ManageEngine
Log360

USE CASE

Using Log360 to detect account compromise

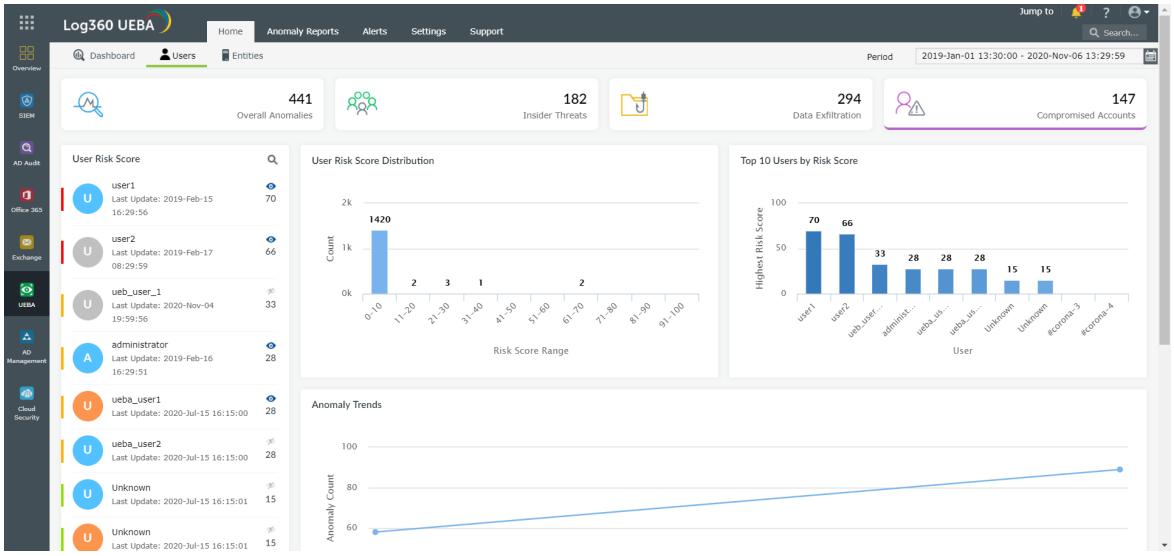
www.manageengine.com/log-management

Using Log360 to detect account compromise

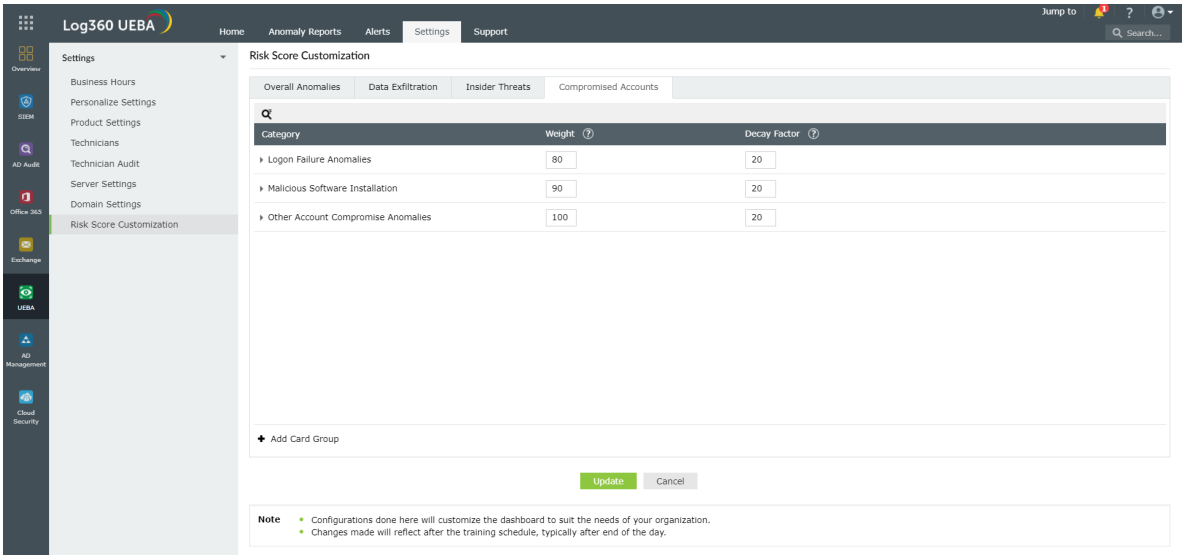
Are people really who they say they are? In cybersecurity as in life, it really is a tough call. What makes an account compromise so difficult to detect is that the actions of a hacker originate from a legitimate user account within the organization. Once an account is compromised, even a malicious act that can take down the network might not immediately raise red flags. The higher the privileges of a compromised account, the greater the risk. One possible way to discover an account compromise is to detect anomalies in established usage patterns within an organization. To detect anomalies in usage, calculating the normal patterns of users and entities first is crucial.

