CitiusTech

Shaping Healthcare Possibilities

The self-driving SOC as Cybersecurity's next frontier

From automation to AI-driven autonomy

Vipin Varma
SVP, CitiusTech

Pawan Jaiswal
AVP, CitiusTech

The urgency of evolution

Security Operations Centers (SOCs) are the beating heart of enterprise cybersecurity. Their nimbleness in tackling cyber threats allows business to be carried on normally. However, seen in the light of the greater diversity of relentless cyber challenges that enterprises face today, SOCs seem stuck in a bygone era.

To draw upon an analogy, they remind us of the era of the horse-drawn carriage. The advent of the automobile changed the face of the transport sector. Speed and efficiency became its defining features. Then came the leap to a driverless automobile. This quantum leap replaced drivers with complex AI and machine learning algorithms to redefine how we get from point A to point B.

Traditional SOCs operating primarily with a human-in-charge approach are increasingly failing against the velocity and sophistication of today's cyberattacks.[1] Automation at the SOCs provided an edge with speed and efficiency: a good first step in evolution (the automobile). However, such gains were incremental, and automation was applied in silos for enrichment or orchestration. Being rule-based, they could not dynamically adjust to the sophistication of modern attacks. A quantum jump to a fully autonomous SOC (self-driving automobile) is what today's businesses need. One, where security analysts "steering" every alert and incident is augmented by AI algorithms that analyze and take split-second decisions to steer organizations clear of oncoming threats, with humans still retaining overall control.

The three phases of SOC transformation

Automation
The first leap

Phase 1

SOCs were first automated via Security Information and Event Management (SIEM) platforms. Analyzing large amounts of data from different sources (like firewalls and servers), a SIEM platform could spot suspicious activities. Think of strange login attempts or malware, these were identified and reported for further probing by the security staff.

As a logical follow-on came the Security Orchestration, Automation, and Response (SOAR) platforms. They feed on data from the SIEMs and run automatic investigations by looking up IP addresses. After checking for known threats, they decide if an alert is real or a false alarm. They can go a step further to follow automated instructions like blocking a suspicious IP or isolating a computer.

SIEM and SOAR platforms provided efficiency gains and reduced analyst fatigue but remained rule-based. The rules-based approach of these platforms meant that unpredictable threats that fell outside predefined scenarios could still gatecrash through the cyber-defenses.

Augmentation
Intelligence meets expertise

Phase 2

AI and machine learning entered the SOC as a way of augmenting human decisions. Detecting anomalies, prioritizing threats, and allowing data-driven advanced threat hunting were a few areas that got an AI boost. AI provided recommendations and context, but human analysts made the final decisions. It was the age of "human-in-the-loop".

Autonomy
The self-driving SOC

Phase 3

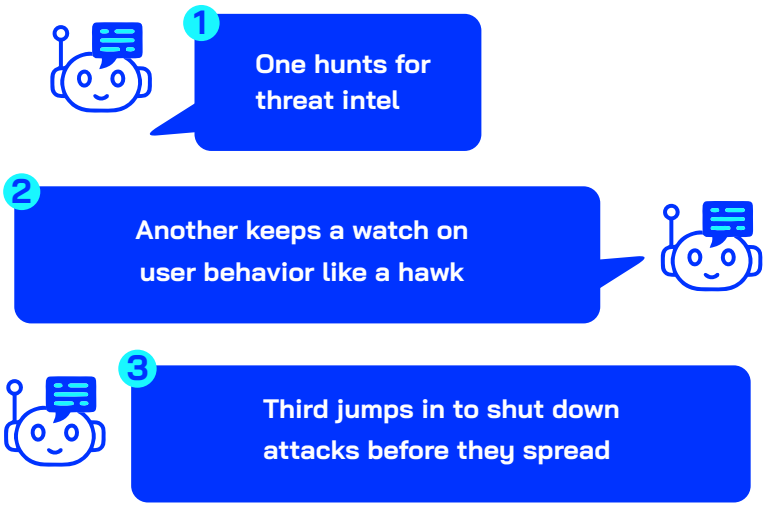
In a huge leap forward, multi-agent AI systems today can unleash the power of autonomy. These specialized agents collaborate with one another to detect, analyze, and respond to threats in real time, with minimal human intervention. Reinforcement learning[2] (that allow these AI agents to learn the most optimal defense strategies and adapt on the fly to dynamically changing threats) and self-healing (which allows the system to repair and restore itself after attacks) form the crux of these systems. With great responsibility thrust on autonomous SOC, explainable AI[3] to help humans audit the 'smart decisions' will bring transparency and trust.

