WHITE PAPER

HID SAFE™ Analytics

Predict and prevent possible threats with data-based analysis

> *"The goal is to turn data into information, and information into actionable insight."*

Introduction

As security's focus evolves, security professionals are no longer only risk mitigators; they are key players in overall business strategy. The truth for every business unit is that it is far more expensive to explain what went wrong than to allocate funds to prevent threats. Yet most organizations struggle to justify preventative spending.

Traditionally, high security organizations spend a fortune annually to ensure both physical and digital security. This includes spending on access systems, security operations centers, alarm management, surveillance and other security monitoring, as well as a large team of security personnel concerned with mitigating emerging threats. However, most of the spending is on real-time reactive systems. Real-time monitoring can only have a positive impact if threats are detected, analyzed, and solved rapidly enough to prevent incidents. The response window where real-time monitoring can prevent loss is measured in minutes if not seconds. Often, a lot of security resources are used up in monitoring these physical and cyber systems, but many have failed to prevent a major crime. The cost of improving real-time solutions often exceeds the threat itself. This short response window makes the spending on monitoring systems very inefficient. When real-time isn't fast enough, the focus must shift to prevention.

This white paper discusses the concept of predictive analytics and how it can help security transition to a proactive resource and strategic business partner that plays a key role in business growth. Effective use of predictive solutions (especially for physical security) focuses priorities to mitigate the largest security threats first, and in doing so, focuses spending to help make operations efficient.

Predictive Solutions

Descriptive analytics looks at what already has happened; predictive analytics uncovers what is likely to happen in the future. It is the branch of data mining concerned with understanding probabilities and trends with an eye to guiding decisions. Data modeling and forecasting are used to determine future possibilities allowing you to move towards the best possible outcome.

The ability to model, anticipate and predict has been made easier with recent technological breakthroughs that can manage and make sense of vast amounts of unrelated data. Predictive analytics analyzes large amounts of data with different variables; it includes complex mathematical algorithms to turn large data stores into knowledge and insight instantly.

Benefits of Predictive Solutions

Smart organizations don't just gather and report information – they leverage business analytics, and the benefits are visible across many departments. Retail firms use analytics to increase cross-selling opportunities by analyzing customer purchase behavior. Banking and financial services firms use analytics to reduce fraud. Sports teams study statistics to drive personnel decision making to win more games.

Organizations adopting more sophisticated analytical approaches is a rapidly growing trend.

Challenges in Adoption

Some of the key challenges that organizations perceive about the adoption of predictive solutions are as follows:

Lack of Quality Data

The most common perceived issue is the lack of quality data to derive trustable output from predictive solutions. The various systems and devices generate massive amounts of data, but because the information exists in so many different buckets, and because the correct data isn't always retained, collection is difficult. This slows down decision making capability and could cause decisions to be made with a high amount of uncertainty without visibility to the entire dataset.

To ensure that the data is accurate, organizations should make sure that the predictive system chosen establishes consistency among the disparate systems continuously by planning, owning, managing, scheduling and controlling the data synchronization process.

> *"An automated response to an IOC helps take timely action to prevent threats and increases security departments' efficiencies."*

Lack of Expertise and Understanding

Lack of experience and knowledge of successful predictive analytics applications is another key barrier preventing organizations from switching to predictive solutions, although hardly an insurmountable one. However, an even greater risk is created when consultants poorly understand the needs of the department. Many predictive projects have gotten off track due to the inability of the data scientists to understand the relevant questions.

To prevent any bottleneck because of inexperienced staff, organizations should seek out a partner with experience not only in predictive analytics but also in their department's business needs. Such a partner can help avoid both experience traps.

Perceived as an All or Nothing Proposition

Many organizations believe that despite the benefits that predictive analytics might provide, it as an all-or-nothing proposition requiring data or algorithmic perfection before actions can be taken. While a common approach is to first collect any and all data then apply advanced machine-learning tools and processes, this is far from the only approach.

