toughest jobs in tech: They must allow users access to critical data — but also protect that data from insider threats, credential abuse and human error. It's their job to detect and respond to all threats — while toughest of all — relying upon a team that's overwhelmed and understaffed.

This eBook helps you understand how AI can help optimize your SOC operations while successfully thwarting ever-increasing cyber threats. It augments your security team by automating routine SOC tasks, finding commonalities across investigations and providing actionable feedback to analysts, freeing them up to focus on more important elements of the investigation and increasing efficiency.

[1] Build (Don't Buy): Solving the Cybersecurity Talent Shortage, Emsi (July 2020)

2

How does AI help me get the balance right?

You've heard the AI evangelists, but how can you ensure the AI solution you invest in is an intelligent, AI solution that can make your job easier? The no-hype answer centers around making sure it can learn and can be proactive. It should automate your repeatable tasks to mitigate fatigue and solve what might be your biggest challenge — people.
It's as simple as that.

3

How does AI actually toughen my security stance?

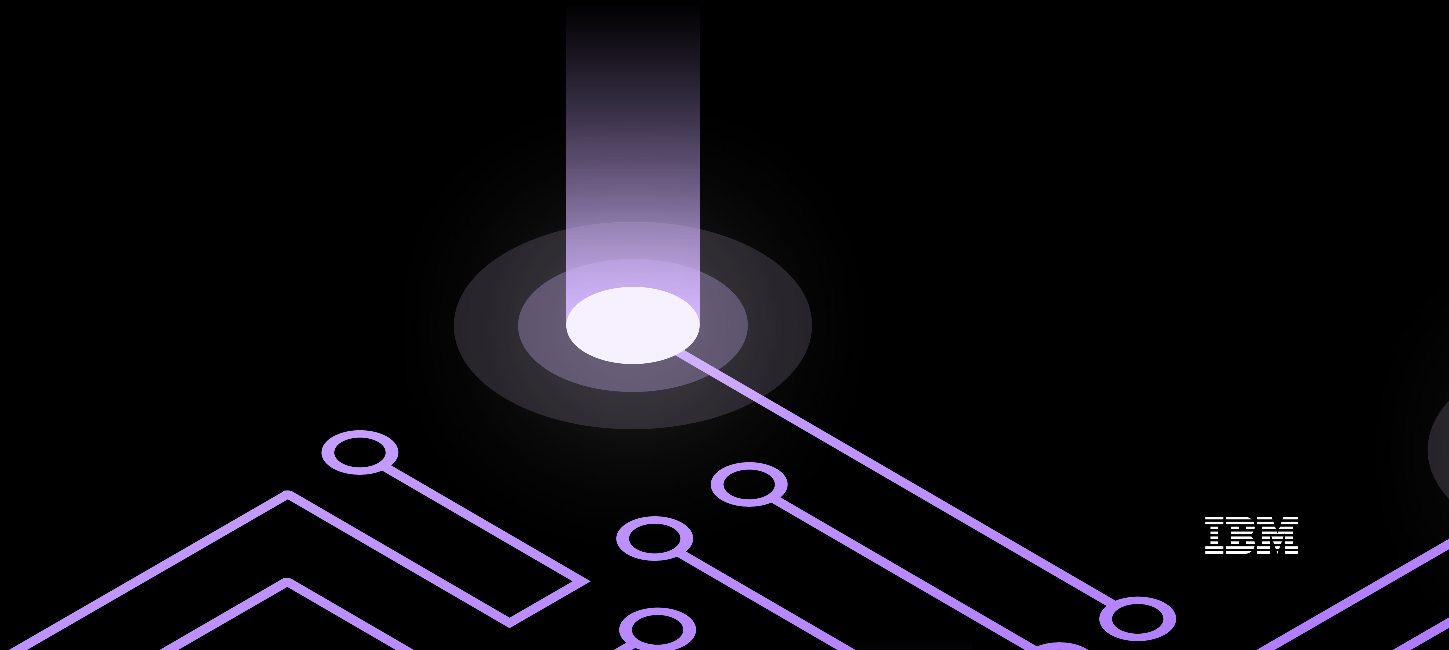
Fact is, it isn't humanly possible for you to keep up with the ever-expanding threat landscape, especially given how busy you are juggling leadership, maintaining your organization's security posture and the day-to-day tasks of running your SOC. You need an arsenal of tools readily available to protect your SOC.

