Technical White Paper

IT / IOT Devices / Data Center
Device Security

SIEM and PLATFORM LIFECYCLE ASSURANCE

ADDING "BELOW the OS" PLATFORM INTEGRITY MONITORING TO SIEM

Authors

TOM DODSON

Supply Chain Security Architect

JERRY YU

Cloud Security Architect

SIEM / Intel® Platform Lifecycle Assurance

SIEM is a crucial component of an organization's security framework. It collects, analyzes, and correlates data across the network to provide real-time analysis and a holistic view of potential security incidents throughout the fleet. SIEM solutions have become an integral part of the network and data security ecosystem and are critical in tackling advanced and targeted cyberattacks. Traditional security information and event management (SIEM) tools have limited visibility into platform integrity and "Below the OS".

Intel® Transparent Supply Chain Platform Lifecycle Assurance (PLA) provides enhanced security and integrity solutions for enterprises by combining continuous "Below the OS" monitoring with in-depth insights and lifecycle management. The solution ensures that hardware and firmware components remain compliant and optimized, helping to safeguard enterprises against emerging threats and operational inefficiencies.

Intel® PLA offers REST APIs that enable organizations to add monitoring for below-the-OS threats to their existing SIEM dashboards.

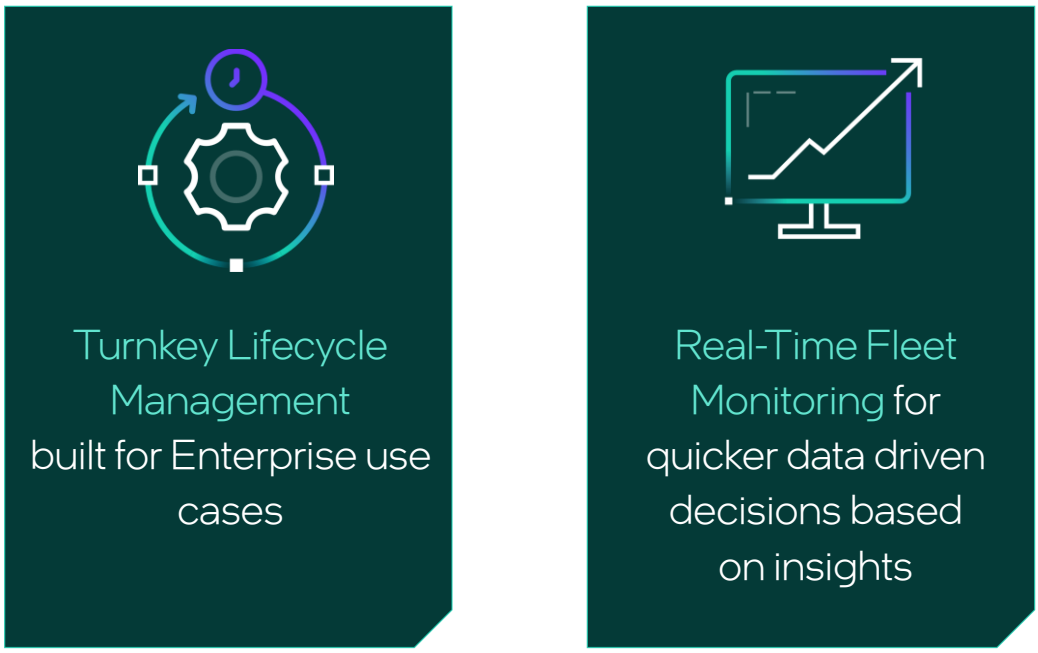
Platform Lifecycle Assurance Overview

From Deployment through Decommission Intel® PLA addresses the IT Fleet Administrators' key pain points by providing Enterprise Level ongoing fleet monitoring to validate the security posture of enterprise assets, detecting any deviations or issues that may compromise their integrity and compliance throughout the platform's lifecycle.

