



Using Log360 to detect account compromise



ManageEngine

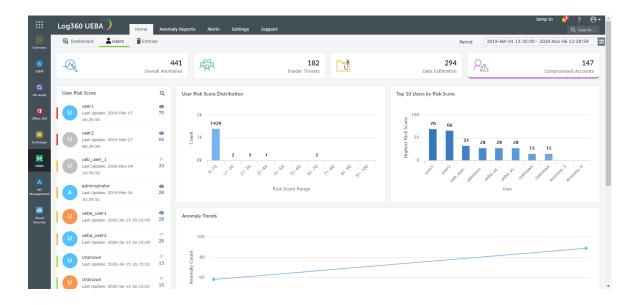
Log360

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.

	Log360 UEBA	ne Anomaly Reports Alerts Settings Support			Jump to 🤌 ? 😖 - Q. Search							
Overview	Settings •	Risk Score Customization										
SIEM	Business Hours Personalize Settings	Overall Anomalies Data Exfiltration Insider Threats	Compromised Accounts									
Q	Product Settings Technicians	Category	Weight 🕐	Decay Factor (?)								
AD Audit	Technician Audit	Logon Failure Anomalies	80	20								
	Server Settings Domain Settings	Malicious Software Installation	90	20								
Office 365	Risk Score Customization	+ Other Account Compromise Anomalies	100	20								
Stange Stange												
O UEBA												
AD Management												
Cloud Security												
		+ Add Card Group										
			Update Cancel									
	Note • Configurations done here will customize the dashboard to suit the needs of your organization. • Changes made will reflect after the training schedule, typically after end of the day.											

- 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.

