

Defect Exists	Inherent defect, not sure whether this defects degrades security attributes --> need brainstorming		
In Progress	Attack is in progress		
Attack Fail	Failure on attacker's perspective		
Attack Success	Success on attacker's perspective		

Defect Exists	herent defect, not sure whether this defects degrades security attributes --> need brainstorming
In Progress	Attack is in progress
Attack Fail	Failure on attacker's perspective
Attack Success	Success on attacker's perspective

* Analyze threat list, security requirement and mitigation of team 6 project and then find missing items.							
Written by Team 6							
Checked and Analyzed by Team 5							
TR-ID	Threat	Review	SR-ID	Security Requirement	MI-ID(matched to SR-ID)	Mitigation	Evaluation by team 5 -> Evaluate Threat, SR and MI
TR-01	If the user credential data is stored as plain text, it can be disclosed.	User credential should be kept securely	SR-13, SR-12	User Credential Data should be encrypted in the storage. Use well-known cryptographic libraries and robust algorithms.	MI-03, MI-07	Encrypt user credential data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use cbc of gcm mode Integrity Check with hash - Use an algorithm that are stronger than sha256	
TR-02	An attacker modify user credential data.	User credential should be kept securely	SR-11, SR-10, SR-12	the system shall know the change of the user credential data. The system must perform an integrity check before using user credentials. Use well-known cryptographic libraries and robust algorithms.	MI-03, MI-07	Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than sha256 Encrypt user credential data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use cbc of gcm mode	
TR-03	An attacker modify user credential data and then server can use it without checking.	User credential should be kept securely	SR-11, SR-09, *No matching SR	the system shall know the change of the user credential data. Server and client must communicate using an encrypted channel. Input validation check is required in Server side.	MI-05, (It seems to assume that do not considering in server side.) MI-02, MI-07	Input validation check - Input sanitization Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than sha256 Communicate using Encrypted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client	Need to make sure the server is doing input validation.

	TR-04	An attacker spoof the user (Client)	Need to more stronger authentication process	SR-02, SR-01	Cryptographically strong password should be used. A strong authentication method should be used.	MI-01, MI-10	Apply setting policy of cryptographically strong password - Enforce passwords longer than 7 characters. - Forces the use of mixed the letters of the alphabet and numbers. Strong authentication method - Consider 2-Factor-Authentication method	
	TR-05	An attacker tampers Login or Mode control data to server in order to get information.	Need to encrypt communication channel	SR-09	Server and client must communicate using an encrypted channel.	MI-02	Communicate using Encrypted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client	
	TR-06	Clients can repudiate the actions they have performed.	Need to apply mutual authentication	SR-05, SR-08	#include #include #include in	MI-09, MI-11	Use mutual authentication - Using protocol TLS1.2 or higher - Use mutual authentication between server and client Save contents of communication as a log - Save log of the request and response between the server and the client	
	TR-07	An attack can sniff the data on the connection.	Need to consider encrypting the data flow.	SR-09	Server and client must communicate using an encrypted channel.	MI-02	Communicate using Encrypted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client	
	TR-08	Weak Authentication may lead to disclose information	Need to more stronger authentication process	SR-02, SR-01	Cryptographically strong password should be used. A strong authentication method should be used.	MI-01, MI-10	Apply setting policy of cryptographically strong password - Enforce passwords longer than 7 characters. - Forces the use of mixed the letters of the alphabet and numbers. Strong authentication method - Consider 2-Factor-Authentication method	
	TR-10	the information of the communication between client and server is interrupted by attackers.	Need to use TLS	SR-09, SR-05	Server and client must communicate using an encrypted channel. Only the verified server and client should be connected and communicated.	MI-02, MI-11	Communicate using Encrypted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client	Threats are mapped to security RQs, but MI-11 is most likely not taken into account. --> M1-02 and MI-11 are the same.
	TR-13	An attacker sends a malicious data to server in order to change the flow of program execution.	Need to apply input sanitization	*No matching SR	Input validation check is required in Server side.	MI-05, (It seems to assume that do not considering in server side.)	Input validation check - Input sanitization	Need to make sure the server is doing input validation. --> Server is doing a range check. So no problem.

