IBM Resilient

Orchestrated Response: A Game-Changing Strategy

Introduction

Security Operations Centers (SOCs) are evolving to help cyber security professionals face today's rising challenges. These challenges include complex cyberattacks, a growing number of security tools, and a widening skills gap. Organizations are rapidly adopting advanced security automation and orchestration (SAO) strategies to alleviate these cyber threats.

Orchestration and automation are often used interchangeably in security, yet they serve different purposes – especially in incident response (IR). Orchestration is the broader, process-based strategy. It is the alignment of the people, processes, and technologies used in incident response to determine what needs to be done, by whom, and with which tools. Automation is technology-focused and is used to accelerate tools-based workflows, like threat intelligence lookups.

Once the broader orchestration strategy is understood, organizations are better primed to automate workflows with less risk and greater impact. When orchestration and automation are used together effectively, they complement and support strategic, intelligent response.

> "We can automate and scale parts of IT security...but we can't yet scale incident response. We still need people. Security orchestration represents the union of people, process, and technology. It's computer automation where it works, and human coordination where that's necessary."
>
> **Bruce Schneier**
> **Chief Technology Officer,**
> **IBM Resilient**
> **Special Advisor, IBM Security**

The goal of orchestrated incident response is to support the humans involved in incident response – from intelligence gathering through intelligent action. Process needs to be decided first so that the correct actions are automated to serve the humans in the loop. Automation, then, is an important part of achieving that goal. Many repetitive, tools-to-tools workflows should be automated, such as SIEM queries, threat intelligence lookups, or IT ticket creation. Doing so ensures accuracy, offloads work from over-taxed and under-staffed security teams, and increases response speed. By automating repetitive functions that do not need human oversight or intervention, analysts are empowered to do their jobs better, faster, and smarter.

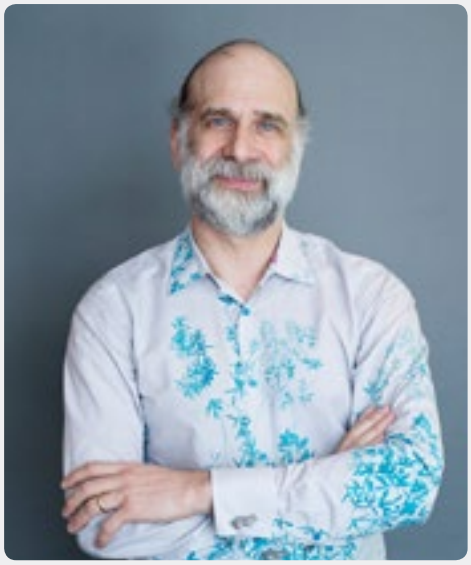
Bruce Schneier, IBM Resilient CTO and Special Advisor to IBM Security, has long talked about the key differences between orchestration and automation. Here is one of Bruce's recent pieces on this topic:

BRUCE'S BLOG

Security Orchestration for an Uncertain World

At the RSA Conference, I saw a lot of companies selling security incident-response automation. Their promise was to replace people with computers — sometimes with the addition of machine learning or other AI techniques — and to respond to attacks at computer speeds. While this is a laudable goal, there's a fundamental problem with doing this in the short term. You can only automate what you're certain about, and there is still an enormous amount of uncertainty in cybersecurity. Automation has its place in incident response, but the focus needs to be on making the people effective, not on replacing them. Orchestration, not automation.

This isn't just a choice of words; it's a difference in philosophy. The US military went through this in the 1990s. What was called the Revolution in Military Affairs — RMA for short — was supposed to change how warfare was fought. Satellites, drones, and battlefield sensors were supposed to give commanders unprecedented information about what was going on, while networked soldiers and weaponry would enable troops to coordinate to a degree never before possible. In short, the traditional fog of war would be replaced by perfect information, providing certainty instead of uncertainty. They, too, believed certainty would fuel automation, and in many circumstances allow technology to replace people.



Bruce Schneier
Chief Technology Officer, IBM Resilient
Special Advisor, IBM Security

Of course, it didn't work out that way. The US learned in Afghanistan and Iraq that there are a lot of holes in both our collection and coordination systems. Drones have their place, but they can't replace ground troops. The advances from the RMA brought with them some enormous advantages, especially against militaries that didn't have access to the same technologies, but never resulted in certainty. Uncertainty still rules the battlefield, and soldiers on the ground are still the only effective way to control a region of territory.

But along the way, we learned a lot about how the feeling of certainty affects military thinking. Last month, I attended a lecture on the topic by H.R. McMaster. This was before he became President Trump's National Security Advisor-designate; then he was the director of the Army Capabilities Integration Center. His lecture touched on many topics, but at one point he talked about the failure of the RMA. He confirmed that military strategists mistakenly believed that data would give them certainty. But he took this change in thinking further, outlining the ways this belief in certainty had repercussions in the way military strategists thought about modern conflict.

His observations are directly relevant to Internet security incident response. We too have been led to believe that data will give us certainty, and are making the same mistakes that the military did in the 1990s.

In a world of uncertainty, there's a premium on understanding; commanders need to figure out what's going on. In a world of certainty, knowing what's going on becomes a simple matter of data collection.

I see this same fallacy in Internet security. Many companies exhibiting at the RSA Conference promise that they'll collect and display more data, and that the data will reveal everything. This simply isn't true. Data does not equal information, and information does not equal understanding. We need data, but we also must prioritize understanding the data we have over collecting ever more data. Much like the problems with bulk surveillance, "collect it all" provides minimal value over collecting the specific data that's useful.

