Guide to Reducing False Positives & Ensuring Data Accuracy with XDR Solution

As the threat landscape of cybersecurity continues to evolve, enterprises now find themselves spending countless hours on identifying and mitigating potential threats while managing overwhelming amounts of data. But one persistent problem for security teams is the flood of false positives alerts that indicate possible threats but turn out to be benign. Not only do these waste valuable time and resources, but they also contribute to alert fatigue, reducing the overall threat detection ability of teams. Add to that poor data quality, which impairs the effectiveness of risk mitigation by hiding valuable detections.

This blog dives deeper into how enterprise-grade XDR platform helps address these challenges, minimizing false positives and ensuring data accuracy to enable enterprise cybersecurity and freeing IT teams from investigating noise and allowing them to focus on real threats.

What is a False Positive?

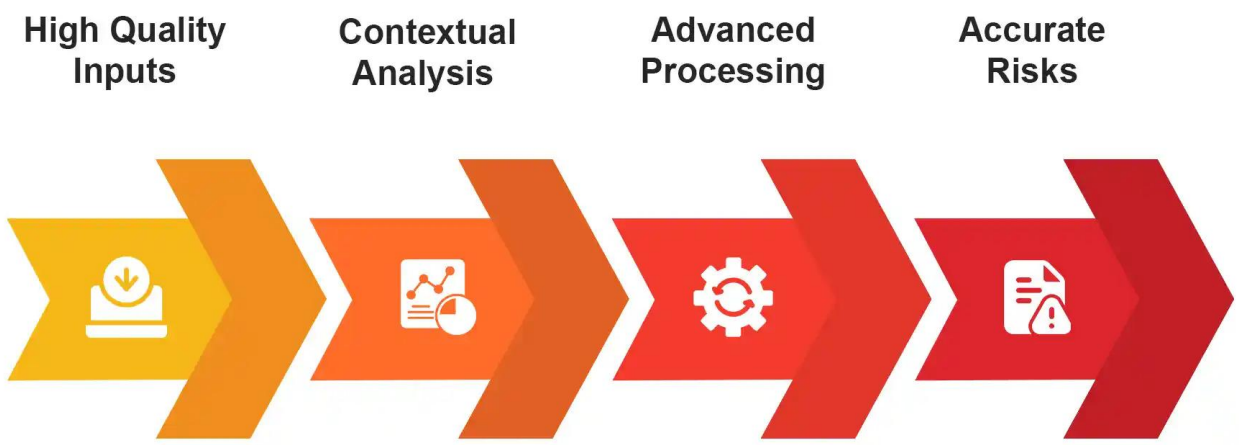
False positives in cybersecurity are triggered when a system incorrectly identifies a benign activity, event, or entity as a potential security threat. An example of a false positive is a legit user logging in from a new device that would trigger an alert for suspicious activity even though it posed no harm.

False positive alerts stem from overly sensitive detection algorithms, outdated threat intelligence feeds, lack of contextual data, or misconfigured security tools. Static rules and signature-based detection are particularly prone to triggering false positives because they cannot adapt to changing user behaviors or distinguish between legitimate activities and malicious activity. Although their aim is to be over-assured, false positives can swamp IT teams and detract from focusing on real threats.

How Algorithms Help Reduce False Positives in Detection Tools

Modern threat detection systems use machine learning algorithms to minimize false positives while maintaining accurate threat detection. These algorithms analyze historical data, user behavior patterns, and network traffic to establish baselines for legitimate activities. By understanding normal patterns versus malicious behavior, algorithms can accurately detect true threats while reducing false alarms from routine tasks and legitimate files.

What is Data Accuracy in Cybersecurity?



Cybersecurity data accuracy means that the information utilized for detection and response against all threats is precise and reliable. This helps to ensure that security tools and security monitoring systems can identify the differences between normal activity and potential threats with minimum false positives.

Achieving accurate threat detection requires implementing robust data validation processes, maintaining updated threat intelligence feeds, and establishing behavioral baselines. Security systems must be able to distinguish between routine operational changes—such as network configurations, system updates, or scheduled backups—and genuinely suspicious behavior that warrants investigation.

Real threats and a secure enterprise depend on accurate data. Inaccurate or missing data may result in false positives. This can put an organization’s security posture at risk by wasting resources on non-issues or perhaps exposing vulnerabilities to exploitation.

Moreover, better data gives the right context to prioritize threats. For example, security systems can prioritize and allocate resources by cross-referencing alerts with real-time threat intelligence to identify the highest-risk threats. In an age of increasingly sophisticated cyberattacks, only data accuracy enables quicker detection, precise mitigation, and reduced incident response times.

- Maturing Advanced Threat Defense
- 4 Must-Do’s for Advanced Threat Defense
- Automating Detection and Response

[Download the Whitepaper Now!]