	TR-29	It may be physically damaged and you may not be able to get Data from Camera	Need to protect camera unit from physical damage	SR-06	Protect Camera from physical damage	MI-08	Protect from physical damage - Wrap the camera module out of sight, or glue the cable to the camera.	
	TR-34	It is possible to add a lot of Images in the storage.	Need to limit the number of images	SR-07	Restrictions related to files are necessary to avoid system problems.	MI-12	Validation of image when file saving - Limit on number of files - File name verification when image save - File size validation when image save	
	TR-35	User credential may be disclosed.	Need to encrypt user credential data	SR-13, SR-12	User Credential Data should be encrypted in the storage. Use well-known cryptographic libraries and robust algorithms.	MI-03, MI-07	Encrypt user credential data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use cbc of gcm mode Integrity Check with hash - Use an alforithm that are stronger than sha256	
	TR-41	User Credential Data can be exposed to attackers.	Need to encrypt user credential data	SR-13, SR-12	User Credential Data should be encrypted in the storage. Use well-known cryptographic libraries and robust algorithms.	MI-03, MI-07	Encrypt user credential data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use cbc of gcm mode Integrity Check with hash - Use an alforithm that are stronger than sha256	
	TR-44	Server (Jetson) may be spoofed by an attacker	Need to apply mutual authentication	SR-09, SR-05	Server and client must communicate using an encrypted channel. Only the verified server and client should be connected and communicated.	MI-02, MI-11	Communicate using Encryted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client	Threats are mapped to security RQs, but MI-11 is most likely not taken into account. --> M1-02 and MI-11 are the same.
	TR-45	Client (PC) may be spoofed by an attacker	Need to apply mutual authentication	SR-09, SR-05	Server and client must communicate using an encrypted channel. Only the verified server and client should be connected and communicated.	MI-02, MI-11	Communicate using Encryted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client	Threats are mapped to security RQs, but MI-11 is most likely not taken into account. --> M1-02 and MI-11 are the same.
	TR-46	Video Stream may be tampered with by an attacker.	Need to protect the video stream over the connection	SR-14	Video Stream over the connection should be protected.	MI-02	Communicate using Encryted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client	

	TR-48	Video Stream may be sniffed with by an attacker.	Need to protect the video stream over the connection	SR-14	Video Stream over the connection should be protected.	MI-02	Communicate using Encrypted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client	
	TR-49	Client (PC) crashes, halts, stops or runs slowly.	Need to remain stable in abnormal cases	SR-03	Errors, exceptions, and abnormal conditions that may occur in the software must be handled robustly.	MI-04	Implement robust system - Error handling - Exception handling - Finding countermeasures for predictable abnormal conditions	
	TR-52	Server (Jetson) may be able to remotely execute code	Need input sanitization	*No matching SR	Input validation check is required in Server side.	MI-05, (MI-05, (It seems to assume that do not considering in server side.)	Input validation check - Input sanitization	Need to make sure the server is doing input validation.
	TR-53	An attacker may pass data into 1.1 Client (PC)	Need input sanitization	SR-04	Input validation check is required in Client side.	MI-05	Input validation check - Input sanitization	
	TR-56	Change the image data not to recognize registered users.	Need to protect user credential data	SR-13, SR-12	User Credential Data should be encrypted in the storage. Use well-known cryptographic libraries and robust algorithms.	MI-03, MI-07	Encrypt user credential data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use cbc of gcm mode Integrity Check with hash - Use an alforithm that are stronger than sha256	
	TR-57	Disclose administrator's ID/Password to the employees in the company.	Need to more stronger process for authentication	SR-02, SR-01	Cryptographically strong password should be used. A strong authentication method should be used.	MI-01, MI-10	Apply setting policy of cryptographically strong password - Enforce passwords longer than 7 characters. - Forces the use of mixed the letters of the alphabet and numbers. Strong authentication method - Condider 2-Factor-Authentication method	
	TR-59	Sniff the communication channel between server and client to get user credential data.	Need to protect the data over the connection	SR-09, SR-05	Server and client must communicate using an encrypted channel. Only the verified server and client should be connected and communicated.	MI-02, MI-11	Communicate using Encrypted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client	Threats are mapped to security RQs, but MI-11 is most likely not taken into account. --> M1-02 and MI-11 are the same.
	TR-60	Compromise the connection of network physically by an attacker	Server need to be robust in abnormal case.	SR-03	Errors, exceptions, and abnormal conditions that may occur in the software must be handled robustly.	MI-04	Implement robust system - Error handling - Exception handling - Finding countermeasures for predictable abnormal conditions	