Enterprise IT Turnkey Lifecycle Management

Intel® PLA as a SaaS platform, scales effortlessly as you grow, offering powerful features with simple onboarding—no hidden complexities to deal with.

- Hosted SaaS Offering or deployable on-prem*
- Single pane of glass for simplified management of all assets throughout the lifecycle.
- Optional APIs designed to integrate with existing ISV solutions
- Role based access controls
- Multi-Tenant for Enterprise device segmentation or Managed Service Providers
- Automated Backups and Disaster Recovery



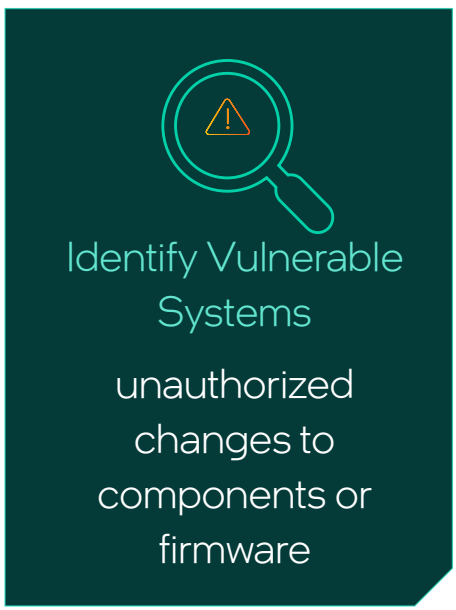
Intel® TSC Platform Lifecycle Assurance

Real-Time Security Monitoring

Intel® PLA provides **real-time security monitoring**, continuously keeping an eye on both hardware components and firmware. This means you can ensure the integrity of your platforms from deployment all the way to decommissioning. Intel® PLA actively checks and validates the security posture of your enterprise assets, quickly identifying any issues that might compromise their integrity and compliance.

Detection of the Vulnerable Systems

First off, Intel® PLA **detects vulnerable systems**, helping you spot insecure components and outdated firmware before attackers can exploit them. This proactive approach can significantly cut down the risk of data breaches and security incidents.





Security Postures and Policy Compliance

Intel® PLA also provides **compliance detection**. PLA continuously assesses your IT Fleet compliance with established IT standards and regulations, catching any non-compliance issues in real time. Many areas of the banking and financial sector require ongoing Compliance Audits.

Platform Lifecycle Assurance

Visibility, Traceability, and Lifecycle Management

Let’s dive into turnkey lifecycle management with our hosted SaaS offering, designed to simplify the management of all your assets throughout their entire lifecycle.

At the heart of this solution is the "single pane of glass" interface, which provides a unified view for easy management of all your assets in one place. If you're using existing ISV solutions, our optional APIs integrate seamlessly with your current systems, enhancing workflows without requiring a complete overhaul.

Security is a top priority, and our role-based access controls ensure that only authorized users can access specific functions, maintaining compliance and safeguarding sensitive information. For Managed Service Providers, our multi-tenant architecture allows effective management of multiple clients while keeping their data secure and separate.

Additionally, automated backups and disaster recovery options protect your data and minimize downtime, ensuring quick restoration in the event of an issue.

In summary, our turnkey platform lifecycle management solution combines user-friendly features like unified management, seamless integration, robust security, multi-tenancy, and data protection, all designed to streamline operations and enhance resilience.

Initial Device Setup

Once the end user deploys the new equipment, a platform baseline, **Figure 1** shows the process for the Initial Device Setup. To initiate the Initial Baseline Device Setup, the Intel® Transparent Supply Chain Client (Intel® TSC Client) is loaded onto the Platform. The Intel® TSC Client application is then executed and will read the TPM Attributes, Platform Attributes and then sign the data. The signed Platform Baseline data is then uploaded to the Intel® Transparent Supply Chain Backend Cloud and stored in the Platform Evidence Database.

