Compromise trustworthy visibility in working systems
Remote ATtestation ProcedureS (RATS) BOF

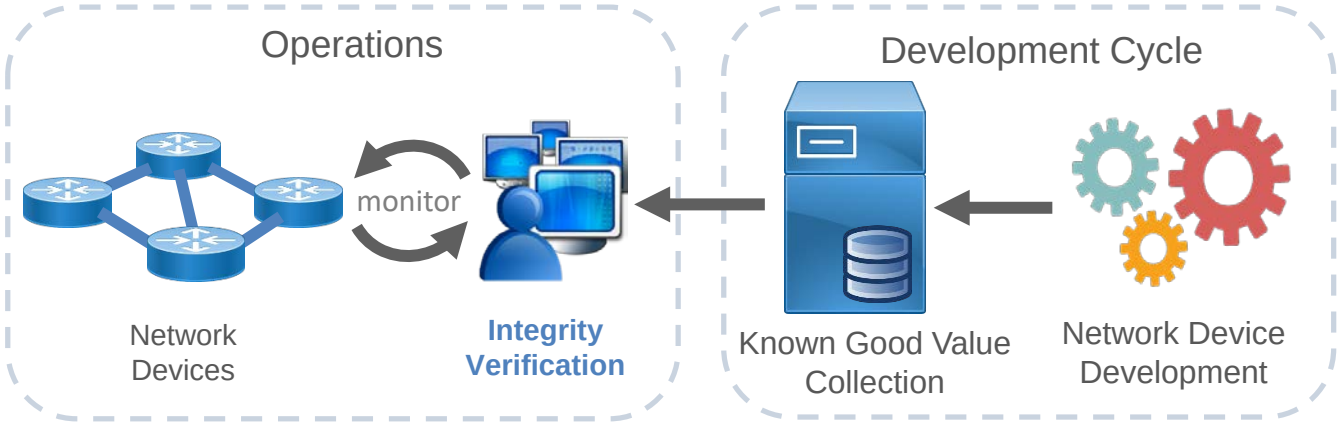
IETF #103

Eric Voit
Principal Engineer – Cisco Systems, Inc.
evoit@cisco.com
Nov-2018

Agenda

- Remotely attesting switches and routers
- ~ Demo

Remotely attesting switches and routers



Known Good Value – **is it correct?** - compare attested measurement against verifiable know good value

Imprint Value – **has it changed?** - compare attested measurement against initial snap shot value

Event Occurrence – **did it happen?** – monitor device for attested events that should not occur

More than just at Boot time

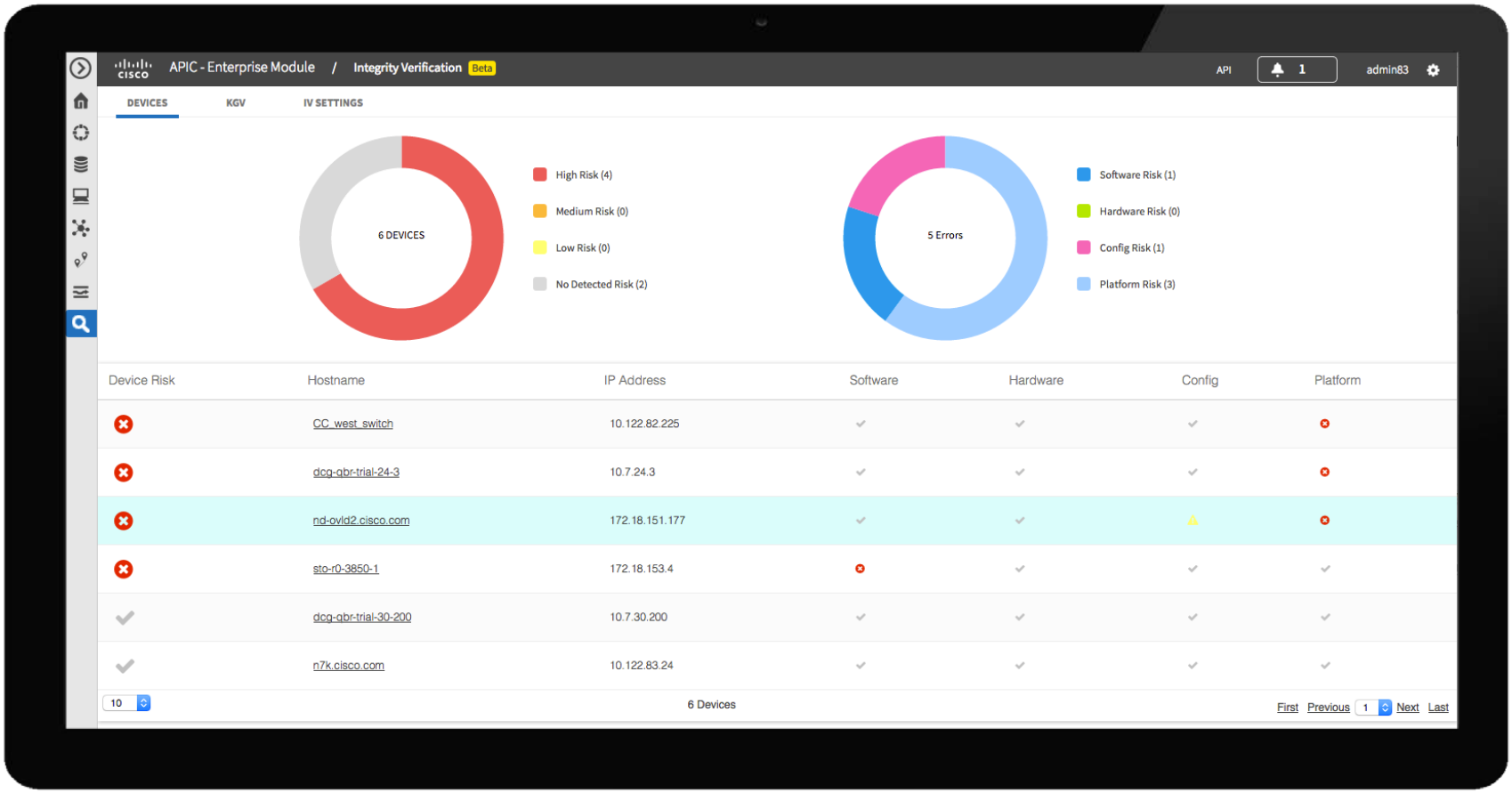
Platform	Verification of the secure boot and the identity of the device.
Software	Checks of the software files and in-memory contents. Logs.
Hardware	Inventory of hardware components as expected.
Configuration	Unexpected changes in the device configuration? Logs.

