LMNTRIX
BE THE HUNTER | NOT THE PREY

Why SOCs Fail

A SOC is related to the people, processes and technologies that provide situational awareness through the detection, containment, and remediation of IT threats. A SOC will handle, on behalf of an institution or company, any threatening IT incident, and will ensure that it is properly identified, analyzed, communicated, investigated and reported. The SOC also monitors applications to identify a possible cyber-attack or intrusion (event), and determines if it is a genuine malicious threat (incident), and if it could affect business.

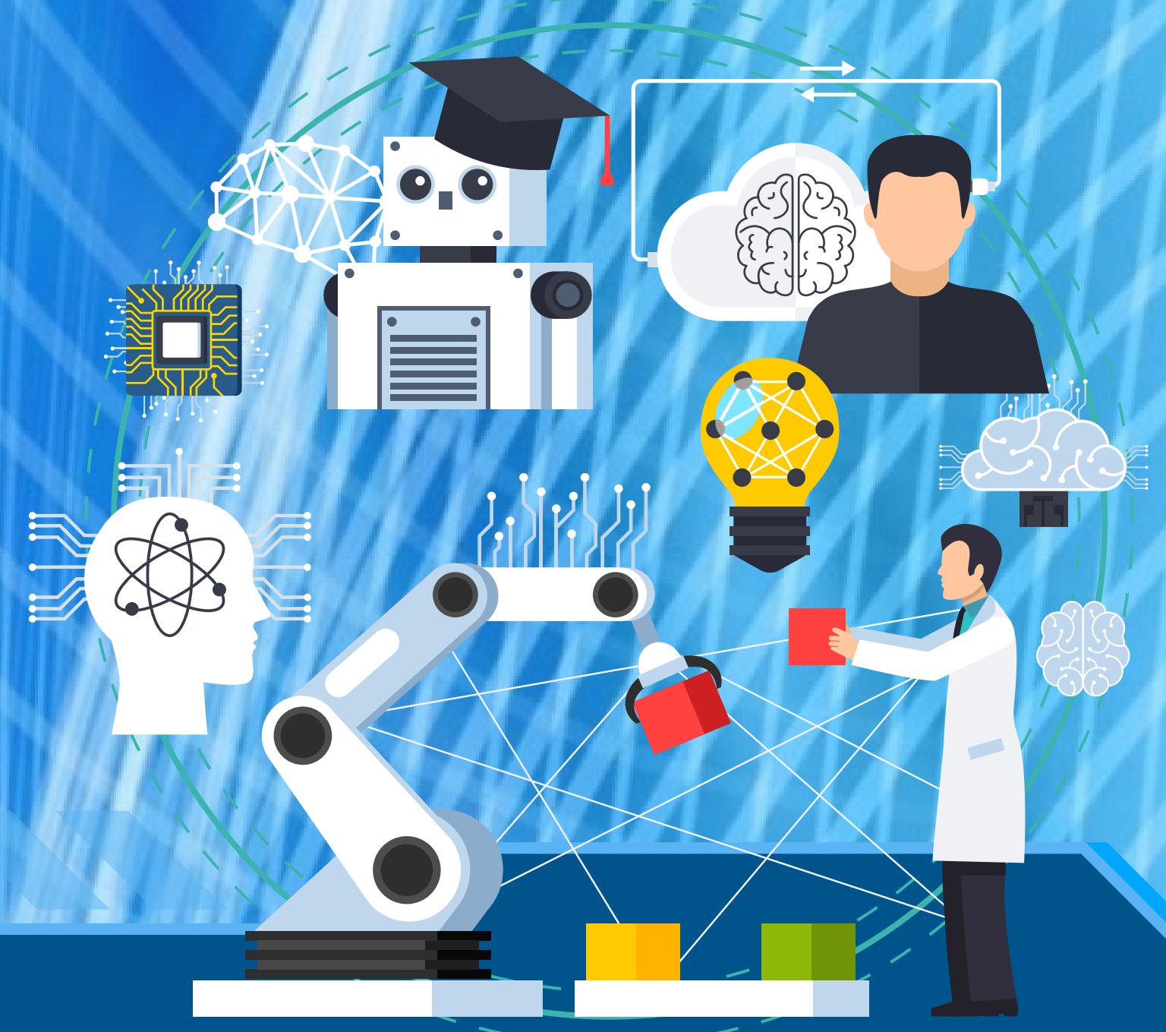
Today's SOCs should have everything it needs to mount a competent defense of the ever-changing IT enterprise. Yet most SOCs continue to fall short in keeping the adversary—even the unsophisticated one—out of the enterprise.

The deck is clearly stacked against the defenders. While the adversary must discover only one way in, the defenders must defend all ways in, limit and assess damage, and find and remove adversary points of presence in enterprise systems. And cybersecurity experts increasingly recognize that sophisticated adversaries can and will establish lasting footholds in enterprise systems. If this situation were not bad enough, more often than not, we are our own worst enemy. Many SOCs expend more energy battling politics and personnel issues than they do identifying and responding to cyber-attacks. All too often, SOCs are set up and operate with a focus on technology, without adequately addressing people and process issues. The main premise of this infographic is that a more balanced approach would be more effective.

SOC Function
SOC Management

Shortcomings and problems

Lack of skilled staff undermines the ability of in-house and centralized SOCs to take full advantage of the available cybersecurity tools and research capabilities.



SOC Function
Automation, AI and Machine Learning

Shortcomings and problems

SOCs experience deficiencies in critical security fields like process automation and use of AI and ML to detect and fight unknown threats.

SOC Function
Integrations

Shortcomings and problems

SOCs are lagging in integrating many security tools that boost the capabilities of proactive solutions.

SOC Function
Threat Alerts

Shortcomings and problems

SOCs produce an overwhelming number of alerts and false positives, which lack context and do not correlate between each other.

SOC Function
Operations

Shortcomings and problems

Many SOCs and their customers experience problems with silo mentality as well as issues originating from legal or regulatory requirements.

SOC Function
Threat Analysis

Shortcomings and problems

As SOCs produce large amounts of statistical data and alerts, it is hard to get and analyze eventual threats in a context.

SOC Function
Complexity

Shortcomings and problems

SOCs are highly complex environments that are increasingly hard to manage and make them effective.

In addition to the above shortcomings of the SOC model, cybersecurity experts often cite problems related to the lack of adequate information about the digital assets and nodes to be protected and the lack of visibility related to actual and possible threats. This is a major problem when you are not able to protect an asset you do not know, against threats you do not know.

LMNTRIX
BE THE HUNTER | NOT THE PREY