TR-61	By changing the server/client's certificate or key, an attacker may attempt to connect to an unauthorized client. And attacker can try to steal the information of the encryption channel.	Need to protect or verify the certificates and keys used by the server and client for TLS communication	SR-15	A server and client program must perform an integrity check before using a certificate or key.	MI-13	Certificate & Key file existence check Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than sha256	
TR-62	By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition result. By stealing facial recognition data, an attacker can steal information from the system.	Need to protect face recognition data	SR-16, SR-12	Face recognition data should be encrypted in the storage. Use well-known cryptographic libraries and robust algorithms.	MI-03, MI-06, MI-07	Encrypt face recognition data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use cbc or gcm mode Integrity Check with hash - Use an alforithm that are stronger than sha256	
TR-63	An attacker can find out the ROOT KEY used for encryption through reverse binary analysis, decrypt the encrypted file, and steal information. An attacker can infer the key used for encryption through statistical analysis of the encrypted file.	Need to preventing reverse analysis of encrypted information Need to protect ROOT encrypt key	SR-17, SR-18	Every encyption time, newly generated random key is used for encryption to make reverse analysis difficult ROOT encrypt key must be protected from binary analysis	MI-14, MI-15	Use random encrypt key - use TRNG (True Random Number Generator) is best - Cryptographically secure pseudorandom number generator can be used alternatively Protect ROOT encryptpion key - HSM (Hardware Secure Module) is best - alternatively White-box Cryptography or Code obfuscation method can be used	

* Test Team 6's system with the provided test cases and then evaluate it.								
		Written by Team 6						
		Cheked and Anaylzed byTeam 5						
Test Cases								
TC Name		Step		Expected	Execution Result	Result	Evaluate	
TC1	id validation	1	type id more than 10 len	cannot type character more than 10	OK	OK	It's negative case. It will be better if describe positive case and note about case type.	
TC2	pass validation	1	type pass more than 20 len	cannot type character more than 20	OK	OK		
TC3	login	1	type id something	check login button is not activated	OK	OK		
		2	make id to empty string	check login button is not activated	OK	OK		
		3	type pass something	check login button is not activated	OK	OK		
		4	type id,pass something	check login button is activated	OK	OK		
		5	disconnect client and server in the local network		OK	OK		
		6	push login button	check alert 'Connection Fail'	OK	OK		
		7	connect client and server in the local network		OK	OK		
		8	Do not meet the condition below - type alphabet and number in id - Minimum eight characters, at least one letter, one number and one special character on password	check login button is activated	OK	OK		
		9	push login button	check alert 'Login Fail'	OK	OK		
		10	type valid id,pass		OK	OK		

