2024-05-07 Security Subcommittee Meeting Notes

Please find below the Minutes of Meetings and recording for the SECCOM meeting that was held on 7th of May 2024.

Jira No	Summary	Description	Status	Solution
	Logging modifications proposal	Mateusz Pilat from Tata presented changes in log format for its unification. Change Request will be prepared by Mateusz. Discussion will be followed at the OOM meeting on Wednesday. RBAC changes could be provided: Improvement for NewDelhi Release Root access for container need was explained.		
	ONESummit and DTF takeaways	Concerns about assurance. Observability in 5G Core, collecting metrics. Lacking data to apply in ML/AI. ONAP streamlining. Cross comunity efforts (with ORAN). Nephio ha ssome issues with Porch https://kpt.dev/guides/porch-user-guide	ongoing	
	GitHub Actions integration pipeline	LF IT migrating CI pipeline to GitHub actions - may take to the end of fall or later, once ONAP is completed for GitHub Actions , we will do security review. Last update from Matt is that LF IT is continuously shipping one project at a time. 4/2: in progress	open - WIP	
	LFN AI/ML use cases	Muddasar Ahmed presented the draft deck about LFN AI/ML use cases. **Maggie shared link:** **https://www.nist.gov/itl/ai-risk-management-framework** We need to have Ops feedback (NOC manager) on AI, what pain point could be solved by AI. Deck shared with Marian from Orange, feedback expected in first week of December. Under WG 11 in ORAN Alliance (doing standards for ORAN) - threat analysis will be done in the domain of AI security - OWASP TOP 10 - planned by March'24. Runtime influence under interest. Maggie shared the link: https://www.cisa.gov/news-events/alerts/2023/11/26/cisa-and-uk-ncsc-unveil-joint-guidelines-secure-ai-system-development Feedback from Marian received to be discussed at the next SECCOM. China Mobile and Infosys would like to work on use cases. First call done yesterday, agreed on a model to move forward. Intent Based Mode would use Generative AI. 3 layers approach: business layer, services layer, domain layer. Each Intent Manager would have its own AI. Generic model would be used: business language into ONAP consummable, for services more data oriented and finally domain oriented. We do not focus on 5G only architecture but rather on any so could be used by any organization. Topic is in forming group. China Mobile and Infosys interested in Intent context. China Telecom is also interested with focused on user input and Intent. Muddasar Ahmed Byung-Woo Jun Maggie update China Telecom: New Delhi - data service. CCVPN use cases - LLM does not give enough intelligence. Develop domain specific model to generate more intelligent decisions. China Mobile & Infosys: Intent based networking - Level 3 autonomy. Infosys is consulting with MNOs and has experience developing small AI-based autonomous loops. New Delhi release: CM/Infosys will deliver LLM for Intent based networking. Intelligent decision making. Post New Delhi will evaluate if the two tracks can leverage each other. UUI is impacted system for both tracks. No impact to other components NSA/Georgia Tech: AI/ML for security. Collecting and tagging security data to correlate the data. Amy Zwarico provided reference to NIST AI 100-2e2023 Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations Call this week booked. AI/ML use cases focus group still works on platform and use cases priorities. CCVPN use case and intent based networking. China Mobile and Infosys starting work on that in more downstream. ORAN WG11 is working on security aspects. WG2 (non-real-time RIC) and WG3 (near-real-time RIC) are working on xApps and rApps (AI/ML capabilities). **Need to write LF informative position white paper for AI/ML - team to write constitued. Meeting is planned with convinient time for all contributors. Goal is to produce it by DTF.** **Structure bulleted paper available on Confluence - https://wiki.lfnetworking.org/pages/viewpage.action?pageId=120652848** China Mobile focus: generative AI. (New Delhi UUI) China Telecom focus: intent transformation & LLM tuning parameters to create domain specific solutions. (New Delhi UUI) **Both projects are in progress.**	open - sceleton structure of the document	LFN AI-ML Use case formulation.pptx