A more immediately beneficial approach is the Top Five Approach. In this approach, the top five questions to answer or risks to address are implemented as the first short-term goals, while also building towards longer-term perfection.

Predictive Solutions for Physical Security

Predictive solutions for security help security transition from being a reactive resource to a proactive strategic business partner that plays an integral role in business growth. With the right investment in predictive solutions to leverage the benefit from physical security data, security organizations are provided with two key benefits:

- Ability to predict and prevent possible threats based on contextual analysis of data from multiple devices and systems

- More effective and efficient management of security operations processes after analysis of historical trends

Instead of treating data as alarms, predictive systems analyze data looking for statistical trends to measure which policies are effectively enforced, and which risk controls are ineffectively applied.

However, even though many enterprises understand the benefits of predictive analytics for security, they are only just now beginning to grasp the potential that predictive analytics have in the security sector. For instance, more than two-thirds of security directors consider it important to be able to do predictive analysis to improve operational effectiveness and reduce risk, yet just under one-third of them have technology in place to capture predictive security metrics . Even with this high level of interest, there is still work to be done. Many enterprises are neither equipped nor prepared to deploy predictive analytics initiatives focused on security.

Predictive Strategy

A smart predictive security strategy helps answer the following questions:

- What is the source of the next threat?
- Which assets are most vulnerable and likely to be targeted?
- What is the automated response to tackle the threat?
- Which processes need improvement?

Key Physical Security Terminologies

To achieve the goals mentioned above, each security organization must be familiar with some critical security terminologies:

Context-Aware Security

Context-aware security is the use of comprehensive security information from many systems to improve security decisions at the time they are made, resulting in more accurate security decisions capable of supporting dynamic business and environments.

Instead of spending on the technology directly, it is important for organizations to be aware of how and what context-aware security can do to support current and future business. Organizations should ensure that rather than deploying all possible controls, they shift to intelligent and adaptive placement of controls based on the context of the action being requested. The best way to prevent attacks is an integrated tool that performs continuous monitoring and tracking, provides appropriate data analysis and generates automatic responses to prevent any compromise in the physical security. All the systems and devices in the security architecture should share key contextual information and event logs with the integrating system to enable it to find correlations between two sets of information previously thought to be unrelated. For example, an HR anomaly correlated with a log-in time exception could immediately send an alarm to the security teams alerting them to a possible attack. Analysis of HR context information combined with time of day is now something modern predictive systems are able to capture and report.

[1] IDG Research Survey conducted October 21-November 3, 2014.

HID SAFE™ Analytics allows security organizations to predict and prevent possible threats based on contextual analysis of data from multiple security devices and systems.

It also enables organizations to manage their security business and operations processes effectively and efficiently by analyzing the historical trend.

Indicator of Compromise (IOC)

An IOC is an Indicator of Compromise or pattern that is used to identity a person, device (reader/site), or system that has a higher probability of becoming a threat than normal. IOCs provide early indications of bad actors, or deviation from norms that can help identify and contain security incidents before they result in loss.

Automated Response to Possible Threats

An indicator without an automated response associated with it is as good as a post mortem analysis. For instance, if the security operations center is not notified on time (via email or on their mobile devices), when an identity is attempting unauthorized access to a high-risk area multiple times, they won't be able to prevent that identity from causing damage. It is critical for the indicator to have an associated action.

An automated action runs in response to a growing risk and can generate alerts, execute pre-defined tasks, schedule audits, and send email. This avoids delays introduced by manual processes or multiple layers of review. Time to action is slashed by up to 95%. It also enables security analysts to increase efficiencies and provide more consistent response results. Table 1 shows a list of common IOC and the associated automated actions.

IOCs	Automated Response via Policy or Taken Manually
Multiple access denied for same person	• Send manager an email or STOP badge for N repeated attempts • Send email to person, e.g. "Click to request access"
Same badge at different geographical locations	• Send email to person checking, e.g. "Is that you?"
Multiple tailgate instances	• Complete security check of the identity against external and internal watch list databases.