Leveraging machine learning to detect account compromises

Log360 comes with a user and entity behavior analytics (UEBA) add-on that can detect anomalies in user behavior and spot account compromises. This add-on uses unsupervised machine learning (ML) algorithms to ascertain the normal behavior of users and entities, then detects any deviations or anomalies from that.



The Log360 UEBA add-on detects account compromise by taking into account multiple factors, such as anomalous logins, malicious software installations, and abnormal file changes. The key factors that can indicate possible account compromise scenarios in your environment will be grouped under three major categories.

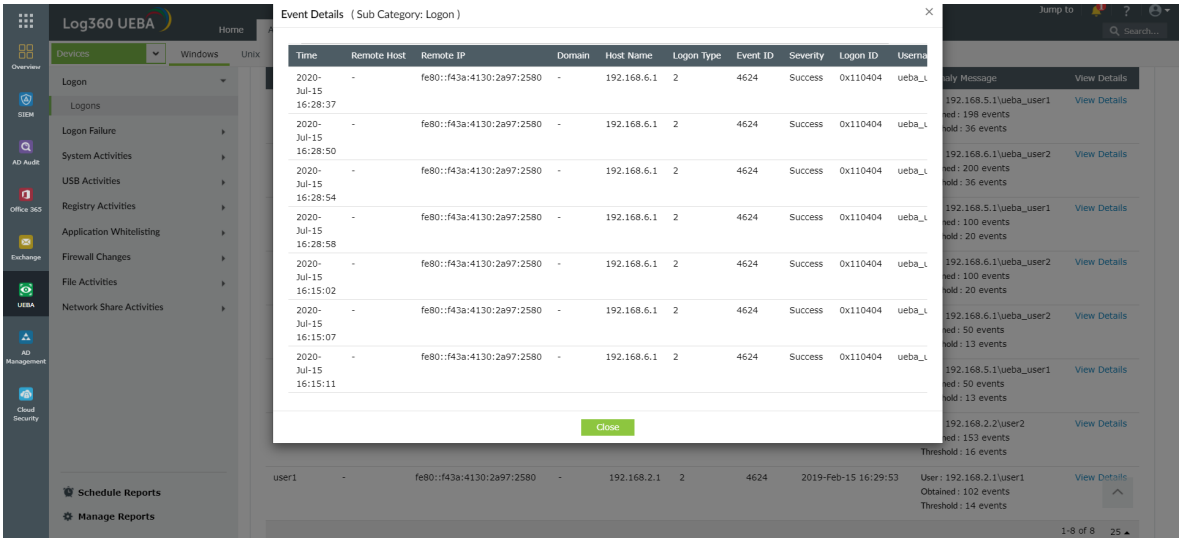


- **Logon Failure Anomalies:** The security analytics dashboard of this category presents you with details of unusual logon failures; unusual logons on applications, servers, or workstations; and more.

- **Malicious Software Installation:** Instances of modifications to the Windows Registry, abnormal service installations, and unusual process creation will be tracked here.

- **Other Account Compromise Anomalies:** In this dashboard, instances of multiple file modifications, account lockouts, and system changes will be listed.

Investigating account compromises



To help in the investigation of account compromise, Log360 can also provide a complete timeline of all user activities to discover what occurred and who the culprit is. The solution has exhaustive analytical dashboards and alert profiles on user logon reports, logon failures, Active Directory activity, member server logon activity, workstation logons, and more. These reports and the graphical dashboards help you investigate a specific event and the associated incident to determine if there was a compromise in a user account.

Apart from account compromises, Log360 can also spot data exfiltration, insider threats, and other advanced persistent threats. The solution's intuitive security analytics dashboard provides you with the insights on the users and entities with the highest risk scores, behavioral trends, watchlisted users, and more. It also helps you quickly drill down and investigate anomalous events.

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities. For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.