			11	push login button	check id,pass,login button component are deactivated secure mode check button activated and checked check running secure run mode (camera is on and I can see the camera)	OK	OK	
	TC4	logout	pre	login is needed		OK	OK	
			1	push logout button	check id,pass components are activated other componens are deactivated all connection with server are disconnected	OK	OK	
	TC5	secure & run mode	pre	login is needed		OK	OK	
			1	enable checkbox of Secure Mode disable checkout of Test Mode	securely receive the image data generated from server camera	OK	OK	
	TC6	secure & test mode	pre	login is needed		OK	OK	
			1	enable checkbox of Secure Mode enable checkout of Test Mode	securely receive the image data generated from server media file	OK	OK	
	TC7	non secure & run mode	pre	login is needed		OK	OK	
			1	disable checkbox of Secure Mode disable checkout of Test Mode	receive the image data generated from server camera	OK	OK	
	TC8	non secure & test mode	pre	login is needed		OK	OK	
			1	disable checkbox of Secure Mode enable checkout of Test Mode	receive the image data generated from server media file	OK	OK	
	TC9	Learn Mode	pre	login is needed select test mode		OK	OK	
			1	push Pause button when no face recognition	photo is stopped. no face recognition Pause button is changed to "Resume need to pause again to Save Picture" button	OK	OK	
			2	push Resume... button	photo is played	OK	OK	
			3	push Pause button when face recognition	photo is stopped. one face recognition is represented Pause button is changed to "Resume" button. Name input is enabled	OK	OK	

		4	type name more than 20 len on Name input	"Learn Mode - Save" button is enabled	OK	OK	
		5	remove and empty name on Name input	"Learn Mode - Save" button is disabled	OK	OK	
		6	type name again on Name input	"Learn Mode - Save" button is enabled	OK	OK	
		7	push "Resume" button	confirm "save done" dialog	OK	OK	

	* Run FlawFinder for static analysis of Team 6's system and then evaluate it.					
	FlawFinder's Output					
	Checked and Analyzed by Team 5					
	FlawFinder Results					
	Strikethrough items - Not Interested in common help code (such as Tensorflow, baseEngine, etc)					
	FlawFinder ID	Sourcecode path (line)	Target	Vulnerability code	Descriptions	Analysis of Team 5
	FF-01	./common/TcpSendRecv.cpp:124	(buffer) memcpy	CWE-120	Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the source data.	need mitigation - alloc size of dst
	FF-02	./common/TcpSendRecv.cpp:129	(buffer) memcpy	CWE-120	Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the source data.	need mitigation - alloc size of dst
	FF-03	./common/TcpSendRecv.cpp:466	(buffer) memcpy	CWE-120	Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the source data.	need mitigation - alloc size of dst
	FF-04	./server/src/faceNet.cpp:122	(misc) open	CWE-362	Check when opening files - can an attacker redirect it (via symlinks), force the opening of special file type (e.g., device files), move things around to create a race condition, control its ancestors, or change its contents? (CWE-362).	Follow the principle of least privilege when assigning access rights to entities in a software system. Denying access to a file can prevent an attacker from replacing that file with a link to a sensitive file.
	FF-05	./server/src/main.cpp:127	(buffer) memcpy	CWE-120	Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the source data.	need mitigation - alloc size of src
	FF-06	./server/src/main.cpp:128	(buffer) memcpy	CWE-120	Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the source data.	need mitigation - alloc size of src
	FF-07	./server/src/main.cpp:129	(buffer) memcpy	CWE-120	Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the source data.	need mitigation - alloc size of src
	FF-08	./server/src/main.cpp:163	(buffer) memcpy	CWE-120	Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the source data.	false alarm
	FF-09	./common/TcpSendRecv.cpp:99	(buffer) strlen	CWE-126	Does not handle strings that are not \0-terminated; if given one it may perform an over-read (it could cause a crash if unprotected) (CWE-126).	false alarm the parameter userid((const gchar*) is called with c_str() which always contains null termination
	FF-10	./common/TcpSendRecv.cpp:100	(buffer) strlen	CWE-126	Does not handle strings that are not \0-terminated; if given one it may perform an over-read (it could cause a crash if unprotected) (CWE-126).	false alarm the parameter userpw(const gchar*) is called with c_str() which always contains null termination
	FF-11	./common/TcpSendRecv.cpp:443	(buffer) strlen	CWE-126	Does not handle strings that are not \0-terminated; if given one it may perform an over-read (it could cause a crash if unprotected) (CWE-126).	false alarm the parameter name(const gchar*) is called with c_str() which always contains null termination
	FF-12	./common/openssl_hostname_validation.cpp:59	(buffer) strlen	CWE-126	Does not handle strings that are not \0-terminated; if given one it may perform an over-read (it could cause a crash if unprotected) (CWE-126).	need mitigation - add a byte for null termination or use std::string
	FF-13	./common/openssl_hostname_validation.cpp:111	(buffer) strlen	CWE-126	Does not handle strings that are not \0-terminated; if given one it may perform an over-read (it could cause a crash if unprotected) (CWE-126).	need mitigation - add a byte for null termination or use std::string
	FF-14	./server/src/faceNet.cpp:47	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	need mitigation - add a check sequence if return of read was ok
	FF-15	./server/src/faceNet.cpp:311	(buffer) strlen	CWE-126	Does not handle strings that are not \0-terminated; if given one it may perform an over-read (it could cause a crash if unprotected) (CWE-126).	null character is inserted between name and image data during data packaging. If tempered?
	FF-16	./server/src/faceNet.cpp:311	(buffer) strlen	CWE-126	Does not handle strings that are not \0-terminated; if given one it may perform an over-read (it could cause a crash if unprotected) (CWE-126).	null character is inserted between name and image data during data packaging. If tempered?
	FF-17	./server/src/main.cpp:45	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	nee mitigation - add a check sequence if return of read was ok
	FF-18	./server/src/main.cpp:133	(buffer) strlen	CWE-126	Does not handle strings that are not \0-terminated; if given one it may perform an over-read (it could cause a crash if unprotected) (CWE-126).	need mitigation - add a byte for null termination to the parameter userid or use std::string
	FF-19	./server/src/main.cpp:134	(buffer) strlen	CWE-126	Does not handle strings that are not \0-terminated; if given one it may perform an over-read (it could cause a crash if unprotected) (CWE-126).	need mitigation - add a byte for null termination to the parameter user_pw or use std::string