Strategy for Dealing with False Positives

To overcome the challenges posed by false positives and data accuracy, companies are relying on eXtended Detection and Response (XDR) solutions. This solution broadens their approach to provide a more cohesive, intelligent, and context-based framework for threat detection and response.

Here's how XDR ensure data accuracy along with reduced influence due to false positives:

Centralized Data Correlation

XDR is an advanced data-driven security model that combines data from different security layers — endpoint, network, email, cloud environment, etc., into one tailor-made platform. Most traditional security systems operate in silos, examining data in isolated pockets in a decentralized manner, resulting in fragmented insights and lost connections.

With XDR for enterprises, you get all this data to be correlated and analyzed together for a better holistic view of possible threats. This centralization serves to eliminate noise and reduce false positives by providing context to each alert, allowing analysts to quickly differentiate between harmful activity and passive benign activity.

Advanced Threat Analytics

Threat analytics advanced by machine learning and artificial intelligence are used by XDR solutions to analyze large volumes of data in real time. Using advanced algorithms, XDR platforms are capable of identifying patterns, as well as spotting abnormalities, with greater accuracy than traditional security tools. Leveraging these advanced analytics makes it less likely for legitimate activity to be misidentified as a potential threat.

For example, instead of creating false alarms for every unusual login attempt, an XDR system will analyze several variables including user context, expected behavior, IP addresses, and physical location before determining whether to generate alerts. This minimizes false positives and enables cybersecurity teams to concentrate on genuine threats.

Behavioral Analysis

Another key component of XDR is that it can help reduce false positives with the help of behavioral analysis. For this, XDR uses historical activity patterns to understand each individual user's normal behavior profile. This method allows the system to identify normal actions vs potentially threatening activity.

For example, if a user typically works 9-to-5 and suddenly tries to access sensitive files in the middle of the night, this will be flagged by the system as suspicious behavior. But this behavior might fail to trigger an alert if the user used to generally log in at strange hours. Conducting behavioral analysis also leads to better detection of anomalies without a bombardment of alerts that contribute to alert fatigue.

Real-Time Threat Contextualization

Another key enabler to ensure data accuracy is XDR's capacity to contextualize threats in real time. Instead of displaying raw data when an alert triggers, XDR systems enable organizations to detect and understand the context around the threat. This includes information like threat intelligence data, historical info, and even external threat feeds that grant security teams things like the context required to prioritize their alerts.

Automated Data Enrichment

XDR platforms automate the enrichment of raw data by adding threat intelligence feeds, vulnerability databases, and other external sources. This process is now automated to provide greater visibility into potential risks while also allowing security teams to make faster, better informed, decisions. XDR infuses real-time insights into data. It not only improves recognition of potential threats but also correlates them with macro trends and known attack vectors, making detection more reliable.

Minimized Data Gaps

Data gaps can result in threat assessments that are incomplete or inaccurate. XDR fills those gaps with deep insights across all security layers. Traditional systems often only watch a single piece of the network or endpoint, and this can lead to failure to see the full picture; XDR ensures nothing critical is missed. XDR can correlate events at the endpoint, network, and cloud with full visibility across the board, providing a more comprehensive accurate view of the threat landscape.

Continuous Learning

Eventually, XDR solutions will learn constantly from the data they process. As they face increasing attacks and scrutinize greater amounts of data, they refine their capacity to discover and distinguish between legit threats and false positives. The ongoing learning enables XDR systems to adjust to emerging attack techniques and trends, making certain detection mechanisms are both current and effective. Over time, this reduces false positives while also accelerating detection of threats more accurately.

By integrating these advanced capabilities, XDR solutions significantly enhance the accuracy of threat detection and reduce false positives. With XDR, enterprises can ensure more effective cybersecurity operations, enabling them to focus on real threats and respond more quickly to emerging risks.

Questions to Ask Yourself When Choosing an XDR Solution

When selecting an XDR solution, it’s crucial to consider how well it can ensure data accuracy and reduce false positives. As modern cybersecurity threats become more complex, your detection solution also needs to have the ability to detect real and actual threats but also reduce false positive alerts that plague your security teams.

To get you started in making the right choice, the following questions will help you determine whether an offering is right for you and how to ensure alerts are actionable and avoid false positives:

- How does the XDR solution handle anomalies in data flow without generating unnecessary alerts for regular business activities?
- Does the XDR solution integrate seamlessly with existing security tools to enhance data accuracy, or will it require a significant overhaul of current systems?
- What level of customization is available in the XDR solution’s detection rules to align with my organization’s specific needs and reduce irrelevant alerts?
- How does the XDR for enterprises ensure data accuracy in cloud environments and multi-cloud architectures where traditional solutions may struggle?
- Can the solution differentiate between true threats and routine operational changes, like system updates or network reconfigurations, to prevent alert spamming?

