IBM QRadar Advisor with Watson

Automate your SOC with AI

Highlights

- Unlock a new partnership between analysts and their technology
- Automate incident analysis and force multiply your team's efforts
- Drive consistent and deeper investigations
- Make quicker and more decisive incident escalations
- Reduce dwell times

Challenges for today's SOC

Whether you have a security team of two or 100, your goals are to ensure the business thrives. And that means protecting critical systems, users, and data, detecting and responding to threats, and staying ahead of cybercrime. But there are a number of serious challenges plaguing today's SOC that may impede your ability to accomplish your goals.

Unaddressed threats

Too much information is overlooked simply because your analysts may not know how the information is connected. It's difficult to uncover actionable insights, and your analysts may then choose to work only on cases that they are confident about, which could lead to missing certain investigations and exposing your organization to risk.

Insights overload

The sheer volume, variety and speed of insights to analyze make it difficult to prioritize work and get to the root cause. This is true for companies of all sizes. No analyst knows where to start piecing together local context that helps them quickly identify the problem at hand. They are overwhelmed by repetitive work, and most experience analyst fatigue, resulting in a breakdown of defined processes and a high probability that an important Indicator of Compromise (IoC) is missed. 93 percent[1] of organizations are unable to triage all relevant threats. Almost one-quarter[2] feel they were lucky to escape with no business impact as a result of not investigating these alerts.

Dwell times are getting worse

One of the most popular metrics security professionals use to measure success in protecting and defending their data is dwell time, primarily the MTTD (mean time to detect) and MTTR (mean time to respond). Dwell time measures the duration of how long a threat actor has undetected access in a network until they're completely removed.

Despite having more solutions and data than ever before, the average dwell time today varies anywhere between 50 and 200 days. Why is this so important? According to the Ponemon Institute, companies that identified a breach in less than 100 days saved more than $1 million as compared to those that took more than 100 days. Similarly, companies that contained a breach in less than 30 days saved over $1 million as compared to those that took more than 30 days to resolve the issue.[3] Lack of consistent, high-quality and context-rich investigations leads to a breakdown of existing processes and high probability of missing crucial insights – exposing your organization to risk.

Lack of cybersecurity talent and job fatigue

Like most security analysts, your team is probably overworked, understaffed and overwhelmed, and it's not their fault. It is humanly impossible to keep up with the everexpanding threat landscape, especially given how busy teams are with the day-to-day security operations tasks required in your SOC.

Your organization is not alone when it comes to experiencing cybersecurity job fatigue. According to ESG Research, 51 percent of organizations report having a "problematic shortage" of cybersecurity skills in 2018. This is up from 45 percent in 2017.[4] Cybersecurity job fatigue is real, and according to ESG, 38 percent of cybersecurity professionals already say that the cybersecurity skills shortage has led to high burnout rates and staff attrition. The situation is only expected to worsen as the mountain of data continues to grow while the skills gap continues to widen, with 1.8 million security jobs excepted to go unfulfilled by 2022.[5] Tier 1 or front-line analysts are often new to the industry and to the workforce. It takes time for them to truly develop the skills, confidence and maturity in their investigation skills.

Rapid adoption of more point solutions

CISOs are adopting more point solutions to stop new, evolving threats. Whatever your use case — protecting critical data, insider threats, identity and access management, credential abuse or something else — you're bound to be inundated with a solution for that. Consequently, integration between solutions, lack of scale, and difficulty of use are becoming serious issues for organizations.

Stakes are at an all-time high

Excuses don't pay the bills, nor do they help regain trust from an upset customer. According to the Ponemon Institute, the average total cost of a data breach rose from $3.62 million to $3.86 million, an increase of 6.4 percent from 2017.[6] Security leaders are also facing increased scrutiny from a variety of sources, including executive leadership, clients, employees, investors, regulators, insurance companies and watchdog groups. With stakes at an all-time high, can your organization afford to not be ready?

Unlock a new partnership between analysts and their technology

Artificial Intelligence bridges this gap and unlocks a new partnership between security analysts and their technology. Each has their strengths such as common sense with humans and bias elimination and tradeoff analytics with AI. But together, as a team, they can better stop threats and reduce dwell times.