Humans move from being the operator to the governor. Higher value-added tasks like strategizing, providing oversight, and focusing on complex, ambiguous edge cases fall into the ambit of humans.

Multi-agent AI

The engine of autonomy

In autonomous SOCs, you've got different AI agents playing distinct roles:



If you think that they work in a boring, step-by-step assembly line fashion, then you are mistaken. They talk to each other, adapt on the fly, and make decisions in real time. It's not just smart - it's lightning fast.

Such operations require key foundational structures like a unified data fabric that stitches together data from multiple sources, transparent AI models that allow closer human inspection of decisions, and red teaming and simulation for improved resiliency. Cutting-edge computing infrastructure for split-second decisions, too, will be key.

Key benefits

SOC operations can gain on more than a few dimensions in addition to autonomy.

Speed and scale:
Autonomous systems can stop threats in their tracks in minutes rather than hours. Automated containment prevents lateral spread while humans validate the response.

Proactive defense:
These systems go a step beyond reacting. They can identify the early indicators of compromise and prevent spread before damage occurs.

Operational efficiency:
With autonomous SOCs, analysts spend less time chasing false positives due to greater intelligent filtering of 'alert noise'.

Inherent challenges

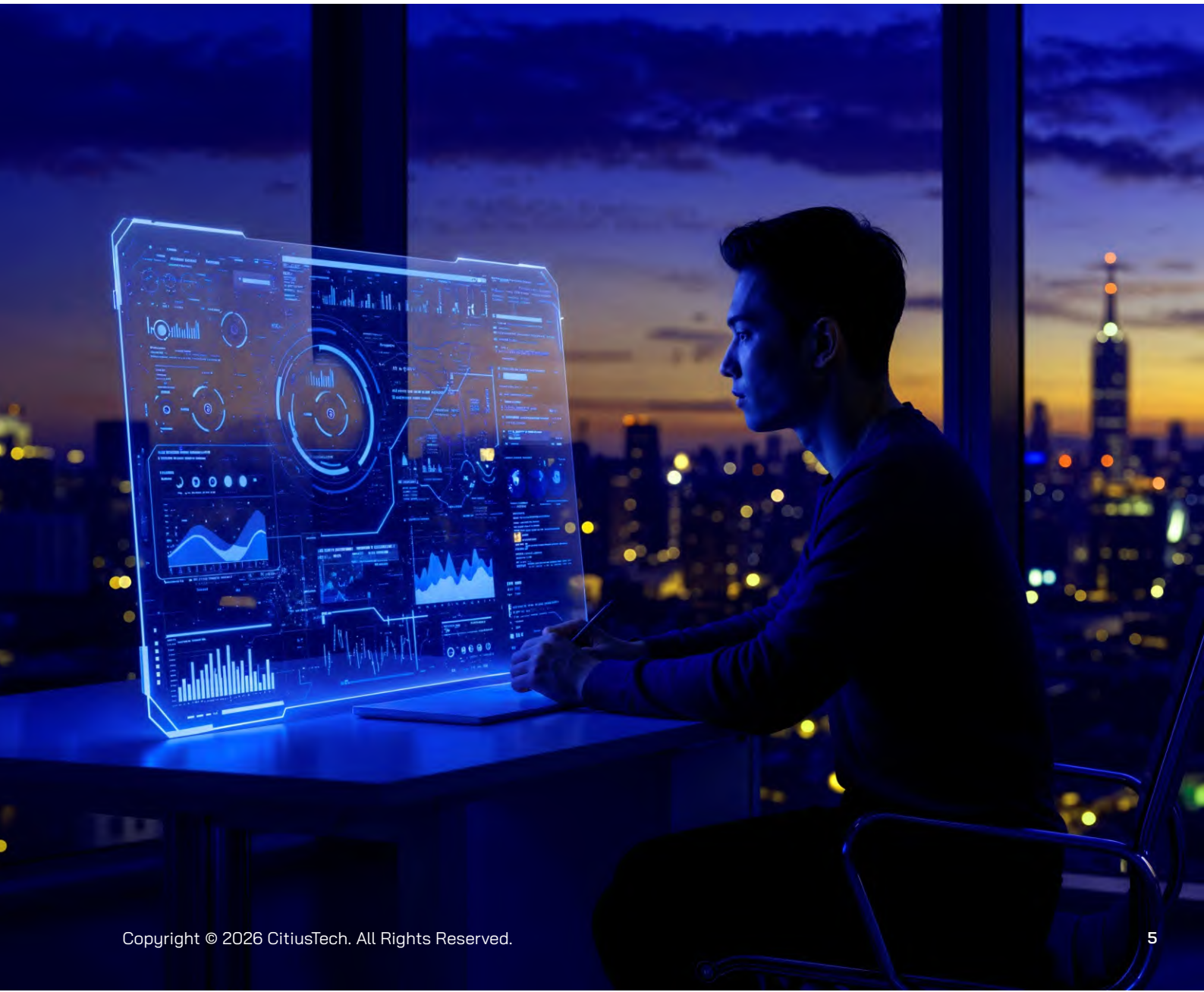
There are, however, some problems with autonomy.