	Nephio security working group	Byung-Woo Jun informed SECCOM that the Nephio security WG is holding a joint meeting with the LF security SIG today at 11AM ET. Nephio plans to adopt 80% of OSSF passing badge. Topic further discussed: It was noted that the passing badge should be straight-forward to achieve. The web page tlhansen.us/badging was discussed. Click on "Single Project…" then fill in a search string or badging ID (e.g. "nephio" or "7665"). For Nephio, Tony recommends to sort by "Type+Section" Nephio SIG Security meeting: By: Lucy Hyde When: Tuesday, October 31st, 2023 8:00am to 9:00am (UTC-07:00) Pacific Time - Los Angeles Repeats: Weekly on Tuesday Location: https://zoom.us/j/96025994457 We could support Nephio by sharing our best practices and processes in place. Lucy OOO for the next few weeks? Byung introduced Tony's tool and was positively perceived by Nephio team. Nephio has GUI and talked about UI: AuthN and AuthZ to be shared by Byung. Nephio Sig meeting last week: https://nephio.slack.com/files/U0503L9UA8N/F065V0AAZRQ/sig-security_action_items.pdf?origin_team=T03LMAUL4HH&origin_channel=D065DKWJJ9X No update - info collection ongoing. Byung will join SIG group. Secrets and Service Mesh ☑ Byung-Woo Jun many above items are done. LF Security and SIG Security joint meeting did not happen. Nephio SIG Security discussion topics are: ■ Secrets management leveraging Vault (open-source version) ■ Service Mesh ■ Ericsson plans to propose Identity and Access Management at the SIG Security meeting today (Jan 23) Byung-Woo Jun Discussing R3 release. • using open source vault for secrets storage • Service mesh: ONAP uses a single management cluster. Nephio has a built-in service mesh component that can be added by the operator. E/// will propose IAM to SIG today. • Considering OpenSSF tool. • Muddasar Ahmed will provide a template for analysis. Byung-Woo Jun The following proposals are under review at Nephio SIG Security Nephio Secrets management user story proposal, https://docs.google.com/document/d/1Ce_cR7afovjWsdECkV8kNbPreG5GirfJXP5IrSiABjg/edit?usp=sharing Service Mesh Requirements, https://docs.google.com/document/d/1UtW20GLTbICTUQyeC1Kx6aDnHlf4EqdhmeD29vsHSEM/edit?usp=sharing Identity and Access Management Requirements proposal, https://docs.google.com/document/d/1qxGZI-HwTA0DfUO_hXKlkEpFzTNcmbDd6IO-CO7mLYo/edit?usp=sharing Package validation user story proposal, https://docs.google.com/document/d/1YeyUZUPFCS4bBgh8ShWVPrGs9HMLtrhwFSIDC6Xl3xc/edit?usp=sharing Package validation under preparation. Rahul Jadhav shared his Nephio workload identity. The team plans to review it. Also, Ericsson plans to share Identity and Access management requirements (2nd review) next week. requirements from Workload Identity perspective. https://docs.google.com/presentation/d/1K0gooS9ge181zNXLvA_SNAtGJyK1I77zOsRy6qpv7ME/edit?usp=sharing Additional meeting planned today, E/// will provide user access control. Interest on workload to wokload access control, https://docs.google.com/document/d/1IwWVGASgdOuLHCHYg82WaZaHdOEXyOM1/edit#heading=h.30j0zll **Byung presented E/// user access control and workload access control under interest. SPIFFE in ORAN as study item. Workload identity still to be addressed.** **Last Tuesday, Shiv Bhagavatula (Nephio SIG Architecture) shared additional Workload Identity design, leveraging SPIFFE infrastructure (SPIRE server, SPIRE agent, SPIFFE Id and SVID…), https://docs.google.com/presentation/d/1L79WrZ64Uar3IrH-jL_IeQTlPoLtXGZKHllfVCXLoco/edit#slide=id.p.** **Byung-Woo Jun , the latest user Identity and Access Management requirements, https://docs.google.com/document/d/1IwWVGASgdOuLHCHYg82WaZaHdOEXyOM1/edit#heading=h.nzahaii2p80p** **For Shiv and team's workload identity design, https://docs.google.com/presentation/d/1L79WrZ64Uar3IrH-jL_IeQTlPoLtXGZKHllfVCXLoco/edit#slide=id.g2bfc4581413_1_5** 4/2: Target R4 (3Q24/4Q24) Nephio Security team POC - (1) OIDC AuthN/AuthZ using Service Mesh and Key Cloak, (2) Workload identity and access management using SPIFFE. **Workload identity and access management in progress. Internal discussions in E/// for next steps for user identity and access management.** ■ Workload Identity User Story, https://docs.google.com/document/d/1nkh7tTltwii1bY877PfzjFCBtmRos4IDh5EOJxWXRdg/edit#heading=h.srlm9p7wuua8 ■ Shiv plans to provide a better definition of "token". Nephio R3, there is an action point, secret management, "sharing secrets across clusters as Skupper generates a secret in one cluster /namespace and that secret has to be shared with another cluster/namespace. To create the tunnel for communication. Now the question is how to share the secrets" It is a narrowed scope of sharing secretes between particular services, which is different from what Nephio SIG Security proposed.	ongoing	
	ONAP Security Implementation Status	Byung-Woo Jun TATA Communications supports RBAC, observability, logging, backup, etc. by leveraging the ONAP currently security mechanism (Ingress, Service Mesh) for their own platform. It is possible they contribute the enhancements they made to the ONAP New Delhi release (TBD). Share of code most probably in Oslo release. Andreas is working on enhancements for OOM Team. Tata communication shared which components in Montreal use STDOUT or not, ONAP Logging alignment for Montreal release.xlsx		