Over the last few years, AI has been hyped and oversold. We get that. But consider this: the right AI applied correctly within your SOC is a highly effective tool that continually learns and updates itself, on its own. It's not a cure-all, but it becomes a vital part of your arsenal of security weapons.

4

Will AI replace my team? Will this solution threaten their livelihood?

AI works with your team, not against it. It handles repeatable tasks and helps you make better-informed decisions. AI proactively combines external data — information from everywhere — and combines it with your native environment to understand what your next move ought to be. In all cases, you decide how much work you want AI to do, from time-intensive tasks to making the routine decisions. In short, AI will always be there, always learning — but you'll set the course and you'll be at the helm.



5

Is this solution AI or machine learning? Do I know the difference?

When people use terms such as “AI” and “machine learning,” they often use them interchangeably. Worse, they also throw around an alphabet soup of abbreviations, such as “ML,” instead of “machine learning,” or they say “artificial intelligence,” instead of “AI.”But don’t let that confuse you: AI (artificial intelligence) and ML (machine learning) aren’t the same, so don’t buy a machine learning solution when you really want AI. Machine learning focuses on the ability of machines to interact with data. It can “learn” and even change an algorithm as it receives more data, but that’s ultimately where it stops since machine learning is a subset of AI.

AI brings the cognitive ability to grow, learn, and carry out tasks based on algorithms. It empowers your SOC by continually becoming more knowledgeable as it gathers information from a near-infinite variety of sources — whether that data is neatly searchable in a database or generated by a machine (structured) or social media or magazine articles (unstructured). AI can learn from data within your company, or externally through blogs, reports, research and security alerts — anywhere and everywhere. It’s all these elements that separate AI from machine learning.

With AI in your SOC, you have access to a repository of institutional memory that can provide recommendations designed specifically for your organization. AI allows you to balance your security operations and solutions — so it’s important to understand if you’re buying a true AI solution.

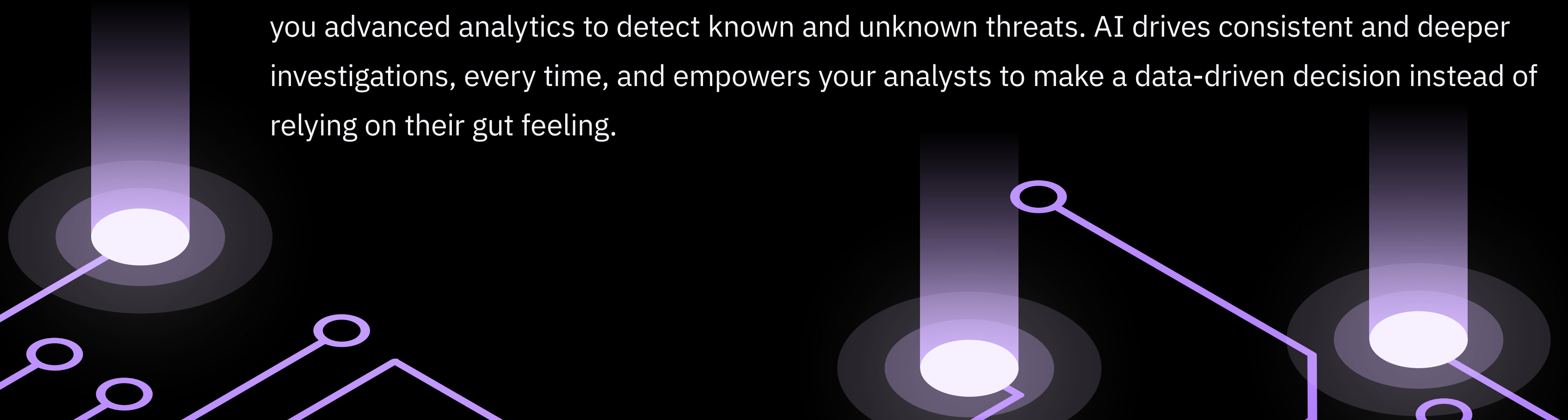
6

What security posture advancements can I expect with AI?

