DATASHEET

PRISM: How Incydr Prioritizes Risk to Data

The best system to detect, prioritize, and address both known and unknown data risks

Mimecast Incydr's effective risk prioritization eliminates blindspots

Every security team has priority data protection use cases and objectives. Unfortunately, most technologies require you to do the majority of the legwork in order to address them. Traditional data loss prevention technologies require practitioners to define policies and alert rules according to those use cases (also known astheir "known" risks) and manually respond to risky events. These rulesets determine what events are monitored and qualify for remediation. If an event does not meet a ruleset, it becomes a blindspot. This self-fulfilling cycle means you only detect the things you know are an issue. But what about the risks to data you have not yet considered? This approach leaves practitioners scrambling to retroactively find answers when a significant data leak or theft event occurs that didn't match their defined policies. Some more "modern" data protection solutions often put too much emphasis on a single piece of context – such as the source of the file, incorrectly prioritizing events based on an incomplete picture.

Incydr works differently. It detects the unknown, undefined risks to data and makes them known to security teams through its **Proactive Risk Identification and Severity Model (PRISM)**. This system uses three dimensional context to determine what's important so you can investigate fewer events, respond to critical activity more quickly, and automate how lower severity events are handled. The combination of Incydr's granular alert rule builder and its PRISM system ensures you s**ee and respond to both your priority use cases, and the ones you didn't even consider.**

How PRISM works

PRISM is the system Incydr uses to prioritize and remediate the full spectrum of data risk. It calculates a PRISM score which determines the severity of each event based on 250+ Incydr risk indicators (IRIs). These risk indicators **cover three dimensions** of event detail:

Data Context
which identifies the file's source and sensitivity

User context
related to the user's behavior and attributes

Destination context
which includes how the file was moved, and where it is going

The data, user, and destination risk indicators associated with an event are then weighted and used to determine the overall risk score, known as a PRISM score.

The PRISM score is calculated on a scale of 0 to 10. To be deemed a critical event, the total weighted event score must equal a 9 or 10. For lesser scored events, Incydr has the unique ability to automate remediation by sending micro-trainings to the user, quarantining their endpoint, or cutting off their system access.

The truth is, security analysts spend the majority of their time triaging events that could have been handled through automation. PRISM ensures practitioners can automate response to a wider range of risks in order to address data loss more comprehensively and with less effort. It also reduces the number of hands-on critical events analysts need to investigate. PRISM aims to provide a manageable median critical exfiltration activity of around 1% of your total exfiltration activity. This helps you confidently identify what is most important so you can investigate fewer events and respond to critical activity more quickly.

PRISM AIMS TO PROVIDE A MANAGEABLE MEDIAN CRITICAL EXFILTRATION ACTIVITY OF AROUND 1% OF YOUR TOTAL EXFILTRATION ACTIVITY.

Conclusion

PRISM is central to Incydr's differentiating ability to accurately surface both known and unknown critical risks to security teams.

- On day 1, it leverages 250+ IRIs to ensure all activity is prioritized using three dimensional event context.
- It recommends new alert rules based on activity in your environment so analysts don't miss critical activity – and provides the ability to implement those recommended rules with just a few clicks.
- Through its proactive, context-based scoring, PRISM enables organizations to quickly and effectively detect and automatically respond to the full spectrum of data risk. To learn more and see PRISM in action, contact us.

To learn more and see PRISM in action, **contact us**.