	No PTL for AAI, DCAE, OOF	-Andreas Geissler and Thomas Kulik made committers -They will do the work necessary for the projects to participate in the release -TSC approved streamlining process (7 September) -SECCOM will create package upgrade recommendations -TSC will recruit resources to perform pgrades for AAI, DCAE, OOF • need options to move forward Kenny's reply is that we could benefit from Mentorship program. We have to define job description and skills needed. **Byung-Woo Jun New Delhi - VFC, SDC PTLs stepped down.** **Byung-Woo Jun temporarily handling the Release Manager role.** **4/2** **DMaaP MR is to be unmaintained. Global Requirement for MR deprecation - Byung to prepare it. Deprecating component of the project shall be initiated by the PTL, if exists.** • **Andreas working on removing DMaaP MR from SO - target is New Delhi** • **Ericsson removed DMaaP MR Policy; Andreas testing - target is New Delhi** **Andreas to generate the list of unmaintained repos and projects.** **TSC activity:** • **decouple ONAP and create open interfaces** • **use cases drive the use of streamlined components**	ongoing	-Byung will discuss with Andreas and Thomas to coordinate release tasks such as backlog prioritization -Muddasar: someone needs to take backlog management role -Muddasar: no mandated best practice to manage technical debt; call for a statement about code quality – all code will be secure -Muddasar & Amy: bring mandate for code quality to LFN TAC 2023/8/16 ■ Pawel to raise a request to TSC with getting resources for upgrades for AAI, DCAE, OOF - done.,

	TSC meeting (April 18th)	Project status for New Dehli and versioning, release planning for Oslo.
		
		Documentation work in progress by Thomas and Andreas.
		
		• Byung-Woo Jun , added the Release Planning: Oslo (for now, it is a draft).
		• Project status for New Dehli and versioning
		
		    ■ Dan Xu , confirmed that CLI and VNFSDK are not active and it is ok to mark them as deprecated.
		      • Andreas Geissler , confirmed there are no dependencies of CLI and VNFSDK.
		      • Byung-Woo Jun , TSC needs to go thru their deprecation processes.
		    ■ DMaaP MR dependencies issues are getting resolved. After then, TSC will go thru next steps
		• TSC voting for unmaintained project deprecation.		

	ONAP Focus for the future	Initial discussion with Dong, Keguang and Byung. Lightweight ONAP under consideration: SO, SDC, Policy, CPS, UUI, DCAE, SDNC. Byung-Woo Jun , refined the ONAP initiative slide deck further (simplified based on Maggie's comments, Thanks!); plan to present it to TSC this week; I will share the slide deck with SECCOM after then.		
	PTL meeting (April 22nd)	Fiete shared info on WIP for NG Portal. Just 2 remaining items for Documentation and python (Thomas and Andreas) Insufficient progress for packages upgrades List of the ONAP components to be disabled prepared by Andreas: OOM New Delhi Release		

