

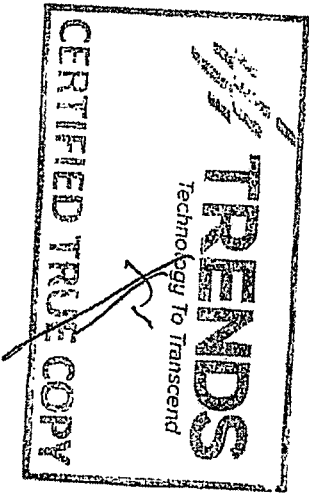
Certificate of Completion

Certifies

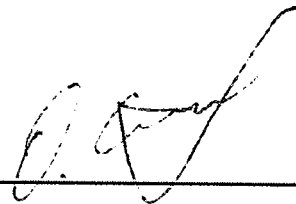
Mardy Anne Vizcarra

For the successful completion of:

Chronicle Certified SOAR Analyst (CCSA)



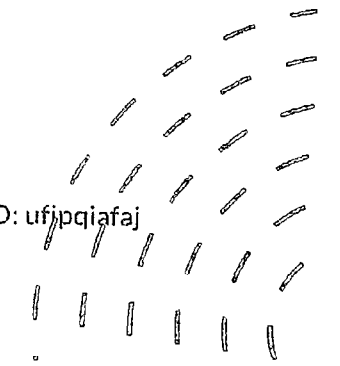
Issued: 2023-09-05



Oleg Siminel, Sr. Security Solutions Architect



Certificate ID: ufjpciafaj



Certificate of Completion

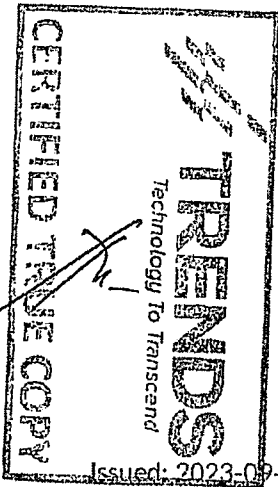
Certifies

Mardy Vizcarra

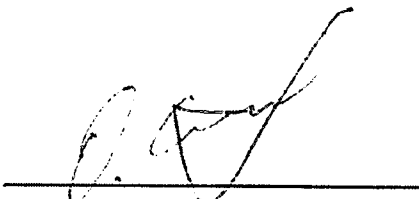


For the successful completion of:

Chronicle SOAR Fundamentals V6 (CSFv6)

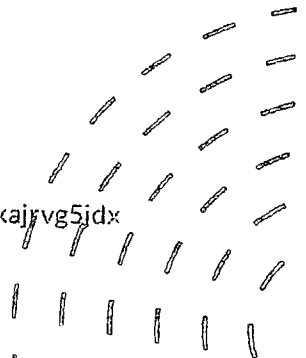


Issued: 2023-09-04


Oleg Siminel, Sr. Security Solutions Architect



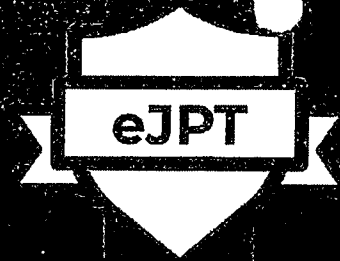
Certificate ID: kajyvg5jdx



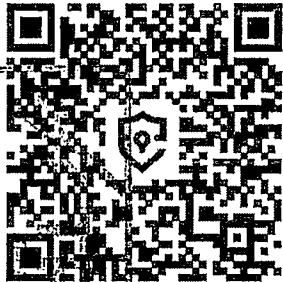
CERTIFICATE OF COMPLETION

PROUDLY PRESENTED TO

**Mardy Anne
Vizcarra**



eJPT eLearnSecurity
Junior Penetration Tester



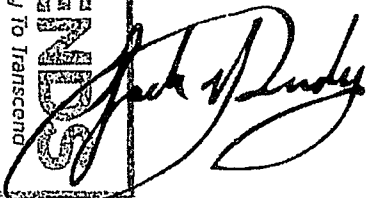
eJPT v1.0
EXAM VERSION

28th of October 2022
DATE

2313273
CERTIFICATION ID

CERTIFIED TRUE COPY

Technology To Transcend



Jack Reedy DIRECTOR OF CYBER SECURITY



Richard McLain PRESIDENT

Certification No. Jer
ECC6012859347

ECSS
EC-Council Certified Security Specialist

EC-Council Certified Security Specialist

This is to acknowledge that

Mardy Anne Vizcarra

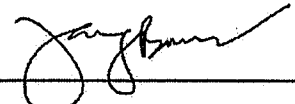
Has successfully completed all requirements and criteria for

EC-Council Certified Security Specialist v9

certification through examination administered by EC-Council

Issue Date: **03 December, 2021**

EC-Council


Sanjay Bavisi, President

CERTIFIED TRUE COPY
TRENDS
Technology To Tomorrow

PeopleCert®

All talents, certified.