1. **Chain together different potential incidents, automatically.**
AI excels at root-cause analysis automation and integration. AI catches connections for threat and risk insight — and it doesn't get fatigued. AI shows interrelationships your staff might miss due to turnover, inexperience or the passing of time. Without AI, inexperienced analysts may close-out an alert because they thought it was a single instance of an attack. It finds commonalities across incidents using cognitive reasoning and it provides actionable feedback with context — whether the commonalities are from a ticket closed yesterday or months prior. AI gathers external threat intel to help you add more context to your analysis and catches what others may miss.

2. **Solve your people problem.**
AI determines root cause analysis and can orchestrate next steps based on the knowledge it has built on threats and your organization. It doesn't go on vacation. It never leaves you for another job. And you don't have to worry about not recognizing a significant IOC.

3. **Drive consistent and deeper investigations, every time.**
AI can read both unstructured and structured data — more than is humanly possible to read. It learns. It gives you the information you need to reduce Mean Time to Detect and Mean Time to Respond (MTTD and MTTR) — with a quicker, more decisive escalation process. AI can give you advanced analytics to detect known and unknown threats. AI drives consistent and deeper investigations, every time, and empowers your analysts to make a data-driven decision instead of relying on their gut feeling.



4. **Conduct more thorough and consistent investigations in a fraction of the time.**
Leveraging AI to conduct automatic data mining of threat research/intelligence allows security analysts to conduct more thorough, consistent investigations in a fraction of the time and allows analysts to focus on strategic threat investigations and threat hunting. AI correlates threat intelligence to investigations giving analysts a more comprehensive view of the threat.

5. **Focus on the most important alerts first.**
Alert prioritization helps analysts triage alerts effectively by focusing on the most critical alerts first, uncovering false negatives and false positives and greatly reducing the chances of missing critical incidents.

6. **Leverage MITRE ATT&CK for more effective threat investigations**
Mapping the attacker's actions to the MITRE ATT&CK™ framework visually depicts a timeline of events showing the progression of a threat, resulting in faster and more accurate threat investigations, which in turn reduces dwell time.

7. **Gain a comprehensive view of the investigation**
Cross investigation analysis reflects a more comprehensive view of the investigation beyond the current offense by identifying and connecting alerts linked to the same attack that on the surface appear to be unrelated, reducing the number of alerts and duplication of work.

8. **Have a robust and automated incident response (IR) workflow that spans people, process and technology.**
AI guides security analysts through a fast, complete response that's driven by data and evidence. It automates workflow and remediation. It enables SOCs to assess and refine their IR processes, continually.

7

How does AI improve the SOC before, during and after an attack?