	/server/MTCNN_FaceDetection_TensorRT/src/mtcnn.cp	(buffer) memcpy	CWE-120	Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the source data.	Not Interested
	/server/MTCNN_FaceDetection_TensorRT/src/mtcnn.cp	(buffer) memcpy	CWE-120	Does not check for buffer overflows when copying to destination (CWE-120). Make sure destination can always hold the source data.	Not Interested
	/server/MTCNN_FaceDetection_TensorRT/src/pnet_rt.c	(misc) open	CWE-362	Check when opening files – can an attacker redirect it (via symlinks), force the opening of special file type (e.g., device files), move things around to create a race condition, control its ancestors, or change its contents? (CWE-362).	Not Interested
	/server/MTCNN_FaceDetection_TensorRT/src/pnet_rt.c	(misc) open	CWE-362	Check when opening files – can an attacker redirect it (via symlinks), force the opening of special file type (e.g., device files), move things around to create a race condition, control its ancestors, or change its contents? (CWE-362).	Not Interested
	/server/src/baseEngine.cpp:114	(misc) open	CWE-362	Check when opening files – can an attacker redirect it (via symlinks), force the opening of special file type (e.g., device files), move things around to create a race condition, control its ancestors, or change its contents? (CWE-362).	Not Interested
	/server/src/pnet_rt.cpp:25	(misc) open	CWE-362	Check when opening files – can an attacker redirect it (via symlinks), force the opening of special file type (e.g., device files), move things around to create a race condition, control its ancestors, or change its contents? (CWE-362).	Not Interested
	/server/src/pnet_rt.cpp:49	(misc) open	CWE-362	Check when opening files – can an attacker redirect it (via symlinks), force the opening of special file type (e.g., device files), move things around to create a race condition, control its ancestors, or change its contents? (CWE-362).	Not Interested
	/server/MTCNN_FaceDetection_TensorRT/src/common	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	Not Interested
	/server/src/baseEngine.cpp:62	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	Not Interested
	/server/trt_l2norm_helper/l2norm_helper.cpp:29	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	Not Interested
	/server/trt_l2norm_helper/l2norm_helper.cpp:30	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	Not Interested
	/server/trt_l2norm_helper/l2norm_helper.cpp:34	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	Not Interested
	/server/trt_l2norm_helper/l2norm_helper.cpp:32	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	Not Interested
	/server/trt_l2norm_helper/l2norm_helper.cpp:33	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	Not Interested
	/server/trt_l2norm_helper/l2norm_helper.cpp:34	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	Not Interested
	/server/trt_l2norm_helper/l2norm_helper.h:127	(buffer) read	CWE-120, CWE-20	Check buffer boundaries if used in a loop including recursive loops (CWE-120, CWE-20).	Not Interested

