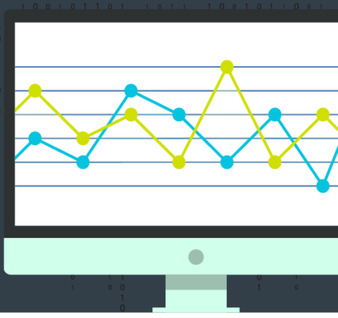
DEVO

5 THINGS
Your Security Data Is Not Telling You



#1. How Long a Threat Actor Persists in Your Environment

The average threat actor is rifling through your systems for months.

Determining the duration of an attack is key to understanding and documenting the nature and extent of the breach. Enabling access to all historical and real-time data at the drop of a hat is critical to analyzing and visualizing the threat vector, and identifying historical patterns. However, data storage costs in traditional solutions can quickly burn a hole in your wallet.

#2. How Much an Incident Impacts Your Business

Security has a heightened profile in the eyes of business executives, customers, and regulators.

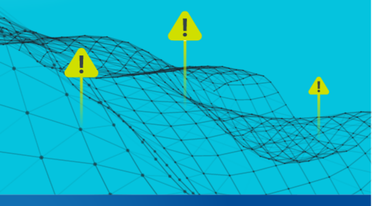
Your team is responsible for determining the ways in which a threat is reaching into and impacting the business. Investigation and digital forensics relies on complete visibility into security data – which is hard to get these days – to understand the scope of damage and risk to the business, and determine the right remediation, recovery, legal, and compliance next steps.

#3. How All Network, Endpoint, and Log Data Sources Relate

The correlation of security data and digital business elements is core to developing the full threat story – from initial entry point to method of data exfiltration or system shutdown.

That said, easy and quick aggregation and correlation of disparate sources can be difficult with hour-long query times and performance degradation, leading to dropped data, slow response times, and a potentially devastating breach.

#4. How an Incident Maps to MITRE



Information on known adversarial tactics, techniques, and procedures (TTPs) can make analysts' lives a heck of a lot easier.

Advanced SOCs must map threats and threat vectors to industry frameworks, like the MITRE ATT&CK framework, to stop adversaries from executing their objectives. However, analysts are underwater, making automation of threat mapping a key factor in its implementation.

#5. How to Action Findings

Rapid response is predicated on quickly understanding the profile of the attacker and how to stop them, enabling you to effectively react to a threat minutes after you detect it.

What's more, you need a seamless and responsive method of actioning your findings to close the loop; this includes automatically updating recommendations on previously solved problems to reduce double-work or integrating case management solutions.