Leveraging Identity Data in Cyber Attack Detection and Response

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Leveraging Identity Data in Cyber Attack Detection

As organizations break away from traditional network-based security concepts, where zones are delegated "trusted" or "untrusted," to people-centric security models like Zero Trust, identity is becoming intrinsically linked to security. In fact, identity data can help security teams determine whether users or organizations are being subject to a cyber attack. This whitepaper will outline what and how identity data can be used as an indicator of a cyber attack, as well as ways to respond to incidents using Identity and Access Management (IAM) systems.

Identity Data Sources

Identity data can be broadly broken down into two main categories: 1. data associated with a user and 2. data associated with the identity and access management (IAM) system itself. Both types of data can be leveraged in the detection and investigation of cyber incidents.

User Activity

User data that is tracked and logged by IAM providers give a detailed view of each user's activity. Applications accessed, time of access, login attempts, and location or IP address of login are some of the information typically tracked by identity providers. By understanding how users typically work, security teams can discover suspicious user activity.

Suspicious user activities to look for can include:

- Access to applications the user typically does not access
- Password changes or resets
- Changes to or removal of multi-factor authentication (MFA) factors. For example, removing MFA requirements, changes to security question answers, or changing the phone number for SMS-based MFA challenges
- Multiple failed login attempts or account lockouts

The challenge of monitoring user data, however, is the amount of data. Each user, through the course of the day, can potentially produce hundreds of logged events. Multiply that by the number of users in the organization, and the amount of data to sift through becomes quite daunting.

In addition, examining user data for suspicious events requires some level of baseline to know what "normal" activity looks like. Normal activity may also vary by user group or regions. For example, access to Salesforce may be typical for users in a marketing group and atypical for users in engineering. Similarly, logins after 5pm may be normal behavior for global support teams on shifts and less typical for corporate HR teams.

Finally, user activity alone may not be sufficient to determine whether an organization is under attack. Suspicious events may prove to be false positives, as there are legitimate reasons why users may do any of the listed suspicious activities. For example, new devices may prompt MFA factor changes, and a return from vacation can result in forgotten passwords and failed login attempts.

While caution is recommended when evaluating user activity data, the data is still valuable. Taken with context and used with other indicators, user activity can be a piece of evidence pointing to an attack. Multiple suspicious user activities within a specific timeframe can also be indicators of a breach. For example, a password change combined with a MFA factor change, during an atypical login time, from a new IP address, would be a strong indicator of suspicious behavior. The value of user activity data is often also realized in later phases of security investigations, when an attack has been confirmed and security teams are piecing together exactly what occurred.

A Note on Privileged Users and Admins

Despite limitations in user activity data, there are two types of users whose activities warrant closer scrutiny: privileged users and admins.

A privileged user is able to perform security-related functions that a normal user would not have authorization to perform. They are often, but not always, admins. Because these users have the access and ability to change security policies, they are coveted targets for attackers. In fact, one of the goals of an attacker is to obtain access to a privileged user or admin account so they can make security changes without detection. Thus, any unusual activities performed by a privileged user or admin should be carefully monitored to ensure there has not been an account compromise or malicious intent.

Identity System Data

The second, and perhaps more important, category of data for security teams to be aware of is data from the identity platform itself.

IAM system log data to monitor for suspicious activity includes:

- Creation of new admins
- Modification/escalation of privileges for admins
- Creation/modification of network zones
- Creation of new API tokens
- Sign-on policy or MFA policy changes
- Creation of new user groups or additions of applications to existing user groups

These activities typically do not occur on a daily basis, making it easier for security teams to track. In addition, most activities that involve changes to the identity system are typically done by IT teams during a planned maintenance timeframe or have associated issue-tracking tickets. By correlating event logs with planned maintenance periods or tickets, security teams can determine whether these activities are part of normal operations or if additional investigation is required.

Correlation and High Value Indicators of Attack

Once any unusual user or system activity is discovered, use that event as a starting point for a broader investigation. For example, when atypical user activity occurs, check the location of logins associated with that user to ensure there's no obvious related suspicious event, like logins from unaffiliated countries Looking at all events associated with a session can also help surface related suspicious activities.

> For a list of Okta events to monitor, including user activity and Okta system events, refer to the "Okta Event Types of Interest for Security Teams" cheatsheet.

