Accelerate your SOC!

Expand visibility. Reduce alerts. Respond faster.

Meet Sara and Jeff. They work in the Security Operations Center (SOC) at a Fortune 500 company.

Pardon their appearance. **They haven't slept much lately.**

Today's SOC operations are challenged by:

- A shortage of skilled team members
- A lack of visibility into enterprise infrastructure
- An overwhelming amount of alerts from disparate security products

There will be **3.5 million** unfilled cybersecurity positions by 2021.[1]

46 percent of organizations use tools from more than 11 security vendors, with some using 50 or more![2]

Nearly **half of the daily alerts** an organization receives go uninvestigated.[3]

These challenges are dramatically impacting Sara and Jeff's efficacy in the SOC, putting their organization at risk. With an ever-expanding attack surface and constantly evolving attacks, time is more critical now than ever.

The average time it takes for an organization to detect a breach is **197 days**.[4]

That's a dangerous amount of dwell time for attackers!

Moving forward

SOCs must operate like well-oiled machines, seamlessly integrating security technology and threat intelligence for automated, streamlined response.

- Integrated Security
- Threat Intelligence
- Streamlined Response

In fact, **Gartner** predicts that by 2022, 50% of all SOCs will transform into modern SOCs with integrated incident response, threat intelligence and threat hunting capabilities, up from less than 10% in 2015.[5]

Studies show organizations that deploy automated security technologies can save over

$1.5 Million

on the cost of a data breach.[6]

How can Cisco help accelerate your SOC?

Expand visibility across your entire attack surface, including the network, endpoint, internet, and cloud.

Reduce massive data sets to critical, high-fidelity alerts with advanced security analytics and integrated threat intelligence.

Respond faster to threats through simplified investigations driven by context.

With Cisco, Sara and Jeff can detect and investigate problems faster...

...so they can quickly remediate them and **move on**.

Get started today

Cisco AMP for Endpoints
Quickly discover and contain advanced malware.
Start free trial

Cisco Threat Grid
Conduct in-depth malware analysis to better prioritize risks.
Start free trial

Cisco Stealthwatch
Detect threats faster across the network and in public cloud infrastructure (even in encrypted traffic).
Start free trial

Cisco Umbrella Investigate
Gain unique insight into attacker infrastructure.
Learn more

Cisco Threat Response
Dramatically simplify security through automated integration. (Already included with several products.)
Learn more

For more information, visit cisco.com/go/security.

1.Cybersecurity Ventures, Cybersecurity Jobs Report 2018-2021. 2.Cisco 2018 Annual Cybersecurity Report. 3.Cisco 2018 Annual Cybersecurity Report. 4.Ponemon Institute, 2018 Cost of a Data Breach Study. 5.Gartner, Selecting the Right SOC Model for Your Organization, 18 September 2018. 6.Ponemon Institute, 2018 Cost of a Data Breach Study.