- How quickly does the XDR solution adapt to emerging threats and trends in the cybersecurity landscape to maintain detection accuracy?
- What is the XDR solution's approach to false positives in critical systems (e.g., financial or healthcare data), and how does it prioritize these alerts?
- Does the solution have the ability to track threat patterns over time and provide actionable insights to prevent future false positives?
- What steps does the XDR solution take to ensure that alerts are not only accurate but also actionable and relevant to my security team's priorities?
- How does the XDR solution balance the need for precision in threat detection with the risk of missing potential threats due to overly cautious filtering?
- Can the solution adapt its detection capabilities based on the unique behavior of users and systems in my organization?
- Does the XDR solution automate data enrichment to provide more context and reduce manual investigation time?

Fidelis Elevate® is the Answer to All Your Questions

Fidelis Elevate is a comprehensive XDR solution that enables you to ensure data accuracy and reduce false positives. It handles anomalous flows of data while not overwhelming security staff with insignificant threats, protecting valuable resources that need to react only for surveillance-worthy threats. Fidelis' integration with current security tools strengthens data accuracy without needing a major platform change.

The customizable detection rules available through the platform let you fine-tune threat detection to your organization's specific needs and reduce false positive alerts. Fidelis excels in maintaining accurate threat detection in cloud environments, an area where traditional intrusion detection systems often struggle.

Moreover, threat patterns are tracked, correlating critical alerts and automating the enrichment of data to minimize the time needed to conduct manual investigations while allowing analysts to focus on actionable intelligence and refining the broader security posture.

Fidelis Security has built Fidelis Elevate to be a reliable XDR solution that reduces false positives, ensuring your team can focus on what truly matters—protecting your organization.

Don't let threats go unnoticed. See how Fidelis Elevate® helps you:

- Streamline security operations
- Improve resource allocation
- Integrate disconnected security tools

Download Now

Frequently Ask Questions

What is the Impact of False Positives on IT Teams?

False positives create a significant drain on IT security operations, impacting the threat assessment of false positives and leading to multiple problems, including:

Wasted Resources: Security teams spend a great deal of time and energy investigating false positive alerts, diverting their attention from real threats.

Alert Fatigue: A large volume of false alarms can make IT staff desensitized, leading them to ignore or dismiss important alerts.

Delayed Threat Response: False positives waste time that can be better used to respond to real security incidents, thereby raising the threat of breaches.

Employee Burnout: The deluge of alerts can be stressful and reduce productivity of security professionals.

How often do false positives happen?

According to research conducted by the Ponemon Institute, 49% of all alerts produced by security tools are false positives, which highlights the inefficiency caused by such alerts and underscoring the need for solving the problem of false positives to maintain a robust cybersecurity strategy.

What does a false positive look like?

In cybersecurity, the term false positive refers to any instance in which a security product fails to correctly identify legitimate activity. For example, if an employee logs in from a different location, even though it's a perfectly legitimate action, it could raise an alert for suspicious behavior.

In the same context, an abnormal increase in data transfer as part of normal backups can be wrongly interpreted as a potential data exfiltration attack. Overly sensitive detection systems, absence of context analysis, and incorrectly configured rules often lead to false positives.

How Do False Positives Happen?

A false positive in cybersecurity may happen for several reasons:

Overly Sensitive Detection Systems: In an effort not to overlook actual threats, some tools often end up flagging anything that looks suspicious.

Misconfigured Tools: If policies or rules are set incorrectly, it can result in an excess of alerts that are not required.

Old Threat Intelligence: old and outdated threat databases, or false positive threat database, can misidentify threats.

Harmless Anomalies: True atypical behavior such as sudden surge in traffic may look like a suspicious activity.

Integration Challenges: Disconnected security systems that don't share data often lead to misinterpretations.

How to ensure data accuracy?

To ensure data accuracy, organizations should implement data validation processes to detect and correct errors at the point of entry. Audits and cleansing of data on a regular basis can help in picking up any inconsistent or outdated information. Using automation tools for data entry reduces human errors, and maintaining data standards helps maintain consistency. Ensuring that employees are well trained in data management and using DLP (Data Loss Prevention) solutions or similar can prevent the loss of data integrity. A solid backup system also enables accurate data restoration if discrepancies show up.

How to verify accuracy of data?

Ensuring data accuracy requires validating the information with reliable sources or primary records. Automated validation tools can flag discrepancies while data profiling techniques can recognize anomalies. Audits and reconciliation should be done regularly to confirm data standards of business are aligned. You can manually verify a piece of data using sampling methods and can also involve stakeholders to validate critical data; bringing in advanced analytics can further enhance data accuracy.

What is the difference between data accuracy vs data integrity?

Data Accuracy is a measure of how correct and error-free the stored data is and if it correctly represents actual values. Making reliable decisions and reaching organizational goals are only possible when you have accurate data that can help guide the path.

Data integrity not only includes the accuracy of the data but also includes consistency, completeness and security of data throughout its lifecycle. It guarantees that data remains trustworthy and unaltered while in storage, transfer or processing.