AI and SOC: the importance of human factor

AI in the SOC: a powerful ally, not a replacement

In recent years, artificial intelligence has transformed the way Security Operation Centers operate.

The introduction of machine learning algorithms into day-to-day security activities makes it possible to analyze massive volumes of logs per second, detect anomalies more accurately, and provide valuable insights into security events.

Yet, in the increasingly heated debate of "AI vs. humans," a fundamental truth risks being overlooked: automation and artificial intelligence have not eliminated the human factor in security operations—on the contrary, they have made it even more strategic.

How to leverage AI effectively: the winning combination with specialized engineers

AI in the SOC performs best when it has a clear objective and structured data.

It excels at event aggregation, noise reduction, automated alert triage, and correlating indicators across multiple systems.

In this respect, it surpasses any human in terms of speed and scalability.

However, AI operates based on what it knows. Its models are trained on known threats, historical patterns, and cataloged activities.

When an attacker adopts new tactics, creatively bypasses controls, or exploits a zero-day vulnerability in a specific context, the algorithm often lacks the references needed to recognize the threat.

This is where the specialized engineer comes into play. Rather than acting as a manual operator processing alerts one by one, they function as an analytical mind, interpreting context, assessing the plausibility of anomalies, forming hypotheses about potential developments, and guiding incident response with an understanding that goes far beyond raw data.

Here are a few examples of how the human factor makes a difference in interpreting and deciding on security actions:

Proactive threat hunting

AI flags anomalies; the engineer builds hypotheses and actively searches for previously unknown threats before they materialize.

Alert contextualization

A false positive can disrupt critical operations; only a human perspective understands the business context needed to decide appropriately.

Continuous model tuning

AI models degrade over time; security engineers continuously fine-tune them to maintain high detection quality.

Real-time response

During critical phases of an incident, the analyst's speed of decision-making and experience make the difference between containment and disaster.

Why a team of people remains a key differentiator

Many organizations evaluating a SOC ask: "Isn't an automated platform enough?"

The short answer is no. The more complete answer requires understanding what truly happens in critical situations.

The most sophisticated cyberattacks—the ones that pose real threats to structured organizations—do not behave in algorithmically predictable ways.

They move slowly, mimic legitimate behavior, and exploit moments of low attention. Their lateral movements within a network can last weeks before leaving traces detectable by automated rules.

A team of experienced engineers brings something no machine learning model can replicate: judgment.

The ability to say, "This technical pattern is correct, but it doesn't make sense in this company's context," or to intuit, from three separate weak signals, that something is happening which requires immediate attention.

There is also a relational dimension that should not be underestimated.

A team that understands the client's infrastructure, business logic, and operational peaks can interpret events with a level of precision that is impossible for a system observing everything in an anonymous and standardized way.

This knowledge is built over time through hands-on experience and continuous dialogue.

SG-SOC Service: a team of specialists for immediate support and assistance

CyberTrust 365's SOC service is powered by a team of specialized engineers providing 24/7 monitoring and dedicated support in Italian, from onboarding through full service implementation.

Operations leverage the SIEM & SOAR capabilities of the proprietary SGBox platform, enabling a centralized, real-time view of the IT infrastructure's security status and the activation of automated, timely threat response processes.

The integration of advanced monitoring and analysis technologies with human expertise is what sets our service apart.

Our goal is to build a relationship of trust and continuous interaction with our clients, supporting them in their daily cybersecurity challenges.

Learn more about the SG-SOC service >>