*	2020- Jul-15 16:28:37 2020- Jul-15		fe80::f43a:4130:2a97:2580	-	192.168.6.1	2	4624	Success	0x110404	ueba_u	aly Message	View Details
	16:28:37											
• •											192.168.5.1\ueba_user1 ned: 198 events	View Details
		-	fe80::f43a:4130:2a97:2580	-	192.168.6.1	2	4624	Success	0x110404	ueba_u	hold : 36 events	
	16:28:50							_			192.168.6.1\ueba_user2 med: 200 events	View Details
•	2020- Jul-15 16:28:54	-	fe80::f43a:4130:2a97:2580	-	192.168.6.1	2	4624	Success	0x110404	ueba_u	hold : 36 events	
	2020- Jul-15 16:28:58	-	fe80::f43a:4130:2a97:2580	-	192.168.6.1	2	4624	Success	0x110404	ueba_u	192.168.5.1\ueba_user1 ned: 100 events hold: 20 events	View Details
•	2020-		fe80::f43a:4130:2a97:2580		192.168.6.1	2	4624	Success	0x110404	ueba_u	192.168.6.1\ueba_user2	View Details
•	Jul-15 16:15:02										hed: 100 events hold: 20 events	
es >	2020- Jul-15 16:15:07	-	fe80::f43a:4130:2a97:2580	-	192.168.6.1	2	4624	Success	0x110404	ueba_u	192.168.6.1\ueba_user2 ned: 50 events	View Details
	2020-		fe80::f43a:4130:2a97:2580	-	192.168.6.1	2	4624	Success	0x110404	ueba_u		
	Jul-15 16:15:11										192.168.5.1\ueba_user1 ned: 50 events nold: 13 events	View Details
				_	Close						192.168.2.2\user2	
	ng >	16:28:54 16:28:54 10:28:58 10:128:58 10:128:58 10:128:58 10:15:07 10:	ide: 2020- 2020- 2020- 16:28:58 2020- 2020- 16:128:58 2020- 16:15:02 2020- 16:15:02 2020- 14:15:07 2020- 2020- 14:15:07 2020-	ne 16:28:54 2020 fe80::f43a:4130:2a97:2580 Jul-15 2020 fe80::f43a:4130:2a97:2580 Jul-15 2020 fe80::f43a:4130:2a97:2580 Jul-15 2020 fe80::f43a:4130:2a97:2580 Jul-15 2020 fe80::f43a:4130:2a97:2580 Jul-15 2020 fe80::f43a:4130:2a97:2580 Jul-15	ne 102-354 1022654 2020- 6 fe80::f43a:4130:2a97:2580 - 102:23:58 2020- 7 fe80::f43a:4130:2a97:2580 - 102:15:02 2020- 7 fe80::f43a:4130:2a97:2580 - 102:15:02 2020- 7 fe80::f43a:4130:2a97:2580 - 102:15 2020- 7 fe80::f43a:4130:2a97:2580 - 102:15	ne 16:28:54 2020 fe80:;f43a:4130:2a97:2580 - 192.168.6.1 Jul-15 2020 fe80:;f43a:4130:2a97:2580 - 192.168.6.1 2020 fe80:;f43a:4130:2a97:2580 - 192.168.6.1 Jul-15 2020 fe80:;f43a:4130:2a97:2580 - 192.168.6.1 Jul-15 2020 fe80:;f43a:4130:2a97:2580 - 192.168.6.1 Jul-15	ne 16-28:54 16-28:54 2020 fe80::f43a:4130:2897:2580 - 192.168.6.1 2 M-15 2020 fe80::f43a:4130:2897:2580 - 192.168.6.1 2 2020 fe80::f43a:4130:2897:2580 - 192.168.6.1 2 2020 fe80::f43a:4130:2897:2580 - 192.168.6.1 2 2020 fe80::f43a:4130:2897:2580 - 192.168.6.1 2 2020 fe80::f43a:4130:2897:2580 - 192.168.6.1 2	16:28:54 2020- - fe80::f43a:4130:2897:2580 - 192.168.6.1 2 4624 16:15:002 - fe80::f43a:4130:2897:2580 - 192.168.6.1 2 4624 16:15:002 - fe80::f43a:4130:2897:2580 - 192.168.6.1 2 4624 10:1-15 - fe80::f43a:4130:2897:2580 - 192.168.6.1 2 4624 10:1-15 - fe80::f43a:4130:2897:2580 - 192.168.6.1 2 4624	ne 12:28:54 10:28:54 2020 fe80:f43a:4130:297:2580 - 192.168.6.1 2 4624 Success 10:15 02 10:15 02 1	16:28:54 16:28:54 2020- 680::f43a:4130:2897:2580 192.168.6.1 2 4624 Success 0x110404 2020- 7 fe80::f43a:4130:2897:2580 - 192.168.6.1 2 4624 Success 0x110404 2020- 7 fe80::f43a:4130:2897:2580 - 192.168.6.1 2 4624 Success 0x110404 161:15:002 2 62020- 7 fe80::f43a:4130:2897:2580 - 192.168.6.1 2 4624 Success 0x110404 161:15:002 2 62020- 7 fe80::f43a:4130:2897:2580 - 192.168.6.1 2 4624 Success 0x110404 161:15:002 2 62020- 7 fe80::f43a:4130:2897:2580 - 192.168.6.1 2 4624 Success 0x110404 161:15:002 2 62020- 7 fe80::f43a:4130:2897:2580 9 192.168.6.1 2 4624 Success 0x110404 10:1-15 2 6202 5	All 324 All 324 All 324 All 324 All 324 All 32 All 32 A	16:28:54 2020-5 - fe80:1f43a:4130:2a97:2580 - 192.168.6.1 2 4624 Success 0x11040 ueba_L 41:00 events 16:15:02 - fe80:1f43a:4130:2a97:2580 - 192.168.6.1 2 4624 Success 0x11040 ueba_L 40:10 events 40:10 eve

Investigating account compromises

ManageEngine

Log360

USE CASE

USE CASE

ManageEngine

Loq360

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.

Gartner's Peer Insights Voice of the Customer 2023 is out!

ManageEngine named a Customers' Choice for SIEM

Check out why

Latest Gartner Magic Quadrant for SIEM is out!

ManageEngine recognized in Gartner's Magic Quadrant for Security Information and Event Management, 2020.

Get the report

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.

ManageEngine

\$ Get Quote

± Download