Tipsheet
Cisco Public

CISO's Survival Guide

5 tips to make your operations more efficient

Juggling security and business risks is a challenge when you're facing talent shortage, evolving threats, and a sprawling vendor landscape.

How can you go from overwhelmed to empowered?

1. Consider integration to be a key part of your buying decision.

The vendor sprawl in a typical security environment causes unnecessary complexity and inefficient workflows. To make matters worse, chronic talent shortages make it difficult to fully adopt existing solutions which increases exposure. One tactic to mitigate these challenges is to adopt an open, portfolio-based platform that enables your solutions to work together.

This type of platform approach is unique in two ways. First, it natively integrates the portfolio's backend solutions with a unified frontend. Second, it enables other vendors' technologies to seamlessly integrate with that frontend.

When the burden of integration is shifted primarily to the vendor, you end up leveraging existing investments, building on what you have, and creating a strong foundation for future needs.

2. Make NetOps and ITOps an extension of SecOps.

Network, IT, and security teams have traditionally worked in siloes, but their reliance on each other to solve problems causes bottlenecks. You can unify your teams with collaborative workflows and shared context to enable ITOps to remediate issues with meaningful alerts and allow NetOps to enforce policies more consistently. This reduces the burden on SecOps and improves the productivity of all three teams.

Achieving this level of collaboration isn't easy, but it's possible with the right approach. An integrated platform can help, so long as it provides a customizable unified view, allowing each team to see the alerts, metrics, and context that are most meaningful to them without disrupting the others.

3. Guide your decision making with a security maturity model.

With the pressures of tight budgets, chronic staff shortages, and a constantly changing threat landscape, it is easy to fall into a reactive mode of security. However, in this reactive paradigm, your investments may only help you maintain the status-quo rather than free you to mature your security organizations.

Pick a security maturity model and be proactive about your trajectory. There are many to choose from, but most models reflect unified visibility across control points, cross-environment automation, and clear security metrics as advanced capabilities. While it's possible to achieve these outcomes via manual SIEM/SOAR integrations, all of these are native functions of an integrated security platform.

4. Give your people one view to focus on, not twenty.

Your security teams are constantly swiveling between different consoles and interfaces which slows them down and generates conflicting alerts.

Give them a unified view by integrating your security infrastructure. This streamlines workflows and maximizes the value of your investments. It also enables your teams to act on alerts, harmonize policies, respond to threats, and learn best practices – unlocking value faster with a simpler, more consistent experience.

5. Use automation wherever you can to make your people more efficient.

Your teams probably lose a lot of time to repetitive, manual processes – this is inefficient and leaves room for human error. With a platform, you can use automation to handle many tasks such as sharing threat and trust context, and adapting network or application access for compromised endpoints.

For example, you could use these capabilities together to prevent unhealthy devices from accessing sensitive data. First, use your secure access solution to identify endpoints that are infected or unsecure, then use automation to change the authentication policy for that device across your entire environment until the threat is remediated.

By blocking access for untrusted devices, you can respond to threats faster and prevent data breaches without getting in the way of business.

Unlock new potential in your investments today

Start the journey with SecureX

cisco.com/go/securex