Asynchronous !

- Inserted hardware
- ACL configuration
- Filtered Syslog entries
- Configured keys
- Users, and their permissions
- Checksum of software binaries
- Running software processes
- Adjacent L2 / L3 neighbors
- Interface state (up/down)

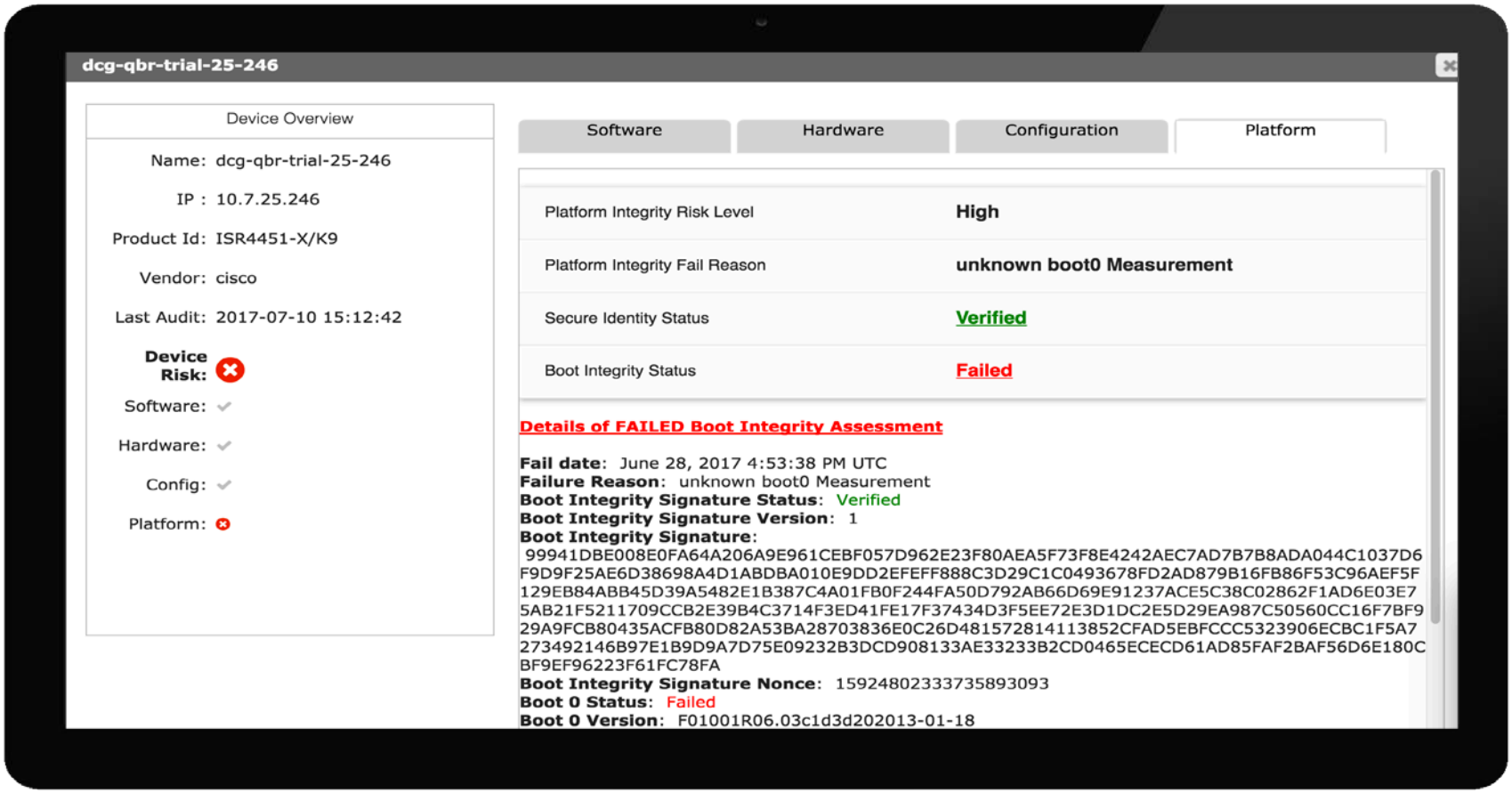
~Demo

(Screen-shots of Demo due to time constraints)



~Demo

(Screen-shots of Demo due to time constraints)



More info
https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/application-policy-infrastructure-controller-enterprise-module/1-5-x/integrity_verification/user-guide/Cisco_Integrity_Verification_Application_APIC-EM_User_Guide_1_5_0_x.pdf

Thank you!