What is Intel® SecL-DC?
Intel® SecL-DC is designed to simplify the integration and deployment of hardware-rooted Intel security technologies at cloud scale by bringing optimized programming interfaces and management tools for many Intel security technologies together in one easier-to-use set of libraries and tools compatible with cloud environments like OpenStack*, Docker*, and Kubernetes* Extensions.

Why Intel® SecL-DC?
Hardware-based security technologies need consistent and pervasive software components to discover, interact, attest and evaluate policies against, for use in the Datacenter. These functions have to happen with high degree of automation, and at cloud scale. Intel Security Libraries-DC makes it significantly easier for CSPs, ISVs and datacenter security and devops personnel to leverage the critical hardware security technologies that are part of the Server platforms.

What are the capabilities of Intel® SecL-DC?
The first release of Intel® SecL-DC supports three primary security usages:
- Platform Integrity: Intel’s work in platform integrity builds on our Intel® Cloud Integrity Technology (Intel® CIT), which helps ensure cloud workloads run on trusted, unaltered servers and virtual machines that have not been tampered with. Customers want integrity assurances to answer questions like, “Is my data running on the right hardware, or has my platform been compromised in any way?” Intel® SecL-DC provides attestation capabilities for integrity and compliance across compute pools in the cloud, made possible with an established hardware-based root-of-trust.
- Data Sovereignty: As data breaches gain in public visibility, governments and regulators are stepping in. The most prominent example of this is the General Data Protection Regulation (GDPR) from the European Union. Intel® SecL-DC provides attestation capabilities for integrity and compliance across compute pools in the cloud, made possible with an established hardware-based root-of-trust. Solutions built on Intel® SecL-DC can enable Data Sovereignty and geo-location policies which verify user data is kept only on servers provisioned in approved regions.
- Intel® Threat Detection Technology (Intel® TDT): Augments existing ISV security solution capabilities to improve the detection of advanced cyber threats and exploits. Intel® TDT can detect exploits using advanced telemetry registers in the CPU in conjunction with Machine Learning (ML) to identify threats in real-time based on known threat models.

Can Intel technologies work without Intel® SecL-DC?
Yes, Intel hardware security technologies work independently of ISecL-DC. With out Intel® SecL-DC, every company/ISV has to invest in building some core enabling technologies to interface and interact with the hardware features via APIs and other mechanisms. ISecL provides a solid reference implementation with integrations into OpenStack, Kubernetes, and a well-tested APIs for easy integration with variety of security monitoring, and automation tools.
How is this different from CIT?

CIT was the first generation attestation solution that was built specifically to interface with Intel TXT. Intel® SecL-DC is the next generation security management and attestation framework, that works with all Intel security technologies to provide real security use cases at Cloud scale. The components of Intel® SecL-DC are built to be deployed as Application containers or VMs – which ever the customer chooses to deploy. The new Flavor model for managing integrity measurements has been redesigned from the ground up for improved intuitive behavior, reduced complexity, and significantly better management of datacenter lifecycle events like upgrades and downgrades. Flavors are now portable, and the rules used for integrity attestation are extremely customizable to suit a wide variety of needs, while maintaining easy-to-use defaults to suit most deployments.

Is there support for Intel® SecL-DC?
The open source project is maintained on 01.org and has assigned maintainers and portal based support structure in place.

What is the roadmap?
You can refer to the Intel® SecL-DC use cases and features at: 01.org/intel-secl/releases

Where can I access the latest Documentation?
You can refer to the collaterals at: 01.org/intel-secl/documentation

What are the OSes supported for v1 Use Cases?
We support RHEL* 7.6, Windows* Server 2016 Datacenter, VMware* vSphere 6.5u2, VMware* vSphere 6.7u1

What programming languages does it support?
The components support REST APIs for Consumers (orchestrators, Security tools, key management servers etc., to use). ISecL components are built with C and Java, with the target of move entirely to Golang through future versions.

How will it work with VMWare?
Vmware provides the needed hardware support and interfaces for Intel SecL-DC to manage Platform Integrity and enable Data Sovereignty for ESXi servers. Security software partners like HyTrust can consume the Intel SecL-DC security attributes and enable policy-based controls – preventing migrations of VMs or data onto noncompliant hosts, and preventing decryption of sensitive data outside of security boundaries.

What are the integration points for OpenStack?
Intel has worked with the OpenStack community to extend the Traits feature in OpenStack to support hardware security feature assertions. Intel SecL will periodically update the Compute node Traits for platform integrity and other features as Custom_Traits, which are then utilized
by the Placement APIs to filter appropriate compute nodes for the VMs. VMs specify the security features they expect via Image meta-data. These extensions are part of mainstream OpenStack.