

Mitigating Privilege Escalation Attack by User Behaviour Analytics and Threat Hunting



Snapshot

Client Industry:	ATM Service Provider
Country:	UAE
Challenge:	A privilege escalation attack that could have caused a serious data compromise
Solution:	On-time threat detection with User Behaviour Analytics and threat hunting
Benefit:	Fighting against a potential breach and building a sophisticated security posture

The Challenge

Today, organizations are digitally evolving by choosing among diverse technology options to store business-critical data. On the other side, the cyber threat landscape is expanding geographies and constantly looking for vulnerabilities in the security layers to perform security compromises. Cyber attackers are consistently staying a step ahead than the security measures taken by organizations and succeeding in their data breach menace.

Amongst the most infamous cyber-attacks, privilege escalation attacks occupy a top place. They are used to escalate the privileges of vulnerable user accounts to gain higher access benefits, restricted to authorized users of an organization.

A similar challenge was faced by one of SISA's clients, where a brute force attempt followed by a vertical privilege escalation incident were detected by SISA's threat hunting team.

Every time intruders do not get to their target directly when they compromise a user account. Different users of an organization can have different access policies. The adversary may need to perform privilege escalation to upturn privileges of a compromised user to gain access to targeted information.

Brute forcing is a type of trial and error method to identify the access credentials of users and access the user accounts, exclusive to an organization. Password guessing software is used in brute-forcing to generate multiple access-key guesses. Once, the desired value is obtained, adversaries can compromise the sensitive data present in the compromised account or can perform privilege escalation to gain higher benefits, restricted to authorized parties.

Threat Detection with User Behaviour Analytics

While monitoring the client's environment as part of security operations, SISA's Threat Hunting team received high-alert notifications from SISA EOT (Eye of Tiger), an in-built SIEM tool by SISA. EOT warned about a brute force attempt consisting of a series of failed login attempts followed by a successful login. The Threat Hunting confirmed the presence of an adversary in the client environment and started investigation on the issue immediately. SISA's Threat Hunting team applied User Behavior Analytics (UBA) to study the historic log patterns generated for the user account to identify malicious traffic and its lateral movement.

The User Behaviour Analytics showed that an employee's account with higher privileges restricted to administrative level users. Using UBA, SISA hunted for the adverse activity and confirmed the occurrence of privilege escalation and the lateral movement of an intruder.

SISA's Proactive Threat Mitigation

After hunting the threat successfully, SISA notified the client with a high alert warning about the adverse activity along with necessary action points to mitigate the adversary. Standing with the client throughout the threat mitigation process, SISA helped them in the closure of all action-points.

The action points included setting up user account policy with more firm guidelines to restrict data usage to authorized users and those with a true business need. Then, SISA helped the client to revoke access to compromised user accounts.

The proactive Threat Hunting and Mitigation helped the client in securing their organization from a potential cyberattack within no time.

"The expertise that SISA's Threat Hunting team has gotten over the years made it possible to timely detect the adverse activity potential enough to cause severe damage to the entire organization in one go."

User Behaviour Analytics for a Better Security Posture

Increasing cyber-attacks bring up a serious need for organizations to monitor network architecture and detect suspicious activities with a SIEM solution. Security monitoring helps in log analysis of network components such as servers, hosts, and apps and to study user behavior patterns.

SISA's EOT is one such SIEM solution with cutting edge capabilities to study user behavior patterns, correlate to events, and analyze network components. EOT is managed by SISA's Threat Hunting, who abides by the brand promises viz, True Security, Fanatic Support, and On-time delivery to achieve security excellence.

With all these features, SISA's threat hunting team has helped the client in detecting the biggest threat and eliminating it from the environment completely.