ADOPTING PROACTIVITY: How SOCs Can Evolve to Advanced Fusion Centers

What Once Worked

In recent decades, security operations centers (SOCs) have emerged as a reactive defense strategy, dedicated to threat detection and response. But with today’s volume, velocity and complexity of security threats, many SOCs simply cannot keep up.

- 63% of organizations have a shortage of IT staff dedicated to cybersecurity¹
- 68% of security breaches take months or longer to discover²

An Evolution Is Needed

Forward-thinking organizations are starting to make the move toward building modern SOCs, or full-scope advanced fusion centers (AFCs). This evolution brings together all the proactive, preventive and predictive components needed to optimize your cyber operations program.

- 50% of all SOCs will transform into modern SOCs with integrated incident response, threat intelligence and threat hunting capabilities by 2023³
- Security orchestration, automation and response (SOAR) tools will begin to deliver credible decision support capabilities powered by advanced analytics, such as machine learning⁴

SOC TO AFC: SIX EVOLUTIONS

1. People–Tech Connection

   Traditional SOCs are built around people who are enhanced by technology. AFCs are built around technology that is enhanced by people.

2. Task Focus

   Traditional SOCs focus on monitoring and managing alerts reactively, while AFC intelligence, automation and orchestration proactively work together to reduce manual, repetitive tasks.

3. Integration

   Traditional workflows for SOCs are generally not integrated. Forcing staff to manage multiple consoles and reports. AFCs fuse and analyze data from multiple sources in real time to enrich threat intelligence and improve fidelity.

4. Operational Coverage

   SOCs typically cover endpoints and networks, while AFCs extend that coverage to include all security domains—like on-premises, cloud, email and mobile.

5. Cyber Measurement

   Key performance indicators (KPIs) used by SOCs tend to measure tactical activities and tool output, whereas AFCs use business- and industry-specific KPIs and key result indicators (KRIs) to focus on efficacy, proactivity and future trends.

The Best Way to Evolve Your SOC is to Be Proactive

As the world’s leading end-to-end security solutions integrator (SSI), Optiv partners with enterprises to advance their cyber operations—from planning, to building, to running. We can help you take the meaningful steps you need to build your Advanced Fusion Center and secure your security.

Get Proactive

References:

1. (ISC)/two.num Cybersecurity Workforce Study, 2018.