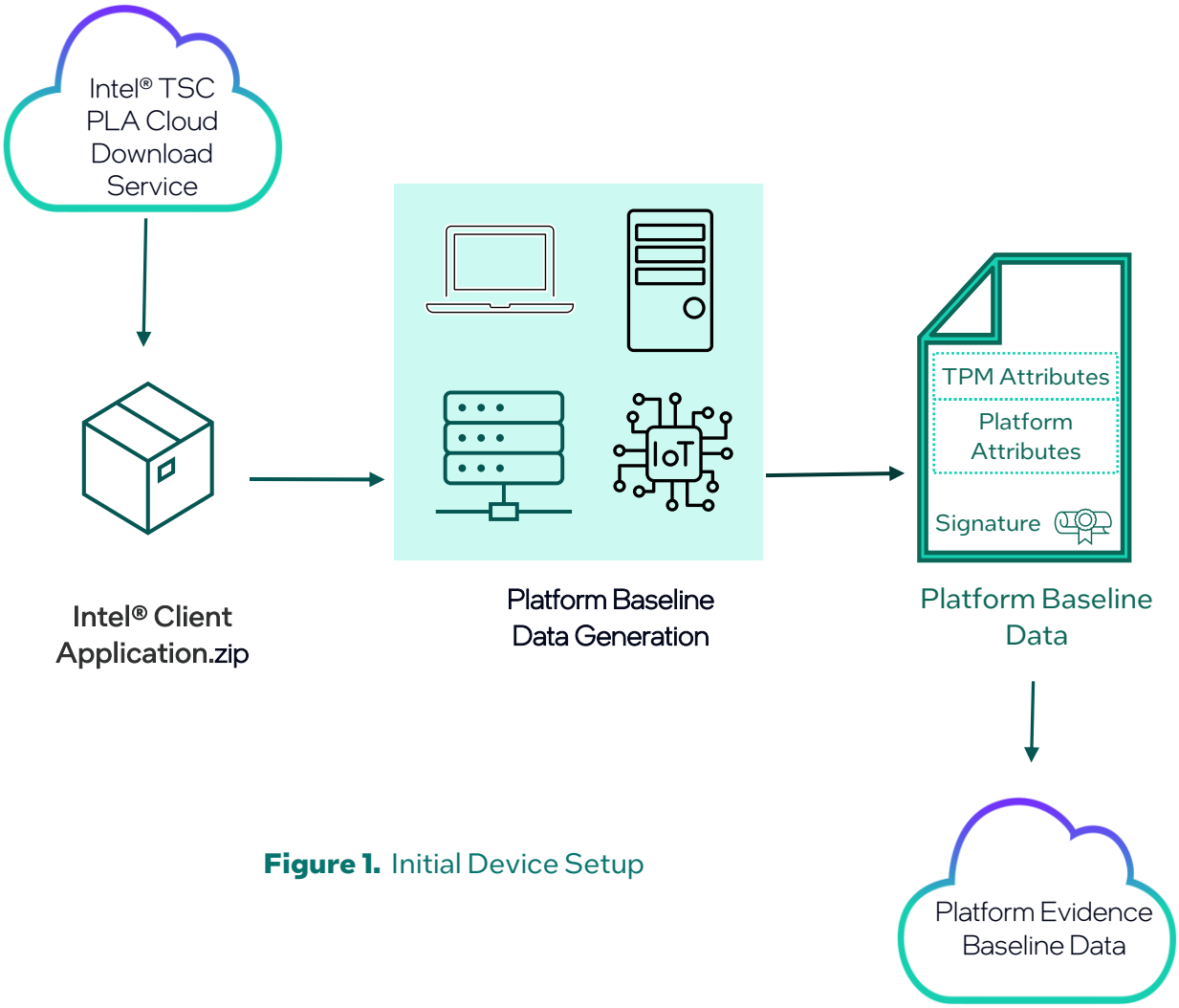


Figure 1. Initial Device Setup

Ongoing Device Management

Ongoing Device Management is the key feature of PLA. Using the Fleet Dashboard, Fleet managers can now monitor the compliance of their fleet in real time. **Figure 2** shows the process for Ongoing Device Management.