Trust and explainability:
Analysts need to know how AI makes decisions and check them. Building trust and accountability depends on explainable AI (XAI).

Ethical and regulatory hurdles:
Allowing AI to act independently raises concerns about unintended consequences. What happens if an AI shuts down a business-critical system in the name of security? Who is to set the limits? Clear policies and safeguards become essential.

The evolving skill set:
SOC professionals must upskill from their roles as 'tactical responders' to 'AI system managers and architects'.

Autonomy is not a magic bullet. Rather, it opens up doors to possibilities that must be approached with balance and responsibility.



Case study:

The healthcare imperative

A major healthcare Provider recently began down the path of obtaining SOC independence. The problems were formidable: securing extremely sensitive patient data, remaining HIPAA compliant, and minimizing disruption of essential patient care.

With SOC operations being manual and broken up, false positives were eating up time, and the organization was quickly falling behind.

Within months, the Provider was able to deliver tangible results using multi-agent AI technology.

- Visibility **improved 98%**, achieving consistent visibility from endpoints to networks to cloud deployments.
- Alert noise was **cut by 90%**, so analysts were now able to concentrate on real, high-risk threats.
- And significantly, **Mean Time to Respond (MTTR) plummeted**, closing the gap for threat actors who were looking to do damage.

The human-centric future

The journey from automation to autonomy is not that of people being substituted by robots, but rather a tale of people being able to access machine speed, accuracy, and scale to extend human intelligence as never before. The most secure companies of tomorrow won't be the ones who have the biggest SOC team; they will be the companies with the smartest and most autonomous defenses, constructed with humans in the cockpit, in a smart way.

References

1. Alert fatigue in security operations centres: research challenges and opportunities (acm.org)
2. Deep reinforcement learning for adaptive cyber defense in network security (acm.org)
3. What is explainable AI (XAI)? (paloaltonetworks.com)

CitiusTech

About CitiusTech

CitiusTech is a global technology services, consulting, and business solutions enterprise 100% focused on the healthcare and life sciences industry. We enable 140+ enterprises to build a human-first ecosystem that is efficient, effective, and equitable. Leveraging deep domain expertise and next-generation technologies, including AI, Cloud, Data, and Intelligent Automation, we assist our clients to realize their vision, accelerate transformation, and achieve business outcomes. With 7,700+ healthcare technology professionals worldwide, CitiusTech powers digital innovation, business transformation, and industry-wide convergence through next-generation technologies, solutions, and products. Follow CitiusTech on Twitter or LinkedIn.

Shaping Healthcare Possibilities