Detection Strategy for Forged SAML Tokens, Detection Strategy DET0148

Archived: 2026-04-05 12:34:35 UTC

AN0418

Forged SAML tokens can be observed as authentication attempts with valid signatures but missing expected preceding Kerberos or authentication events. Defenders may correlate SAML assertions with absent Event IDs 4769, 1200, or 1202, or tokens issued with abnormal lifetimes, issuers, or claims compared to baseline.

Log Sources

Mutable Elements

Field	Description
TokenLifetimeThreshold	Defines the maximum expected lifetime of a SAML token (e.g., >1 hour considered anomalous).
TrustedIssuerList	List of approved SAML issuers and certificate thumbprints.

AN0419

Forged SAML tokens in IaaS environments often manifest as cross-cloud or cross-account authentication without matching STS events. Defenders may see AssumeRole or GetFederationToken API usage without a corresponding SAML assertion log from the trusted IdP.

Log Sources

Mutable Elements

Field	Description
CrossAccountUsage	Flag SAML tokens used across unexpected accounts or cloud tenants.

AN0420

Forged SAML tokens may be used on Windows systems to authenticate to federated apps without normal Kerberos activity. Defenders may detect anomalous event correlation, where access to SaaS/O365 via SAML occurs without prior TGT requests or user logons.

Log Sources

Mutable Elements

Field	Description
ClaimAnomalyThreshold	Number of unusual claims in a SAML token (e.g., excessive privileges).

AN0421

Forged SAML tokens can appear as SaaS logins where authentication succeeded without MFA, or where tokens contain claims inconsistent with the user profile. Look for concurrent sessions across different geographies with the same SAML assertion ID.

Log Sources

Mutable Elements

Field	Description
GeoVelocityThreshold	Triggers when same SAML token used in different geographies within short timeframe.

AN0422

Forged SAML tokens may be leveraged to access O365 apps such as Outlook or SharePoint. Defenders should monitor for token replay across multiple clients or access attempts to privileged mailboxes without prior interactive login.

Log Sources

Mutable Elements

Field	Description
ReplayDetectionThreshold	Number of times a token is reused within short timeframe.