To initiate the Ongoing Device Management the IT Administrator will deploy an application that executes the Intel® TSC Client application. The Intel® TSC Client application will then take a snapshot of the platform and send the platform evidence to the Intel® Transparent Supply Chain Cloud backend.

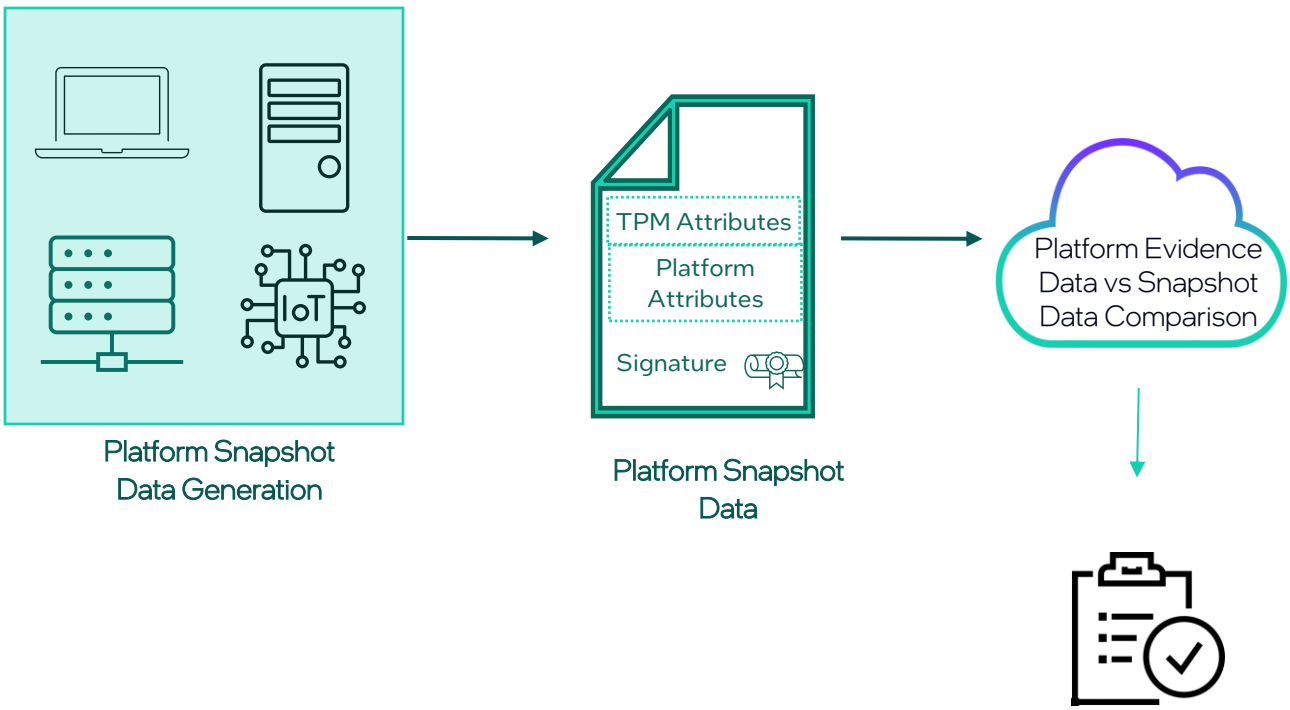


Figure 2. Ongoing Device Management

Managing Platform Lifecyle Integrity

Managing the Platform Lifecycle Integrity is the key feature of Intel® PLA. Using the Fleet Dashboard, Fleet managers can now monitor the compliance of their fleet in real time. Figure 3 shows the Platform Lifecycle Integrity Dashboard. The Intel® PLA Dashboard shows the status of the devices in the fleet by displaying the remote attestation records archived in the Intel® Transparent Supply Chain Cloud in the cloud.

