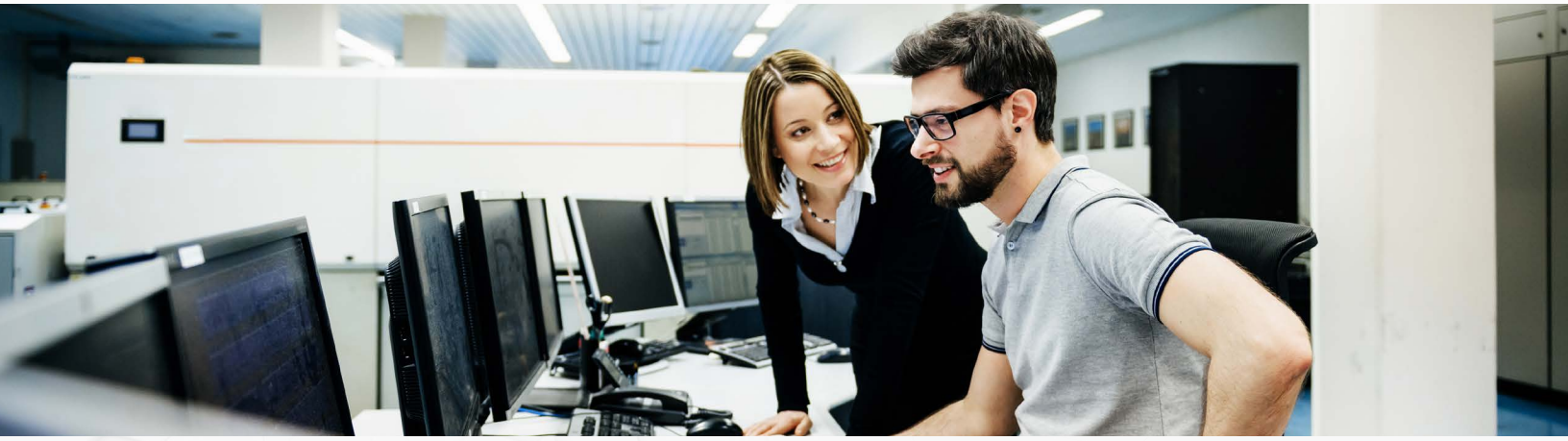
SHERLOCK



The Future SOC

How Security Operations Centers must evolve to meet tomorrow's cyber threats

SherlockCloud.io | @Sherlock_Cloud | info@sherlockcloud.io

Are you waiting for something bad, or going somewhere good?

A CEO asked me that once. It is one of those deep questions that we should all ponder at times.

In the world of cybersecurity, the conventional thinking for a Security Operations Center (SOC) is to plant people at consoles and have them passively monitor alerts. When an alert is serious enough, they react to stop the attack. Whether this is done internally or through a managed security provider, the end result is the same: a passive approach to security.

> "People passively monitoring alerts is not an effective SOC strategy. We need a Future SOC."

Passive security is not effective. Every breach over the past 10 years is proof of this, including recent megabreaches from Equifax, Target, and even Panera Bread. All of the breached companies from the past five years had a SOCs and/or managed security providers. They still missed the attack.

People passively monitoring alerts is not an effective SOC strategy. We need a Future SOC.

SOC Fail

We can trace the failure of SOCs to four primary reasons:

- **It is reactive**
  Once the alert has gone off, it is too late to stop it. Alerts are the hacker's way of saying goodbye. A SOC must become proactive.

- **It incentivizes inaction**
  When people are in a passive role, a serious incident means additional work and intense scrutiny. This creates panic and therefore an incentive to dismiss alerts. A SOC must force-multiply analysts so they can avoid panic conditions.

- **It assumes you know everything**
  Passive security assumes your data provides a complete picture of the environment. Even under ideal conditions, there are ample blind spots in the data. SOC must provide quick access to data.

- **The 4:00 AM Fallacy**
  Waiting for an alert or a call from a managed security provider hinges your cybersecurity decision-making on panic. It is

unrealistic to think an analyst, sitting at a console in the middle of the night, can react with the speed and decisiveness necessary to protect the business. People generally make short-sighted decisions in moments of panic. The SOC should not be put into a position of having to make such a decision, the technology should do this for them.

If the security of your business depends on people passively watching data, you can almost count on a breach. We need a new approach.

> "You must get in the game, to win. That means owning the responsibility of security, completely."

The Game is On

To overcome these weaknesses, we must transform IT security teams from passive victims, to active hunters. The SOC of the future will look much different:

- **Fully automated**
  Only technology can react at the speed of attack. The future SOC will automate security in every possible way, from deployment, to data mining, and response. Security technologies are now capable of detecting, tracking, categorizing, blocking, and eradicating malicious code with no human intervention necessary.

- **Extreme agility**
  The SOC of the future must adapt quickly to new threats and techniques. SOC teams will require more authority and autonomy to enact change throughout the organization, without resorting to inefficient approval hierarchies.

- **Hunting**
  Rather than waiting for an alert, analysts are actively and aggressively searching attackers and malware. They are conducting routine data hunts, chasing leads, and eradicating potential exploit vectors.

- **Code in the cloud**
  The SOC of the future is entirely in the cloud and it is all code. Physical devices are too inflexible and prone to failure. Only the cloud can provide the automation, speed, scale, and flexibility to handle the mountains of data and react at the speed of attacks.

How do you build this next-generation SOC?

Stick it in the cloud

- **You must get in the game, to win.**
  That means owning the responsibility of security, completely. It also means your managed security partners must be inside your environment, rather than you being inside theirs. Sending events to some far-off data center is fine for storage and reporting, but it is not going to protect your business. The way to solve this, as well as a lot of other issues with security is to move your entire SOC into the cloud, like AWS or Azure.

- **Go hunting**
  Your SOC must become a "hunting platform." The technologies, like SIEM, must be constantly searching for evidence of compromise. Likewise, your people must become agile security ninjas, able to move through the environment effortlessly with a nose for trouble.

- **Automate, automate, automate**
  Rather than obsessing over having the "best of breed" security technologies, obsesses over interoperability. Point solutions are a waste of time and money. You need an integrated platform that automates the searching and reacting. There are orchestration tools which can coordinate responses across disparate platforms.
  Seek out Security Analytics platforms that unite NGFW, endpoint, SIEM, sandboxing, and more into a cohesive ecosystem.

- **Leadership Level-Up**
  If your organization cannot mature, change, and get better, then no amount of new technologies or trained staff will make a difference. You must become comfortable with the uncomfortable. This means security leadership that can persuade, coach, and inspire people.

Cybersecurity is not a passive effort. We cannot wait for an attack. We must go on offense and seek out the attackers before the breach.

What are you waiting for?

Ready to Know More?

If you need any help, the cloud security experts at Anitian and Sherlock Cloud Security are here for you.

Here is some cool stuff to check out:

Security Hardened Operating Systems
Available on the AWS Marketplace

Sherlock Cloud Security
Offering AWS-native managed detection and response services, and more

Anitian's Professional Services
Providing certification, gap assessments, cloud architecture assistance, penetration testing and web application testing services