	* Run CppCheck for static analysis of Team 6's system and then evaluate it.			
		CppCheck's Output		
		Checked and Analyzed by Team 5		
		cppcheck results		
	Strikethrough items - Not Interested in common help code (such as Tensorflow, baseEngine, etc)			
	CppCheck ID	Sourcecode path (line)	Type	Analysis of Team 5
	CC-01	server/src/main.cpp:196	style [unreadVariable]	false positive
	CC-02	server/src/main.cpp:201	style [unreadVariable]	false positive
	CC-03	server/src/main.cpp:209	style [unreadVariable]	false positive
	CC-04	server/src/main.cpp:229	style [unreadVariable]	false positive
	CC-05	server/src/main.cpp:247	style [unreadVariable]	false positive
	CC-06	server/src/main.cpp:248	style [unreadVariable]	false positive
	CC-07	server/src/videoStreamer.cpp:35	warning [noCopyConstructor]	false positive - use openCV library
	CC-08	server/src/videoStreamer.cpp:35	warning [noOperatorEq]	false positive - use openCV library
	CC-09	server/src/videoStreamer.cpp:60	style [unusedFunction]	unused. if not in use, delete it.
	CC-10	server/src/common.cpp:22	style [unusedFunction]	unused. if not in use, delete it.
	CC-11	server/src/faceNet.cpp:414	style [unusedFunction]	unused. if not in use, delete it.
	CC-12	common/Logger.cpp:110	style [unusedFunction]	unused. if not in use, delete it.
	CC-13	common/Logger.cpp:124	style [unusedFunction]	false positive
	CC-14	server/src/common.cpp:8	style [unusedFunction]	unused. if not in use, delete it.
	CC-15	server/src/videoStreamer.cpp:50	style [unusedFunction]	unused. if not in use, delete it.
	CC-16	server/src/videoStreamer.cpp:43	style [unusedFunction]	unused. if not in use, delete it.
		server/src/mtcnn.cpp:39	warning	Not Interested
		server/src/mtcnn.cpp:39	warning	Not Interested
		server/src/onet_rt.cpp:42	warning	Not Interested
		server/src/onet_rt.cpp:42	warning	Not Interested
		server/src/pnet_rt.cpp:71	warning	Not Interested
		server/src/pnet_rt.cpp:71	warning	Not Interested
		server/src/met_rt.cpp:38	warning	Not Interested

	server/src/net_rt.cpp:38	warning	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	performance	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested
	server/trt_l2norm_helper/l2norm_helper.cp	style	Not Interested

15

[illegible]

[illegible]

[illegible]

[illegible]

CX-410	source/server/src/faceNet.cpp		311	MISRA C 2012 10.4 is violated	MINOR	cppcheck:misra_c_2012_10_04			
CX-411	source/server/src/faceNet.cpp		282	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-412	source/server/src/faceNet.cpp		22	MISRA C 2012 12.3 is violated	MAJOR	cppcheck:misra_c_2012_12_03			
CX-413	source/server/src/faceNet.cpp		35	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-414	source/server/src/faceNet.cpp		40	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-415	source/server/src/faceNet.cpp		118	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-416	source/server/src/faceNet.cpp		123	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-417	source/server/src/faceNet.cpp		146	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-418	source/server/src/faceNet.cpp		305	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-419	source/server/src/faceNet.cpp		335	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-420	source/server/src/faceNet.cpp		307	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-421	source/server/src/faceNet.cpp		330	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-422	source/server/src/faceNet.cpp		375	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-423	source/server/src/faceNet.cpp		391	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-424	source/server/src/faceNet.cpp		392	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-425	source/server/src/faceNet.cpp		393	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-426	source/server/src/faceNet.cpp		335	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-427	source/server/src/faceNet.cpp		378	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-428	source/server/src/faceNet.cpp		98	MISRA C 2012 15.7 is violated	CRITICAL	cppcheck:misra_c_2012_15_07			
CX-429	source/server/src/faceNet.cpp		294	MISRA C 2012 15.7 is violated	CRITICAL	cppcheck:misra_c_2012_15_07			
CX-430	source/server/src/faceNet.cpp		324	MISRA C 2012 17.7 is violated	CRITICAL	cppcheck:misra_c_2012_17_07			
CX-431	source/server/src/faceNet.cpp		310	MISRA C 2012 17.8 is violated	MINOR	cppcheck:misra_c_2012_17_08			
CX-432	source/server/src/faceNet.cpp		312	MISRA C 2012 17.8 is violated	MINOR	cppcheck:misra_c_2012_17_08			
CX-433	source/server/src/faceNet.cpp		298	MISRA C 2012 20.1 is violated	MAJOR	cppcheck:misra_c_2012_20_01			
CX-434	source/server/src/faceNet.cpp		314	MISRA C 2012 21.3 is violated	MINOR	cppcheck:misra_c_2012_21_03			
CX-435	source/server/src/network.cpp		55	MISRA C 2012 10.4 is violated	MINOR	cppcheck:misra_c_2012_10_04			
CX-436	source/server/src/network.cpp		56	MISRA C 2012 10.4 is violated	MINOR	cppcheck:misra_c_2012_10_04			
CX-437	source/server/src/network.cpp		98	MISRA C 2012 10.4 is violated	MINOR	cppcheck:misra_c_2012_10_04			
CX-438	source/server/src/network.cpp		99	MISRA C 2012 10.4 is violated	MINOR	cppcheck:misra_c_2012_10_04			
CX-439	source/server/src/network.cpp		107	MISRA C 2012 10.4 is violated	MINOR	cppcheck:misra_c_2012_10_04			
CX-440	source/server/src/network.cpp		108	MISRA C 2012 10.4 is violated	MINOR	cppcheck:misra_c_2012_10_04			
CX-441	source/server/src/network.cpp		14	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-442	source/server/src/network.cpp		15	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-443	source/server/src/network.cpp		55	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-444	source/server/src/network.cpp		56	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-445	source/server/src/network.cpp		67	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-446	source/server/src/network.cpp		105	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-447	source/server/src/network.cpp		106	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-448	source/server/src/network.cpp		86	MISRA C 2012 12.3 is violated	MAJOR	cppcheck:misra_c_2012_12_03			
CX-449	source/server/src/network.cpp		87	MISRA C 2012 12.3 is violated	MAJOR	cppcheck:misra_c_2012_12_03			
CX-450	source/server/src/network.cpp		88	MISRA C 2012 12.3 is violated	MAJOR	cppcheck:misra_c_2012_12_03			
CX-451	source/server/src/network.cpp		27	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-452	source/server/src/network.cpp		48	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-453	source/server/src/network.cpp		80	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-454	source/server/src/network.cpp		85	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-455	source/server/src/network.cpp		101	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-456	source/server/src/network.cpp		5	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-457	source/server/src/network.cpp		8	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-458	source/server/src/network.cpp		22	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-459	source/server/src/network.cpp		24	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-460	source/server/src/network.cpp		28	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-461	source/server/src/network.cpp		82	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05			