The attestation record includes both the original attestation request, i.e. the device evidence data, and the attestation result, i.e., the token. The Enterprise tenant (device owner) is able to authorize the known changes to generate the new baseline of the device, or trigger needed action when specific device integrity is compromised, i.e., unexpected component changes are detected.

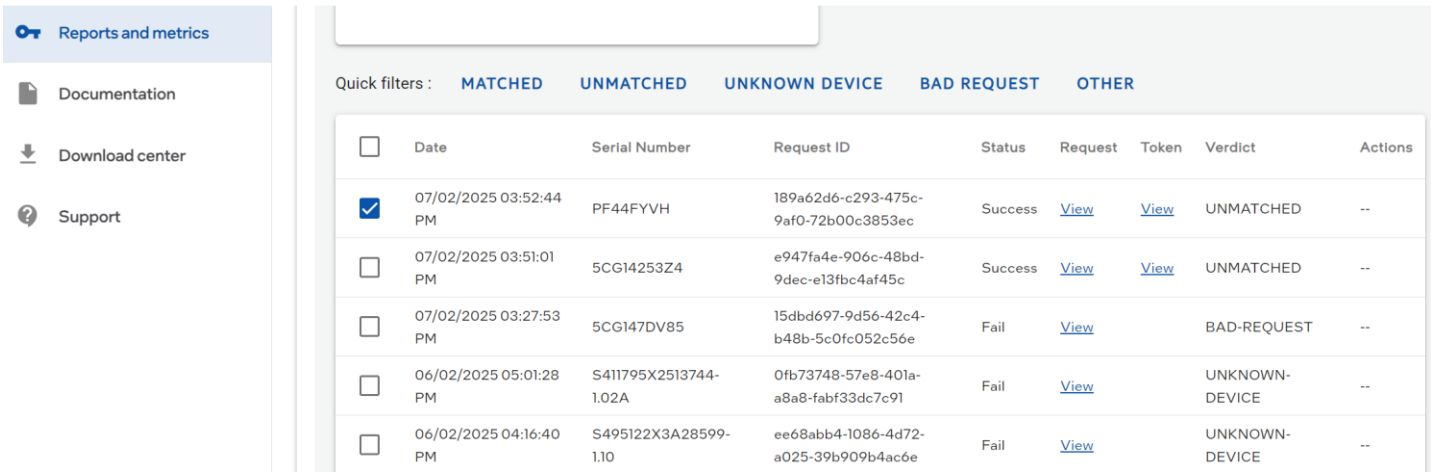
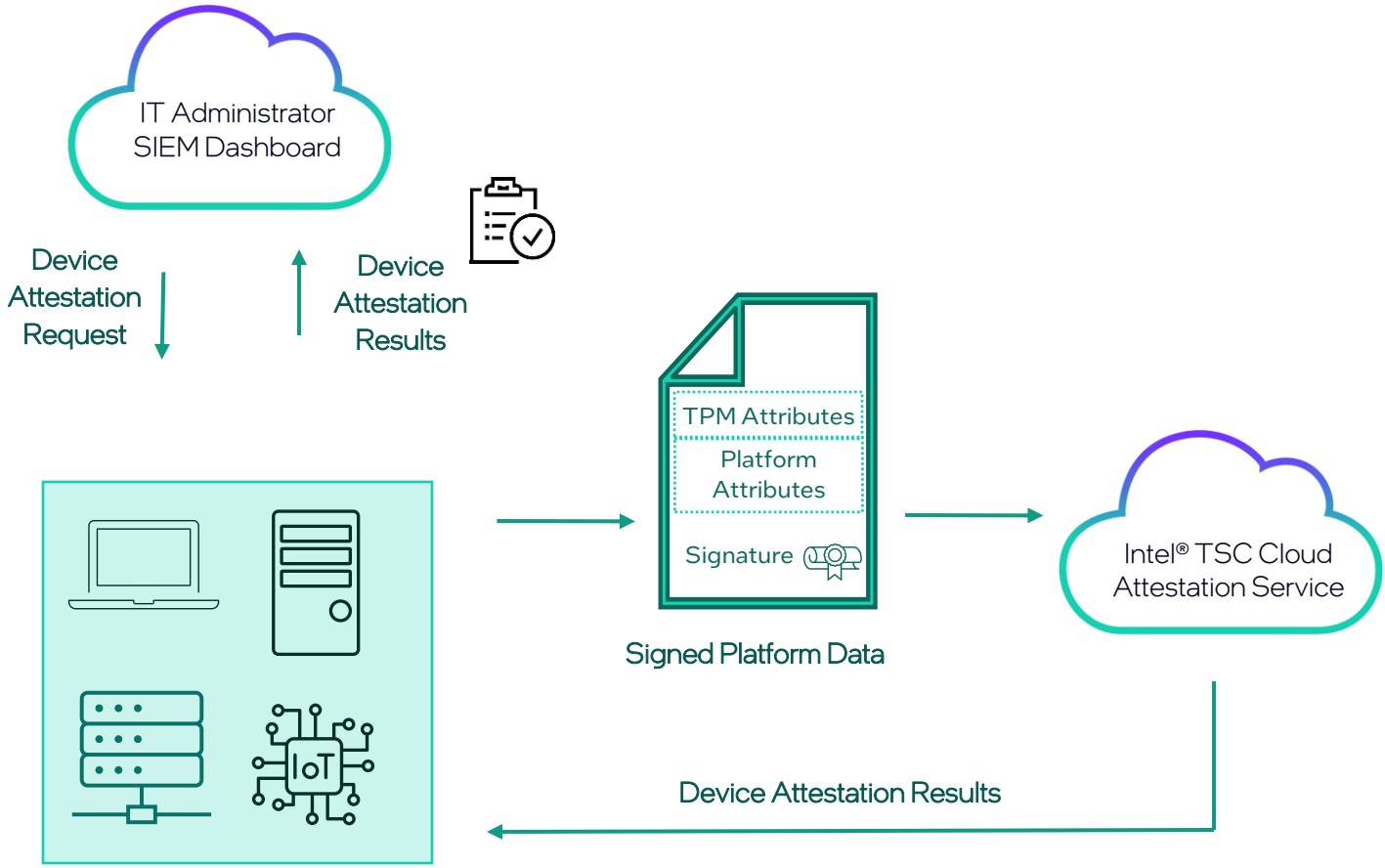