Table 1: IOC and Corresponding Action

Risk-based Identity Monitoring

User activity monitoring is a critical part of active defense against security threats. However, monitoring every identity with the same lens is a high-cost yet ineffective proposition. For an effective security picture, an organization should evaluate identities based on their risk profile, derived from several different categories of information. First, the access profile is derived from the number and levels of access assigned to the identity. Behavioral data measures unusual behavior derived from IOC patterns. Process risk measures how well and how recently audits, background checks and other actions have been applied. Even external data such as HR data can be taken into account. Based on this risk profile, the security team might set different policies for different risk categories. For instance, mandating frequent background checks for high access profile identities as well as identities showing a sudden increase in their overall risk score.

The HID Global Approach to Predictive Security

HID SAFE™ Analytics enables organizations to take the power of their physical security data beyond traditional reporting and use it to predict physical security operations and possible security risks. HID SAFE™ Analytics utilizes the logs maintained for each device and system and using predictive analytics, transforms this data into critical knowledge and actionable insights. These Indicators of Compromise (IOCs) not only help organizations save their operational expenditure but also enable preventive actions for a possible threat.

Data

The HID SAFE™ Analytics integration framework is readily able to connect to a large number of external systems and devices. Because of this, HID SAFE™ has the capability to easily gather data across multiple systems and analyze them to streamline security operations and prevent risk.

Methodology

HID SAFE™ Analytics assigns a risk score to each identity and area based on access and behavioral patterns and allows simple actions to be tied to high or quickly changing risk profiles.

Key Features

- Identify the highest probability risks in time
- Automate appropriate actions
- Minimize security and compliance risks
- Maximize the value of limited budgets by addressing highest needs first

Risk Summary Dashboard

HID SAFE™ Analytics includes the risk summary dashboard, which gives a birds-eye view of all the potential risks associated with an identity in the system. This view takes into account multiple IOCs that affect risk and computes an overall score for the identity based on weights assigned for each IOC parameter. The impact of these IOCs on the overall risk score can also be customized as per organization requirements.

IOC Dashboards

The assessment of risks based on IOCs is divided into two categories:

Behavioral Analysis: Using behavioral analysis of access data, you can identify, understand and take measures to tackle deviant behavioral changes exhibited by identities. Behavioral analysis establishes patterns for every identity and every device in the system in order to search for anomalies that indicate risk. A few important behavioral analysis criteria include:

- Erratic Movement: finds employees with unusual pace of movement
- Unusual Timing: finds employees who are arriving or departing at unusual hours
- Tailgating: finds employees who explore areas by following others who have access (piggybacking), or who hold doors open for others
- Zombie Badge: finds people who use a deactivated access card of an ex-employee
- Card Fraud: finds employees who have either willingly given their credentials to others or whose cards have been stolen and can be potentially misused
- Badge Fishing: finds employees who are exploring places that are not relevant to them or places where they don’t normally go

Expert Indicators: This approach relies on characteristics that identities possess which give scope for a potential misuse or threat. The risk measures here are defined by estimating the assets/access that an identity possesses and evaluating it against the need for such privileges.

- Pack-Rat: finds employees in possession of unusually large amounts of unused access or unnecessary assets
- Privileged User: finds employees with unusually extensive access or control of assets

Benefits

Predictive security, compliance and risk management provided by HID SAFE Analytics delivers business value through the following benefits:

- Increased efficiency: By replacing multiple special-purpose appliances with centrally managed security, organizations save a lot on the capital expenditure and increase the visibility over the security infrastructure.
- Agility: Automating the entire security operations centrally enables security with an agile platform for a faster, flexible response.
- Improved Business Alignment: Metric driven management leads to spending that is supported and in alignment with business goals
- Reliability: Predictive security helps address numerous vulnerabilities from various identities, devices and external threats. The centrally managed systems gather information from the users and devices to keep the organization full informed and proactive.

2018-08-02-iams-hid-safe-analytics-wp-en
PLT-04008