In a world of uncertainty, the focus is on execution. In a world of certainty, the focus is on planning. I see this playing out in Internet security as well. My own Resilient Systems — now part of IBM Security — allows incident response teams to manage security incidents and intrusions. While the tool is useful for planning and testing, its real focus is always on execution.

Uncertainty demands initiative, while certainty demands synchronization. Here again we are heading too far down the wrong path. The purpose of all incident-response tools should be to make the human responders more effective. They need both the ability and the capability to exercise it effectively.

When things are uncertain, you want your systems to be decentralized. When things are certain, centralization is more important. Good incident-response teams know this; decentralization goes hand in hand with initiative. And finally, a world of uncertainty prioritizes command, while a world of certainty prioritizes control. Again, effective incident-response teams know this — and effective managers aren't scared to release and delegate control.

Like the US military, we in the incident response field have shifted too much into the world of certainty. We have prioritized data collection, pre-planning, synchronization, centralization, and control. You can see it in the way people talk about the future of Internet security, and you can see it in the products and services offered on the show floor of the RSA Conference.

Automation is too fixed. Incident response needs to be dynamic and agile, because 1) you are never certain, and 2) there is an adaptive malicious adversary on the other end. You need a response system that has human controls and can modify itself on the fly. Automation just doesn't allow a system to do that to the extent that's needed in today's environment. Just as the military has shifted from trying to replace the soldier to making the best soldier possible, we need to do the same.

For some time, I have been talking about incident response in terms of OODA loops. This is a way of thinking about real-time adversarial relationships, originally developed for airplane dogfights but much more broadly applicable. OODA stands for observe-orient-decide-act, and it's what people responding to a cybersecurity incident do constantly, over and over again. We need tools that augment each of those four steps. These tools need to operate in a world of uncertainty, where there is never enough data to know everything that is going on. We need to prioritize understanding, execution, initiative, decentralization, and command.

At the same time, we're going to have to make all of this scale. If anything, the most seductive promise of a world of certainty and automation is that it allows defense to scale. The problem is that we're not there yet. We can automate and scale parts of IT security — antivirus, automatic patching, firewall management — but we can't yet scale incident response. We still need people. And we need to understand what can be automated and what can't be.

The word I prefer is orchestration. Security orchestration represents the union of people, process, and technology. It's computer automation where it works, and human coordination where that's necessary. It's networked systems giving people understanding and capabilities for execution. It's making those on the front lines of incident response the most effective they can be, instead of trying to replace them. It's the best approach we have for cyberdefense.

Automation has its place. If you think about the product categories where it has worked, they're all areas where we have pretty strong certainty. Automation works in antivirus, firewalls, patch management, and authentication systems. None of them is perfect, but all of those systems are right almost all of the time — and we've developed ancillary systems to deal with it when they're wrong. Automation fails in incident response because there's too much uncertainty. Actions can be automated once the people understand what's going on, but people are still required. For example, IBM's Watson for Cybersecurity provides insights for incident-response teams based on its ability to ingest and find patterns in an enormous amount of free-form data; it does not attempt a level of understanding necessary to take people out of the equation.

From within an orchestration model, automation can be incredibly powerful. But it's the human-centric orchestration model that makes automation work: the dashboards, the reports, the collaboration. Otherwise, you're blindly trusting the machine. And when an uncertain process is automated, the results can be dangerous.

Technology continues to advance, and this is all a changing target. Eventually computers will become intelligent enough to replace people at real-time incident response. My guess, though, is that computers are not going to get there by collecting enough data to be certain. More likely, they'll develop the ability to exhibit understanding and be able to operate in a world of uncertainty. That's a much harder goal. Yes, today it's science fiction — but it's not stupid science fiction, and might happen in the lifetimes of our children. Until then, we need people in the loop. Orchestration is a way to achieve that.

Achieving Cyber Resilience with Orchestration and Automation

The emergence of incident response orchestration is a game-changing development in cyber security. An orchestrated security environment puts your people in control, supported by automation. It aligns them with the processes and tools they need to understand attacks, make decisions, and act quickly. In today's security landscape, that's essential.

How IBM Resilient Can Help

The IBM Resilient Incident Response Platform (IRP) is the only advanced, battle-tested platform for complete incident response orchestration and automation. Today, more than 200 SOCs and fusion centers rely on Resilient to form their IR hub – the center of their SOC.

Resilient orchestrates people, process, and technology for incident response:

- Resilient enables cross-organization collaboration between the SOC, HR, IT ops, executives, and other business units.
- Resilient provides Dynamic Playbooks that are built on NIST/CERT/SANS standards – yet are easy to customize with organizational standard operating procedures and update automatically as incident information is uncovered.
- Resilient's open and agnostic platform integrates with your security infrastructure, enabling key automations throughout your entire security stack.

ABOUT IBM RESILIENT

IBM Resilient's mission is to help organizations thrive in the face of any cyberattack or business crisis. The industry's leading Incident Response Platform (IRP) empowers security teams to analyze, respond to, and mitigate incidents faster, more intelligently, and more efficiently. The Resilient IRP is the industry's only complete IR orchestration and automation platform, enabling teams to integrate and align people, processes, and technologies into a single incident response hub. With Resilient, security teams can have best-in-class response capabilities. IBM Resilient has more than 150 global customers, including 50 of the Fortune 500, and hundreds of partners globally.