Benefits of AI in the SOC

Automate incident analysis and force multiply your team's efforts

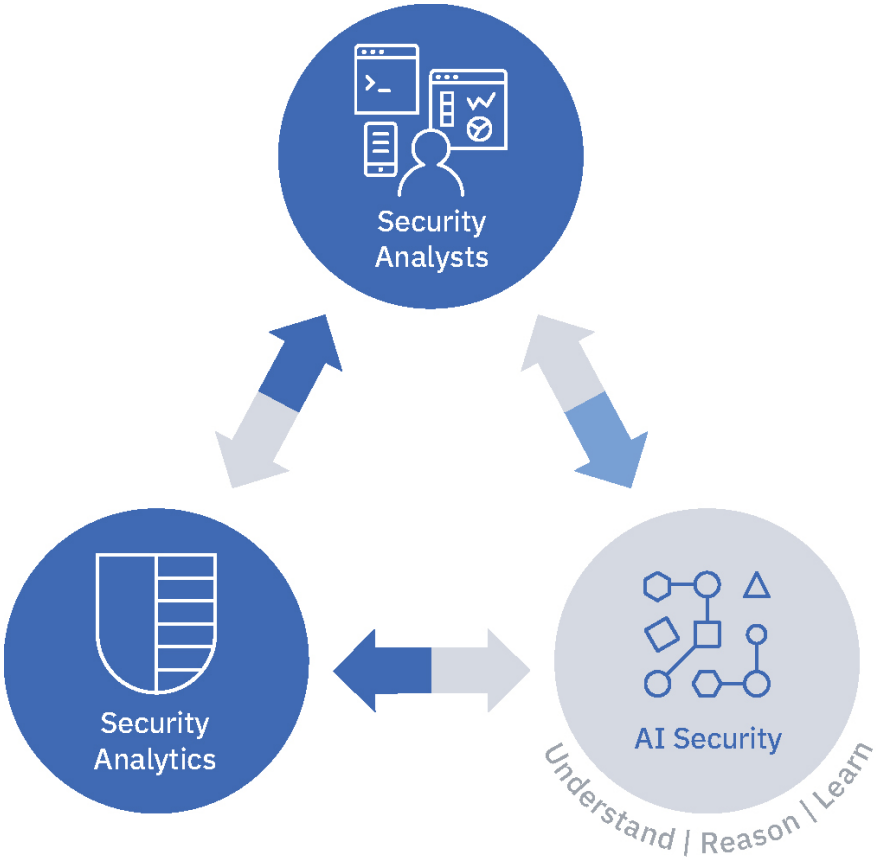
Don't waste human capital on routine analysis. Instead, let AI automate your repetitive SOC tasks, better focus your analysts on more important elements of the investigation, and increase analyst efficiency.

Drive consistent and deeper investigations

Did you know that analysts are only able to keep up with eight percent of the information needed to do their jobs? Upgrade your SOC by letting AI automatically find commonalities across incidents using cognitive reasoning and provide actionable feedback with context. Think of AI as your personal advisor – AI should go out and gather external threat intel to help you add more context to your analysis, and it should chain together different potential incidents that are related so you can save more time. Whether it's 4:30 PM on a Friday or 10:00 PM on a Monday, your analysts should be focused on driving consistent and thorough investigations each and every time.

Reduce dwell times

Reduce MTTD and MTTR with a quicker and more decisive escalation process. Determine root cause analysis and drive next steps with confidence by mapping the attack to your dynamic playbook, such as the MITRE ATT&CK model.



AI unlocks a new partnership between security analysts and their technology.

IBM QRadar Advisor with Watson – Built with AI for the front-line security analyst

IBM QRadar Advisor empowers security analysts to drive consistent investigations and make quicker and more decisive incident escalations, resulting in reduced dwell times and increased analyst efficiency.

Force multiply your team's efforts

- Prioritize a list of investigations with the greatest risk
- Filter and sort through data faster based on criticality
- Act on enhanced IBM Watson feedback using internal and external threat intelligence feeds

Drive consistent and deeper investigations

- Automatically link investigations through connected observables using cross-investigation analytics and extend beyond the current potential incident
- Avoid duplication of effort
- Determine if you need to do additional tuning in the case of multiple duplicate investigations triggered by the same events

Reduce dwell times

- Visualize how the attack has occurred and progressed, a confidence level for each progression, what tactics have occurred, and what tactics can still possibly occur using the MITRE's ATT&CK model
- Take advantage of Easy Incident Scoring to provide your analysts with a quicker and more decisive escalation process
- Increase analyst efficiency and reduce MTTD and MTTR

Don't take our word for it; see the benefits our customers are having with AI. The analysts at Sogeti Luxembourg were able to reduce the investigation time from two to three hours to two to three minutes. That's valuable time that the analysts can better spend on further investigating the real threats and adding richer context to their investigations. Many other customers are using AI to force multiply their team's efforts. And with AI, they are able to use lesser skilled workers to fill the Tier 1 analyst roles – promoting the current Tier 1 analysts to focus on Tier 2 responsibilities and force multiply their teams' efforts.

For more success stories and information about how you can partner with AI, visit ibm.biz/learnAI

[1] McAfee Labs Threat Report. McAfee. 2016. (https://www.mcafee.com/ content/dam/enterprise/en-us/assets/reports/rp-quarterly-threatsdec- 2016.pdf)

[2] McAfee Labs Threat Report. McAfee. 2016. (https://www.mcafee.com/ content/dam/enterprise/en-us/assets/reports/rp-quarterly-threatsdec- 2016.pdf)

[3] Cost of a Data Breach. Ponemon, 2018. (https://www.ibm.com/security/ data-breach)

[4] Cybersecurity Realities and Priorities for 2018 and Beyond. Enterprise Strategy Group. 2018. (https://www.thehaguesecuritydelta.com/media/ com_hsd/report/213/document/ESG-Research-Insights-Paper- Spirent-2018.pdf)

[5] Cybersecurity Realities and Priorities for 2018 and Beyond. Enterprise Strategy Group. 2018. (https://www.thehaguesecuritydelta.com/media/ com_hsd/report/213/document/ESG-Research-Insights-Paper- Spirent-2018.pdf)

[6] Cost of a Data Breach. Ponemon, 2018. (https://www.ibm.com/security/ data-breach)

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and has been granted more than 8,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @ibmsecurity on Twitter or or visit the IBM Security Intelligence blog.

For more information

To learn more about QRadar Advisor with Watson, contact your IBM sales representative or visit: ibm.com/us-en/marketplace/cognitive-security-analytics

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.