Figure 3. Platform Lifecycle Assurance Dashboard

Intel® TSC Client application and Attestation Service

Device Security does not stop at the time of device deployment but rather continues throughout the Lifecycle of the device. Once the end user deploys the new equipment, a platform baseline, the Intel® TSC Client application is deployed on the device to provide continuous below-the-OS device monitoring designed to detect unauthorized changes.
With the Intel® TSC Client application, the IT Administrator doesn't have to download the corresponding signed Platform Certificate or Direct Platform Data in order to do the device integrity verification.
To initiate the Intel® TSC Client application the IT Administrator will deploy an application that calls the Intel® TSC Client application .
The Intel® TSC Client application collects evidence data on the components in the system including TPM and Direct Platform Data. The Intel® TSC Client application the Intel® TSC Client application then sends the Platform Evidence Data to the Intel Trust Authority Service backend via a REST API.
The TSC Attestation Service will then Compare the Platform Evidence collected by the Intel® TSC Client application to the Baseline Evidence stored in the Platform Evidence Database. Figure 4 shows the Intel® TSC Client application SIEM Integration End to End flow.
The Attestation results of the Platform Compare will be returned to the Intel® TSC Client application.



the Intel® TSC Client application

Figure 4. Intel® TSC Application SIEM Integration

Intel® Transparent Supply Chain Client (Intel® TSC Client)

The Intel® TSC Client application is used to collect the initial (baseline) Direct Platform Components Data for the device without the original provenance data (i.e. baseline) in Intel® TSC attestation service. This initial data snapshot can be used to authorize and generate the device baseline. The Intel® TSC Client Figure 5 collects data on all the components in the system including TPM and Direct Platform Components and sends it to the TSC attestation service to do the attestation. The Intel® TSC attestation service compares the coming device evidence snapshot against the known-good baseline archived in the verifier service database. The TSC attestation service signs the attestation result as a Json Web Token (JWT) and sends it back to the Intel® TSC Client application. The RVT Transmits the Platform Evidence Data to the Intel® Trust Authority Service (ITA) TSC Attestation Service.


```
Scanning System Components Completed Successfully.

dpd-xml string generated successfully.
Calling ITA to get token...
Header: {
  "alg": "PS384",
  "jku": "https://amber-dev02-user9.ita-dev.adsdcsp.com/certs",
  "kid": "390dbac49b1733740e25ea692c18abdae635b547c17aae42fbe78528c5b623adbc14bcf1b25e6f58da64658eea5fe301",
  "typ": "JWT"
}
Payload: {
  "BaselineTime": "2024-12-06T11:52:39",
  "ComponentChangeCount": 1,
  "ComponentModified": [
    {
      "Baseline": {
        "AMT": "true",
        "AMTBuildNumber": "1932",
        "AMTHotFixNumber": "25",
        "AMTMajorVersion": "16",
        "AMTMinorVersion": "1"
      },
      "ComponentType": "TYPE131IntelManagementEngine",
      "Snapshot": {
        "AMT": "true",
        "AMTBuildNumber": "2418",
        "AMTHotFixNumber": "32",
        "AMTMajorVersion": "16",
        "AMTMinorVersion": "1"
      }
    }
  ],
  "ComponentScanCount": 13,
  "Matched": false,
  "System": {
    "Manufacturer": "LENOVO",
    "Model": "21BWS0U900",
    "SnapshotTime": "2025-02-07T15:52:42",
    "SystemSN": "PF44FYVH"
  },
  "ver": "1.0.0",
  "verifier_instance_ids": [
    "975628ef-2a37-4719-b2bb-3787bfad4c6a",
    "c1f6ba17-d171-4c75-8175-d0d10738014d"
  ],
  "exp": 1738972664,
  "jti": "910338a5-a495-4864-bcfb-e761485c3862",
  "iat": 1738972364,
  "iss": "Intel Trust Authority",
  "nbf": 1738972364
}
```


Figure 5. Changes identified through Intel® TSC Client Application

The SIEM Integration

This section uses Datadog, a cloud-based SIEM vendor, as an example to walk through how to integrate the Intel® Transparent Supply Chain Client (Intel® TSC Client) with the SIEM service.
The overall workflow is as follows:

1. IT deployed on-device agent calls the Intel® TSC Client application to collect the device platform evidence and initiate the attestation request to remote TSC attestation service.
2. Intel® TSC Client application receives the attestation result (token) which tells the device configuration has been changed.
3. Below is a sample PowerShell script Figure 6, that shows how to send the result as a SIEM event to Datadog:

```powershell
$env:DD_API_KEY = "your-datadog-api-key"

$headers = @{
    "Accept" = "application/json"
    "Content-Type" = "application/json"
    "DD-API-KEY" = $env:DD_API_KEY
}

$token = Get-Content -Path "path-to-rvt-token" -Raw
$currentDateTime = Get-Date -Format "yyyy-MM-ddTHH:mm:ssZ"

$body = @"
{
  "title": "tsc device configuration change detected",
  "alert_type": "warning",
  "aggregation_key": "tsc_attest_event",
  "priority": "normal",
  "text": "$currentDateTime, WARN, token: $token",
  "tags": [
    "TSC", "attest", "PLA"
  ]
}
"@

$siemApiUrl = "https://api.datadoghq.com/api/v1/events"
Invoke-RestMethod -Uri $siemApiUrl -Method POST -Headers $headers -Body $body
```

Figure 6. Sample PowerShell script to send SIEM event

4. The IT administrator will be able to capture this device configuration change event immediately through the event management dashboard on SIEM portal. Figure 7 shows how it looks like on Datadog.