To find patterns and high-value indicators at scale, a log or security analysis tool can also be helpful. Correlated identity events that may point to an attack or attacker performing reconnaissance may include:

- IPs making high login attempts with invalid usernames
- High (i.e. greater than 90%) login failure rates
- Multiple users locked out within a short period of time

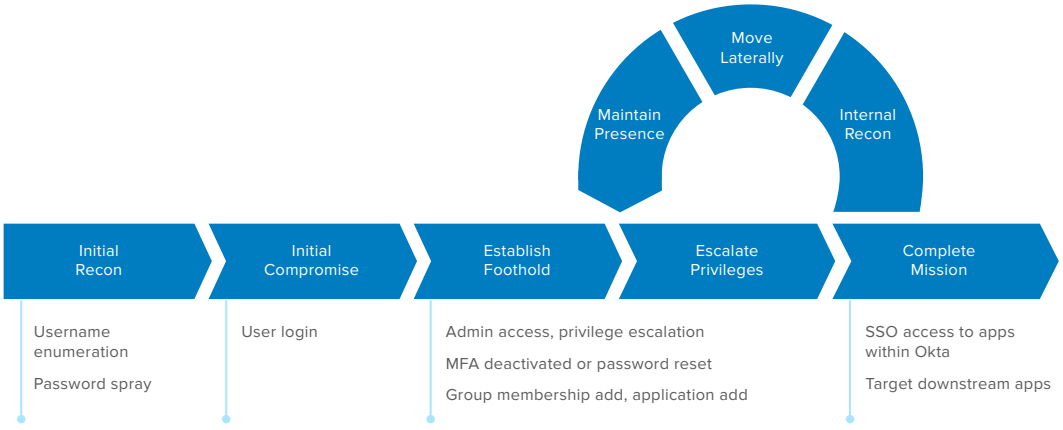
Identity and the Attack Lifecycle

Most cyber attacks follow a typical attack lifecycle, and it can be helpful to map discovered malicious behaviors to this lifecycle to understand the current stage of attack, prepare for the attacker's next moves, and prioritize response. Knowing which stage an attack is in drives what security teams should look for, while anticipating the attacker's next moves helps teams to keep an eye out for specific associated with later stages. The user and identity system activities mentioned in the previous sections can all be mapped to corresponding stages of the attack lifecycle.

The example below shows possible activities to look for in the IAM logs for each attacker lifecycle stage.

Using Identity to Respond to Cyber Incidents

Not only can identity data help security teams detect whether the organization is under a cyber attack, but if one occurs, IAM solutions can aid in responding to a cyber incident.



Identity events in the attacker lifecycle

The first step after a confirmed attack is to contain it to prevent progression and minimize losses. IAM systems can help prevent additional unauthorized access to applications. A compromised user account can be “locked down” by either adding the user to a user group with very limited access to applications, or by suspending the user’s account temporarily. Single Sign-On (SSO) sessions can also be terminated.

Security teams should take care to understand which apps are being used, however, as it is possible that killing the identity session does not immediately terminate access to all downstream applications—especially if existing access tokens are still valid.

Network and policy changes to the IAM system are additional tactics that can help slow an attack. Organizations may choose to allow access to the identity system by whitelisting allowed IP addresses only, or they may blacklist unwanted IPs or locations. SSO and MFA policy aggressiveness may also be increased. For example, forcing users to re-login, reducing the time interval between required SSO logins, and increasing MFA prompts are all steps that can help prevent additional unauthorized access in the wake of an attack. In fact, it is recommended to increase security measures like these once an attack has been discovered, as attackers will often attempt to regain access. Likewise, security teams should also prepare for associated attack campaigns like increased phishing attempts.

Conclusion

With logins and access to applications painting a granular picture of an organization’s activities, identity becomes a valuable data source for the detection and investigation of suspicious activities that may be indicators of a cyber attack. By correlating identity data with that of other security and network systems, organizations can glean additional information to confirm the existence of malicious activity. Once confirmed, identity systems can then also be used to contain users and limit access.

As the leading enterprise identity provider, Okta can provide organizations with the visibility to detect and respond to cyber incidents. And with over 5,500 pre-built integrations within the Okta Integration Network, Okta integrates with other security tools and provides seamless support to business applications. Okta helps users connect securely to the tools they need and provides security teams with the ability to manage enterprise security. To find out more on how Okta’s solutions can be leveraged by cyber security teams to detect, prevent, and respond to incidents, visit okta.com.


okta