



---

# Beyond the Hype: AI in your SOC

Ask Yourself These 7 Questions Before Adopting  
a Cybersecurity Cognitive Solution

# 1

## Am I Confident in Our Risk and Security Balance?

*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.*

*Worse, stakes are at an all-time high and excuses won't cut it. Organizations and their customers and clients demand security. Regulators are watching. Cybersecurity insurance rates are spiking. Investors are restive and lawyers are standing by. Everyone from the C-Suite to the rank-and-file require absolute, airtight security — while themselves are also a vector for vulnerability.*

### **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. According to ESG Research, 51 percent of organizations report had a “problematic shortage” of cybersecurity skills in 2018. This is up from 45 percent in 2017. Cybersecurity job fatigue is real, and according to ESG, 38 percent of cybersecurity professionals already say the skills shortage has led to high burnout rates and staff attrition.

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

The average dwell times vary anywhere between 50 and 200 days. Companies that identified a breach in less than 100 days saved more than \$1 million as compared with those that took more than 100 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?***



# 2

## How Does AI Help Me Get the Balance Right?

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.

You've heard the AI evangelists, but how can you ensure the AI solution you invest in is an intelligent, cognitive 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?

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.

# 4

## Will AI Replace My Team? Will This Solution Threaten Their Livelihood?

# 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.





# 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

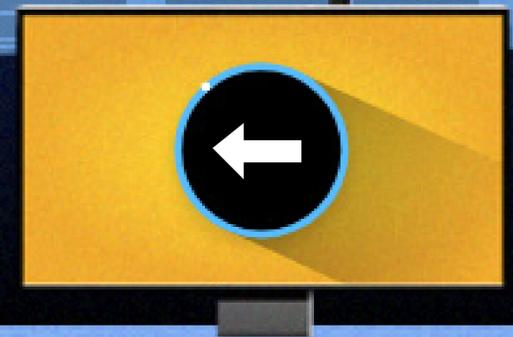
## **Have a Robust and Automated Incident Response (IR) Workflow that Spans People, Process and Technology.**

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

**IBM QRadar SIEM** provides complete visibility and identifies threats and anomalies early in the attack cycle.

**IBM QRadar SIEM** continuously collects ongoing evidence, providing easy access to forensics data. It prioritizes based on business impact.

**IBM QRadar SIEM** continuously tunes detection mechanisms based on lessons learned.

**IBM QRadar Advisor with Watson** automatically investigates all anomalies and identifies high risk attack behaviors.

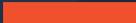
**IBM QRadar Advisor with Watson** force-multiplies your team with automated root-cause analysis and helps you understand the full scope of the threat.

**IBM QRadar Advisor with Watson** adapts models to respond with increasing accuracy to future threats.

**IBM Resilient** enables SOC's to prepare robust and automated IR workflows spanning people, process, and technology.

**IBM Resilient** guides security analysts through a fast, complete response and automates incident workflow and remediation.

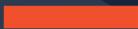
**IBM Resilient** enables SOC's to continually assess and refine IR processes.



# About IBM QRadar Advisor with Watson

With AI, you can optimize your SOC operations while successfully thwarting ever-increasing cyber threats. IBM® 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](#)



# References

[The State of Cyber Security Professional Careers, ESG](#)



IBM Security