cybereason

Will the Excessive False Positives Syndrome Paralyze Security?

As breach detection becomes high on a security team's agenda, many organizations arm themselves with multiple layers of detection and protection solutions. Even though these tools provide security teams with better threat visibility, their dependence on rigid rules creates an unmanageable number of security alerts, many of which are false. The time spent manually investigating alerts and eliminating false positives hinders a security team's ability to protect their organization.

CISOs are concerned with excessive false positives for two reasons:

1. False Positives Decrease Productivity

Numerous studies and media reports have discussed the dearth of security talent. An organization's overworked security staff can't waste time looking into incidents that turn out to be false, especially considering incident response teams spend on average a month investigating true incidents. Any time spent investigating false positives clearly impairs security's efforts to shorten the response time when dealing with true incidents.

2. "Crying Wolf" Desensitizes the Organization

A Bloomberg Business Week news report revealed that "Neiman Marcus hackers set off 60,000 alerts, which were only 1% of the daily entries on the endpoint protection logs used by the company." Since security employees receive so many alerts, many being false, they can accidentally overlook malicious activity and essentially put their company at great risk.

> *The time spent manually investigating alerts and eliminating false positives hinders a security team's ability to protect their organization.*

Why do Most Security Solutions Produce EFPs?

Most security solutions base their detection on a pre-defined set of rules and look for specific indicators of compromise. This means the system will detect a set of behaviors with a very limited context. For example, in order to detect a hacker using brute-force attack, a pre-defined rule is usually set to look for several consecutive failed log-in attempts. While five failed log-in attempts could indicate a cyber attack, it could also be an employee trying to remember his password after returning from vacation.

The problem with rigid predefined rules is that they do not leverage context, forcing security analysts to manually review all alerts and decide if they are valid.

Changing the Threshold is Risky

Security teams will change the threshold of alerts to be less sensitive to decrease the amount of EFPs. However, this adjustment may cause them to miss important alerts.

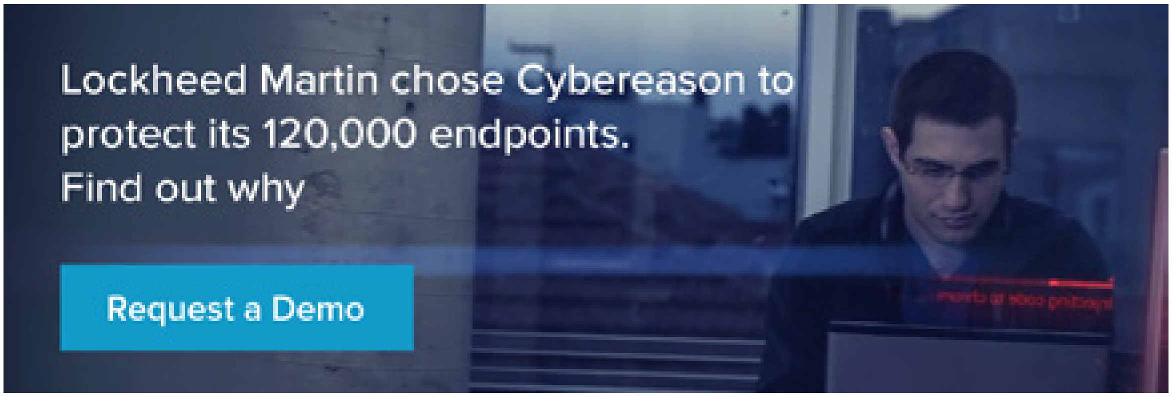
Attackers are well aware of security's tendency to fidget with the threshold and they will leverage this weakness to evade detection. For example, hackers will use "low and slow" attack techniques, where they meticulously plan their steps and spread them out over a long period of time. Making detection capabilities less sensitive would yield less alerts, but would also radically impair the ability to spot attacks.

The Solution: Automated Validation

Although no security system can promise zero false positives, the current situation has teams wasting endless hours on manual validation instead of remediating real threats. In order to reduce EFPs without compromising detection quality, a new approach must be taken. Instead of reducing the amount of alerts and potentially missing valuable pieces of information, use smart technologies that can comprehend everything that is going on in the organization, and deploy artificial intelligence to automatically dismiss false alerts.

Data analytics and machine-learning techniques have been developed to imitate the human brain by using context, past experiences and surrounding evidence to replicate the human thought processes to judge a situation. Such technologies are used for various applications and industries, from medicine to **Google's self-driving car.**

In security departments, data analytics can be leveraged to decide if a threat is legitimate and automatically eliminate false positives. This will free up the security team's time and allow them to deal with the real problem: cyber attacks.


Lockheed Martin chose Cybereason to
protect its 120,000 endpoints.
Find out why
Request a Demo

Cybereason was founded in 2012 by a team of ex-military cybersecurity experts to revolutionize detection and response to cyber attacks. The Cybereason Malop Hunting Engine identifies signature and non-signature based attacks using big data, behavioral analytics, and machine learning. The Incident Response console provides security teams with an at-your-fingertip view of the complete attack story, including the attack's timeline, root cause, adversarial activity and tools, inbound and outbound communication used by the hackers, as well as affected endpoints and users. This eliminates the need for manual investigation and radically reduces response time for security teams. The platform is available as an on premise solution or a cloud-based service. Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv, Israel.