Effective Security Observability

With Vectra AI

February 2023

Unlock the mystery: despite many cyber security investments, organizations still experience breaches

Eliminate the unknowns and start with Effective Security Observability

As cyber threats become increasingly sophisticated, relying solely on one or two security solutions to protect a business is no longer enough. The likelihood of a successful attack evading detection by current security measures is alarmingly high. It is crucial for companies to adopt a comprehensive approach that looks at the effectiveness of their security solutions in order to stay ahead of potential threats.

Unknown security gaps can lead to serious consequences. To prevent attacks, organizations need to use technology and implement proper processes and governance. However, the effective implementation of such technology as well as trained employees following protocols are crucial for comprehensive protection.

69% of IT security decision makers think they may have been breached and didn't know about it; a third (31%) think this is "likely".

Source: Vectra research study *Fit for Purpose or Behind the Curve?* (2021)

Introducing Effective Security Observability

Effective Security Observability (ESO) is KPMG's approach to fully integrate security solutions within your cyber operations, risk processes and response capabilities. By maximizing the combined value of technology, people and processes, we are able to make detection processes more effective, eliminate noise, and focus on cost savings and efficiencies.

Effective observability into your entire IT ecosystem requires visibility into all parts of the IT landscape.

Correlation and orchestration activities need to enable security operations to be efficient and actionable.
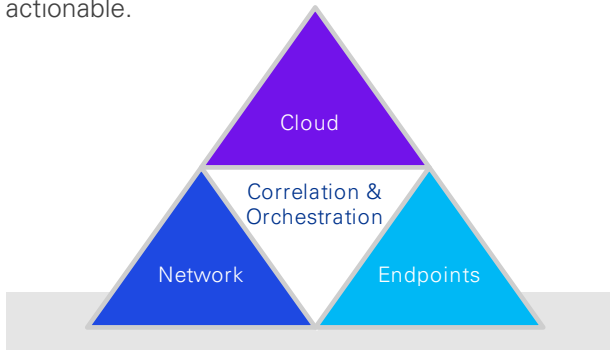
Collaborating with your security teams, we establish a strategic operating model to seamlessly integrate and optimize the performance of your security capability to support this. This model serves as the foundation for a robust and effective security capability, providing peace of mind and protection against threats.

76% of security decision makers bought tools that failed to live up to their promise – citing poor integration, failure to detect modern attacks, and lack of visibility as reasons.

Source: Vectra research study *Fit for Purpose or Behind the Curve?* (2021)

"We made it our mission to help organizations become more effective in detecting threats and mitigating risks. We focus on maximizing business value and operation excellence," explains Henrik Smit, Director of the CyberOps team at KPMG.

How Vectra AI fits into KPMG's ESO?

Vectra's technology fits perfectly into these objectives through a KPMG tailored & cost-effective security operating model.

This enables a streamlined identification and tracking of advanced threats and minimized response times. In other words: eliminating 'unknowns', and enhancing your effectiveness.

In just a matter of days, you'll gain clarity about the security threats to your applications, networks, cloud, and physical hardware as part of our approach.

" Our Security Operations Center actively monitors IT and Medical systems. Effective Security Observability is essential to deliver the best possible patient care, health research and education."
CISO, University Medical Center

Protect against the known and unknown

The core deliverable of Vectra AI is their industry leading Attack Signal Intelligence (ASI) which focuses on what is urgent and needs to be improved within security operations.
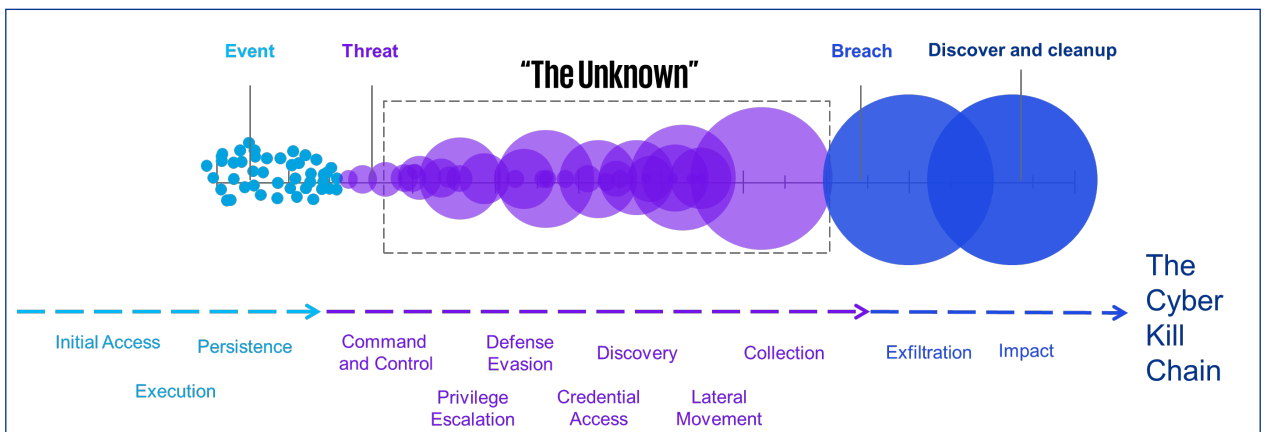
Effective Security Observability with ASI enables:

- Coverage – erasing unknown threats across 4 of 5 attack surfaces – Cloud, SaaS, Identity, Networks – without the need for agents;
- Clarity – automatically detecting, performing triage, and prioritizing threats that matter now;
- Control – optimizing your investments in tools, processes, and playbooks to boost SOC efficiency and effectiveness.

How does ESO maximize your business value?

KPMG provides a balance between people, processes and technology to enable clients to manage their security effectively, by:

- Killing noise. To focus on critical security events based on automation and AI.
- Analyzing critical information first. To be ahead of attackers who use modern methods such as machine learning and social engineering in their approach.
- Using a practical and proven approach. To reduce response times and integrate security within your business processes.
- Keeping it cost effective and feasible. To eliminate unnecessary costs for monitoring your IT landscape.

It's our passion to bring the right balance of quality and affordability for your cyber security needs.

Why KPMG Cyber Operations?

We recognize that each organization has unique needs and ways of working. Our approach is simple and to the point.

We specialize in building trust as a business partner and integrate solutions with the right balance of people, processes, and technology.

1 Our cyber security solutions are designed to help you **stay ahead** of the curve and proactively defend against potential security breaches.

2 Thanks to our global presence (in 144 countries and with 6,300+ cyber security professionals worldwide) we can **scale and deploy anywhere**.

3 With our global partners and capabilities across the entire security spectrum, we **oversee and incorporate the complete picture** of your security organization.

Want to see the benefits for yourself? Contact us to schedule a live demo.

Henrik Smit
Director Cyber Operations
KPMG Netherlands

+31 (0)20 656 7247
smit.henrik@kpmg.nl