CX-462	source/server/src/network.cpp		21	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-463	source/server/src/network.cpp		23	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-464	source/server/src/network.cpp		43	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-465	source/server/src/network.cpp		59	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-466	source/server/src/network.cpp		76	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-467	source/server/src/network.cpp		122	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-468	source/server/src/network.cpp		123	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-469	source/server/src/network.cpp		124	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-470	source/server/src/network.cpp		125	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-471	source/server/src/network.cpp		63	MISRA C 2012 15.7 is violated	CRITICAL	cppcheck:misra_c_2012_15_07			
CX-472	source/server/src/network.cpp		79	MISRA C 2012 17.8 is violated	MINOR	cppcheck:misra_c_2012_17_08			
CX-473	source/server/src/pnet_rt.cpp		136	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-474	source/server/src/pnet_rt.cpp		146	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-475	source/server/src/pnet_rt.cpp		147	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-476	source/server/src/pnet_rt.cpp		148	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-477	source/server/src/pnet_rt.cpp		149	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-478	source/server/src/pnet_rt.cpp		153	MISRA C 2012 12.1 is violated	MAJOR	cppcheck:misra_c_2012_12_01			
CX-479	source/server/src/pnet_rt.cpp		21	MISRA C 2012 12.3 is violated	MAJOR	cppcheck:misra_c_2012_12_03			
CX-480	source/server/src/pnet_rt.cpp		32	MISRA C 2012 12.3 is violated	MAJOR	cppcheck:misra_c_2012_12_03			
CX-481	source/server/src/pnet_rt.cpp		67	MISRA C 2012 12.3 is violated	MAJOR	cppcheck:misra_c_2012_12_03			
CX-482	source/server/src/pnet_rt.cpp		91	MISRA C 2012 12.3 is violated	MAJOR	cppcheck:misra_c_2012_12_03			
CX-483	source/server/src/pnet_rt.cpp		27	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-484	source/server/src/pnet_rt.cpp		38	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-485	source/server/src/pnet_rt.cpp		43	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-486	source/server/src/pnet_rt.cpp		50	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04			
CX-487	source/server/src/pnet_rt.cpp		152	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06			
CX-488	source/server/src/pnet_rt.cpp		41	MISRA C 2012 17.7 is violated	CRITICAL	cppcheck:misra_c_2012_17_07			
CX-489	source/server/src/pnet_rt.cpp		46	MISRA C 2012 17.7 is violated	CRITICAL	cppcheck:misra_c_2012_17_07			
CX-490	source/server/src/pnet_rt.cpp		85	MISRA C 2012 21.3 is violated	MINOR	cppcheck:misra_c_2012_21_03			
CX-491	source/server/src/pnet_rt.cpp		86	MISRA C 2012 21.3 is violated	MINOR	cppcheck:misra_c_2012_21_03			
CX-492	source/server/src/pnet_rt.cpp		87	MISRA C 2012 21.3 is violated	MINOR	cppcheck:misra_c_2012_21_03			
CX-493	source/server/trt_l2norm_helper/l2norm_helper.cpp		68	MISRA C 2012 10.4 is violated	MINOR	cppcheck:misra_c_2012_10_04			

[illegible]

	CX-578	source/server/src/common.cpp	50	MISRA C 2012 13.4 is violated	MAJOR	cppcheck:misra_c_2012_13_04					
	CX-579	source/server/src/common.cpp	52	MISRA C 2012 13.4 is violated	MAJOR	cppcheck:misra_c_2012_13_04					
	CX-580	source/server/src/common.cpp	69	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04					
	CX-581	source/server/src/common.cpp	70	MISRA C 2012 15.5 is violated	MINOR	cppcheck:misra_c_2012_15_05					
	CX-582	source/server/src/common.cpp	41	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06					
	CX-583	source/server/src/common.cpp	69	MISRA C 2012 15.6 is violated	CRITICAL	cppcheck:misra_c_2012_15_06					
	CX-584	source/server/src/common.cpp	15	MISRA C 2012 21.8 is violated	CRITICAL	cppcheck:misra_c_2012_21_08					
	CX-585	source/server/src/videoStreamer.cpp	4	MISRA C 2012 14.4 is violated	MINOR	cppcheck:misra_c_2012_14_04					

[illegible]

[1] AS-XX can be found in the "AttackScenario_EN" sheet.