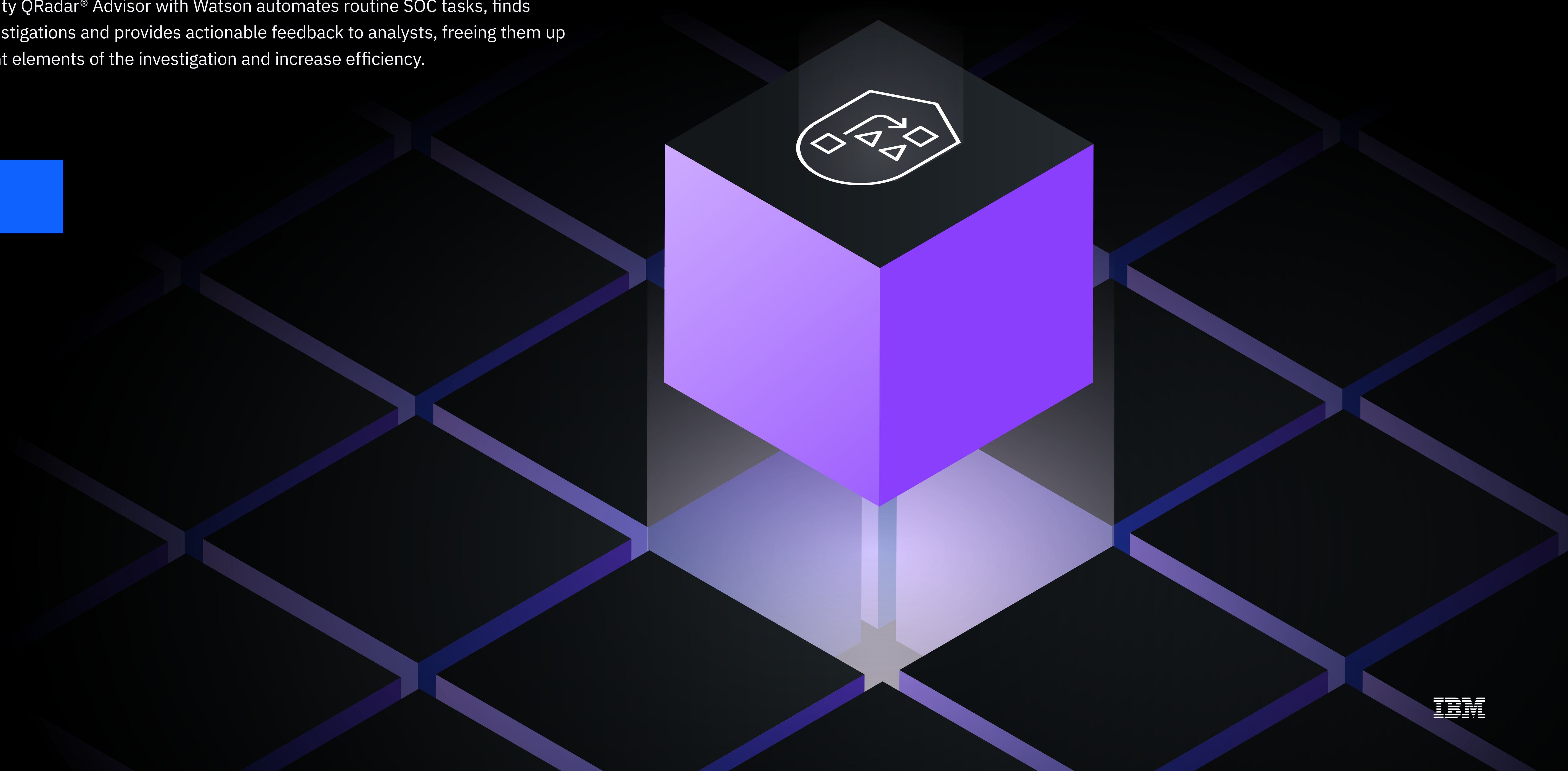
Before, during, and after a data breach, AI enables your SOC to be better prepared and recover faster. The IBM QRadar Security Intelligence Platform takes this technology and integrates it into your SOC to provide an all-encompassing analytics solution — all on a single platform.

Before an attack →	During an attack →	After an attack
QRadar SIEM provides complete visibility and identifies threats and anomalies early in the attack cycle.	**QRadar SIEM** continuously collects ongoing evidence, providing easy access to forensics data. It prioritizes based on business impact.	**QRadar SIEM** continuously tunes detection mechanisms based on lessons learned.
QRadar Advisor with Watson automatically investigates all anomalies and identifies high risk attack behaviors.	**QRadar Advisor with Watson** force-multiplies your team with automated root-cause analysis and helps you understand the full scope of the threat.	**QRadar Advisor** with Watson adapts models to respond with increasing accuracy to future threats.
IBM Security SOAR enables SOCs to prepare robust and automated IR workflows spanning people, process, and technology.	**IBM Security SOAR** guides security analysts through a fast, complete response and automates incident workflow and remediation.	**IBM Security SOAR** enables SOCs to continually assess and refine IR processes.

About IBM Security QRadar Advisor with Watson

With AI, you can optimize your SOC operations while successfully thwarting ever-increasing cyber threats. IBM® Security QRadar® Advisor with Watson automates routine SOC tasks, finds commonalities across investigations and provides actionable feedback to analysts, freeing them up to focus on more important elements of the investigation and increase efficiency.

Learn more



IBM **Security**

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2020

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

00000000USEN

IBM