

SecurityAdvisor for Palo Alto Networks Joint Solution Brief



Challenges

- ~90% of all security incidents that hit an organization are caused by human actions.
- SecurityAdvisor research shows that only 5% of the total workforce is responsible for the majority of these incidents.
- Today's industry standard for security awareness training involves 6-8 hours per employee per year.
- Most security awareness is disconnected from the real problems that SOC teams work on.

Solution

- SecurityAdvisor provides bite-sized, personalized security awareness lessons to employees based on their unique risk profile.
- Our integration with PANW increases SOC efficiency and allows SOC teams to engage with users who were involved in or impacted by security incidents.
- Leveraging the content pack and integration between Cortex® XSOAR and SecurityAdvisor, your security team can automate and optimize complex workflows across the full stack of your information systems and security tools.
- Our integration with PANW is seamless and SOC teams can coach users without even logging into our console.

How does it work?

- SOC teams can use PANW Cortex XSOAR playbooks to engage end users and coach them even as they investigate specific types of incidents including Phishing, Ransomware etc.
- Leveraging the Cortex XSOAR content pack, the SecurityAdvisor platform automatically identifies risky user behavior and delivers a personalized microlesson in real time.
- SecurityAdvisor provides SOC teams with specific teachable moments and bite sized content to engage users.
- Engage employees with targeted, contextual lessons including games, comics, posters, text messages, newsletters, and traditional online training.
- Administrators can customize coaching templates as needed.

Use-Cases and outcomes

- **Leverage insights:** Take data from SecurityAdvisor to coordinate security responses from 550+ Cortex XSOAR third-party product integrations.
- **Enrich incidents:** Use employee information to better understand how incidents happen and help your security team find gaps in their program.
- **Manage employee training:** Using Cortex XSOAR, improve efficiency with targeted modules and reminders to automate security training.
- **Provide evidence:** Produce in-depth summaries of user training to corporate stakeholders, reducing the strain from management.
- **Save time:** SOC analysts spend less time investigating security incidents as a result of fewer security incidents. Measurable reduction in security risk including >80% reduction in incidents that are sent to the SOC.
- **Demonstrate compliance:** Use reports to satisfy compliance requirements around security awareness (NIST, ISO 27001, HIPAA, PCI-DSS, SOC II etc.)

About SecurityAdvisor

SecurityAdvisor offers automated and personalized cybersecurity awareness training and education for end users. We help build a culture of cyber-immunity organization-wide and engage end users as and when events occur. This approach is superior to traditional security awareness training.

About PANW Cortex XSOAR

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices.