SECURITY PRODUCT OVERLOAD?

A look at how K logix understands and measures how technology investments fit in security programs.

Contributor: Don Cook, Director of Program Management

The Security Product Overload Challenge

The security product overload is an enormous challenge facing many CISOs and security leaders. Don Cook, Director of Program Management for K logix says, "New CISOs, even experienced CISOs, come in to a new organization and they are overwhelmed by the multitude of existing technology investments. Is it solving the problem it was originally purchased to solve? Do I have clear visibility to effectively utilize the investments? How do I ensure they are aligned to identified risks?"

Answering these questions may be a challenge for many CISOs. To address this, K logix has developed a **Technology Gap Assessment** to help CISOs understand and measure how technology investments fit within their information security programs.

> ## TECHNOLOGY GAP ASSESSMENT:
> Clear visibility to effectively utilize technology investments and ensure they align to identified risks.

K logix's Technology Gap Assessment Process

Cook says to understand the effectiveness of a specific investment, technology must be evaluated via three lenses:

1. **Operational Impact** – Is the product fully implemented, supported, and being used to its maximum value?

2. **Risk Mitigation** – CISOs need to understand how a technology investment helps reduce risk. One way is to reference the Critical Security Controls Top 20. CISOs need to identify security domains that are over or under-invested in the environment as measured against strategic security goals.

3. **Financial Cost** – The total cost of operating, and supporting a security solution, including staff required to manage the solution must be weighed against its impact on the overall strategy. A CISO should have the ability to look into the future and anticipate where investments in technology may need to shift in order to align with strategic goals.

K logix's Technology Gap Assessment Outcome

Through interviews and information gathering workshops, K logix explores the technical security controls and business impact to determine the current operational posture of each solution. This service answers these critical questions:

1. Are my existing security solutions implemented effectively and realizing maximum value?

2. Are these investments achieving their desired goals?

3. Are these investments keeping pace with the evolving organization?

4. How well are my security investments operationalized?

5. How effective are my people at managing these security investments (including documenting process)?

6. How do these security solutions align to a framework that can be leveraged to make strategic risk-based decisions?

7. In what areas am I underinvested, and where am I overinvested?

8. Is there an opportunity to shift funding to risk areas that need more attention?

Technology Gap Assessment in Action

Recently, a CISO undertook a K logix Technology Gap Assessment to understand and analyze the multitude of security technology solutions in his environment. "The assessment provided a clear picture of the technology investments in my program including their maturity, documentation, deployment status, alignment with SANS CSC, and effectiveness. I was able to identify problem areas to be addressed, and justify my direction and shift in funds, to meet our strategic priorities."