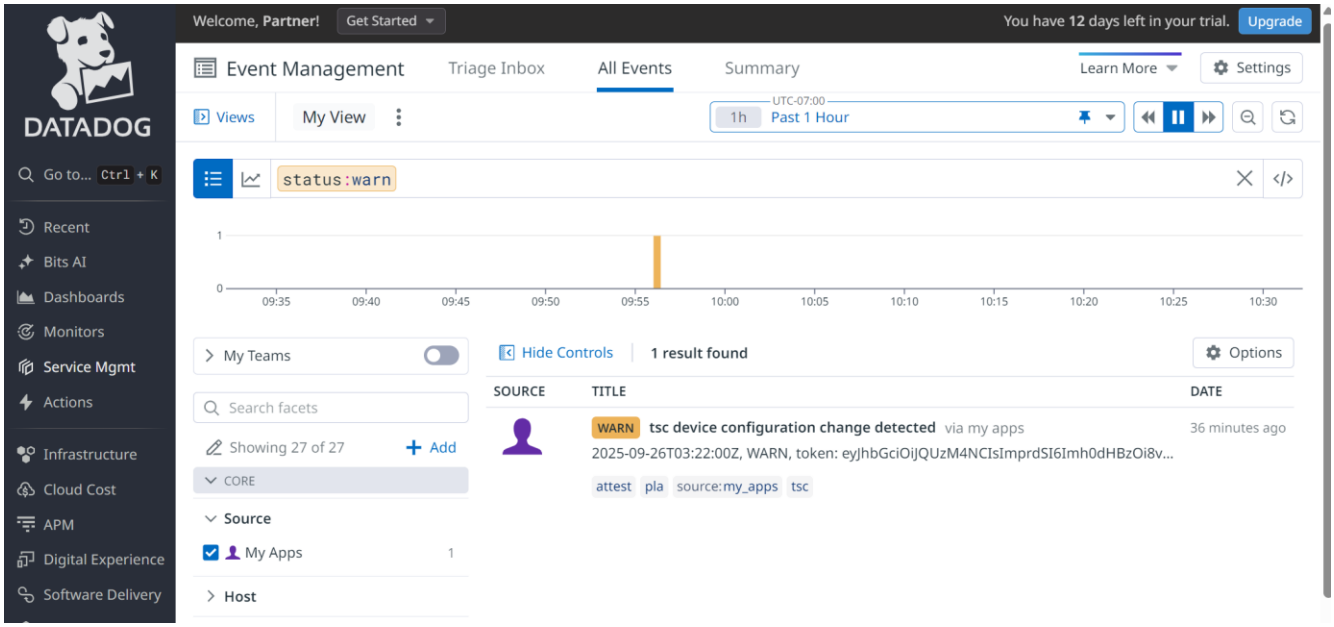


Figure 7. TSC PLA SIEM Event

With this, enterprise IT administrators will be able to monitor the device's integrity for the whole device fleet through SIEM and assure the integrity of the device in the whole platform lifecycle.

Summary

In Summary with the knowledge of the problem and availability of a well-developed solution such as the Intel® Transparent Supply Chain Platform Lifecycle Assurance service brings platform security into the transport, supply chain and deployment cycle with a documented, auditable supply chain security program that enables traceability of components and the system level.

© 2025 Intel Corporation Printed in USA