	LFN-TAC (DTF F2F)	FY24 priority, security was covered - consensus on ONAP best practices. http://tlhansen.us/badging Platform Maturity Requirements (aka Carrier Grade) New project induction and project graduation criteria documentation accepted. Security - discussion should be a separate WG meeting - security scrum of scrums. LFN Security Forum. Updated meeting agenda for tomorrow's TAC meeting (https://wiki.lfnetworking.org/display/LN/2023-12-06+TAC+Minutes) and presentation planned by Amy and Muddasar: - security scrum of scrums proposal - Tony's dashboard for all LFN projects - SAST and SCA tools and onboarding provided by LFN - LFN having responsibility in releasing certifications (incubation, mature etc.) TAC agreed with the proposal provided by Amy. In 6 months trial period we should have recommendations for secure software development. Projects SECCOM representatives to join those meetings. Sense of ownership to be improved. LFN wide security focus group approved by TAC. Align AI/ML initiatives Creating LFN-wide Security FG L3AF project - Microsoft pulled out XGVela - no active contributors FIDO Muddasar Ahmed requested TAC to make a formal quality statement about LFN produced code. CNCF certification and testing topic recently discussed. Tailor from CNCF and Sana presented the need for certification. CNTI (CloudNative Network Function for Telco) conformance discussion - proposal expected by April to Governing Board. Security whitepaper update under consideration - quality goal statement to be drafted. ORAN Alliance is doing yearly publication on security blog post. CNTI - discussion finished last week. CNTI assets (test and documentation for certifying) moved to LFN. Discussion on Superblueprint and documentation. Migration process in progress. Documentation update - modifying Lifecycle. Confidential computing. **Leave automation, CI/CD security, sample statements under prep by Muddasar.** **Having Superblueprint form as TSC. Aiming demonstration of projects interoperability.**		Muddasar Ahmed to check for document availability on software quality goals.
		Technical debt budgeting discussion needed with TSC/TAC - 10% of efforts for app security could be invested. What are best practices to transfer project to Archive or Unmaintained state. This could be part of quality goal**.** Still waiting for Jill Levato action on that. E-mail was sent by Pawel too. but no response received from Jill. **Jill responded and included Rany who suggested TAC level discussion and decision taking.**		Muddasar Ahmed to follow with Jill.
	Badging update	Tony presented additional functionalities: www.Bestpractices.dev/en/projects/1718?criteria_level=2 Gap on ONAP badging: no master editor for the badges. Bring up with TSC to find a LFIT resource to fill the role. TSC topic to be added for the upcoming agenda. **OpenSSF Badging program to be establised by LFN.** **New type of Badge - scorecard which is based on GitHub Actions? - 10 different criterias automatically updated. Ongoing discussion with Kenny by Tony - API info to be shared.** **https://openssf.org/training/** **Standalone version exists and could potentially used in ONAP, so scorecard could be implemented.** **Few weeks ago at the TSC Sandra was asked to become master editor on ONAP Badging projects. Finally, everything was done - she was added as owner of all ONAP projects, existing editors can work as it was. Both Jim and David were removed.** **All OpenSSF projects will have their own TSCs - Tony was proposed to be one - CONGRATS TONY!**		

	Package update recommendations	Amy Zwarico my team will create recommendations.		
		Work in Progress. ETA by end of this week. Leverage Nexus-IQ APIs.		
		All recommendations are available on the restricted Wiki. Jira tickets were created for each project.		
		Full list of project jiras.		
		Project Tasks:		
		• https://jira.onap.org/browse/AAI-3781 • https://jira.onap.org/browse/CCSDK-3987 • https://jira.onap.org/browse/CLAMP-1031 • https://jira.onap.org/browse/CLI-494 • https://jira.onap.org/browse/CPS-2104 - **reported as completed by Toine** • https://jira.onap.org/browse/DCAEGEN2-3410 • https://jira.onap.org/browse/DMAAP-1902 • https://jira.onap.org/browse/EXTAPI-605 • https://jira.onap.org/browse/MODELING-686 • https://jira.onap.org/browse/MSB-767 • https://jira.onap.org/browse/MULTICLOUD-1506 • https://jira.onap.org/browse/SDNC-1835 • https://jira.onap.org/browse/POLICY-4933 • https://jira.onap.org/browse/SDC-4680 • https://jira.onap.org/browse/SO-4124 • https://jira.onap.org/browse/USECASEUI-833 • https://jira.onap.org/browse/VFC-1988 • https://jira.onap.org/browse/VNFSDK-881		
	Lack of CLM scans for NG Portal	**Andreas was informed about lack of Jenkins jobs for Nexus-IQ scans. Fiete will work on this as project PTL.**		
		Update from Fiete Ostkamp :		
		• maven based jobs use the lf-infra-sonatype-clm Jenkins builder that triggers the com.sonatype.clm:clm-maven-plugin • for gradle there currently is no such builder available in global-jjb • Sonatype officially does not provide an equivalent plugin, but there is the Sonatype Scan Gradle Plugin that could provide similar functionality		
		Jira opened by Fiete, ongoing support by LF-IT. Fiete is back from holidays.		
		Update from Fiete:		
		onap-portal-ng-preferences:		
		https://nexus-iq.wl.linuxfoundation.org/assets/index.html#/applicationReport/onap-portal-ng-preferences/b50d4e842a0847bc91437d354075e383/policy		
		onap-portal-ng-history:		
		https://nexus-iq.wl.linuxfoundation.org/assets/index.html#/applicationReport/onap-portal-ng-history/03f1fde4f7ea4f029031bbaf9689cfa8/policy		
		onap-portal-ng-bff:		
		https://nexus-iq.wl.linuxfoundation.org/assets/index.html#/applicationReport/onap-portal-ng-bff/4d9a28df94eb4bad85d858fe72321dac/policy		
	NEXT SECCOM MEETING CALL WILL BE HELD ON MAY 14th 2024	RBAC discussion - code from Tata with enhancements. Outcome of Oslo discussion.		

Recordings:

2024-05-07_SECCOM_week.mp4