This is to certify that

Mardy Anne M. Vizcarra

Has achieved the

ITIL® Foundation Certificate in IT Service Management

Effective from 03 Aug 2020

Expiry date N/A

Certificate number GR671168597MV

Candidate number 9980091728463195

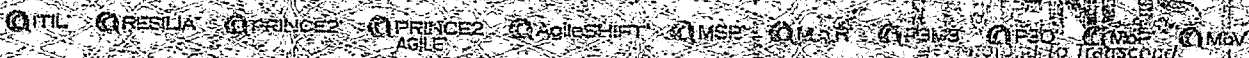
Mark Basham, CEO, AXELOS

Panoraia Theleriti, Certification Qualifier, PeopleCert

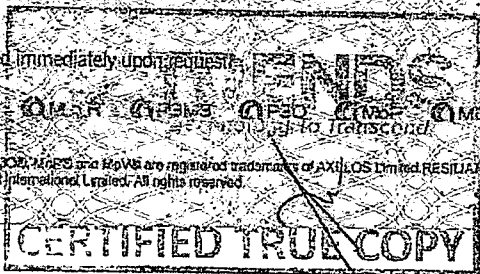
ITIL 4 Edition

Printed on 5 August 2020

This certificate remains the property of the Issuing Examination Institute and shall be returned immediately upon request.



AXELOS, the AXELOS logo, the AXELOS swirl logo, ITIL®, PRINCE2®, PRINCE2 Agile®, AgileSHIFT®, MSP®, ISO®, PMS®, and ISO 9001:2015 are registered trademarks of AXELOS Limited. RESILIA® is a trademark of AXELOS Limited. PeopleCert and PeopleCert All talents, certified, are registered trademarks of PeopleCert International Limited. All rights reserved.



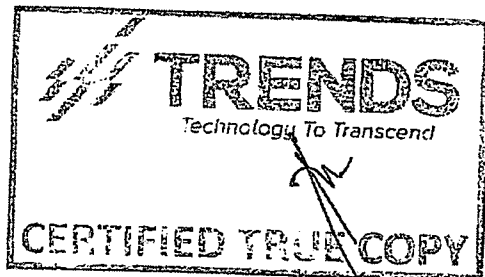
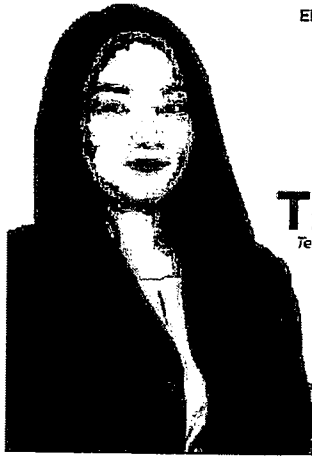
Trends & Technologies, Inc.

MARDY

MARDY ANNE M. VIZCARRA

TTI-1623


EMPLOYEE'S SIGNATURE






October 12, 2023

CERTIFICATE OF EMPLOYMENT

This certifies that Ms. Mardy Anne M. Vizcarra is an employee of Trends & Technologies, Inc. from August 27, 2019 up to the present and holds a permanent position of SOC Team Lead - Security Operations.

This certification is issued to comply with the bidding requirements of the Land Bank of the Philippines.


Grace R. Lorenzo
Human Resources Head

Trends & Technologies, Inc.
23rd Floor Trafalgar Plaza
105 H.V. Dela Costa Street, Salcedo Village
Makati City 1227 Philippines
Phone: +63 2 811 8181 Fax: +63 2 814 0130
www.trends.com.ph



TRENDS

Technology To Transcend

I. PERSONAL INFORMATION

NAME: **VIZCARRA** **MARDY ANNE** **MANAYSAY**
 (LAST NAME) (FIRST NAME) (MIDDLE NAME)

GROUP: **MANAGED ICT SERVICES** POSITION: **SOC TEAM LEAD**

DIVISION: **SERVICE OPERATIONS** DATE HIRE: **AUG 27, 2019**

II. WORK EXPERIENCES

ITEM	INCLUSIVE DATES	COMPANY NAME	POSITION	DESCRIPTION OF FUNCTION
1.	AUG 2019 – PRESENT	TRENDS & TECHNOLOGIES, INC.	SOC MANAGER	<p>Service Operations Management</p> <ul style="list-style-type: none"> Review and approve advisories. Report to immediate head on significant events that happened on the assigned shift and ensuring smooth and orderly transition to the incoming team member. <p>Service Operations Management - Event & Monitoring Management</p> <ul style="list-style-type: none"> Assist and guide SOC Analysts in the monitoring of security events for proper categorization and prioritization. Assist and guide SOC Analysts in the creation and updating of tickets. Provide assistance and appropriate actions in remediation of critical information security incidents. <p>Service Operations Management - Incident Management</p> <ul style="list-style-type: none"> Act as an Incident Handler for P1 and P2 incidents Escalate to Incident Manager for P1 and P2 incidents. For non P1 and non P2 incident, manage incidents and manage escalation. Communicate with Trends SOC Analysts/ Incident Responders and communicate update to Client and Trends internal resources. Projects handled: <ul style="list-style-type: none"> Managed Security Services in a Mutual Life Insurance Company Managed IT Security, Managed Wi-Fi, Managed Network in a Pharmaceutical Company Managed Security Operations Center in a Government Financial Institution Managed Security Services in four (4) Government Financial Institution

Corporate Office
 6F Trafalgar Plaza 105 H.V. Dela Costa St.
 Salcedo Village, 1227 Makati City Philippines

Email: info@trends.com.ph
 Phone: (+632) 811 8181
 Fax: (+632) 814 0130

MAKATI | CEBU | DAVAO | HANOI | DA NANG | HO CHI MINH
 www.trends.com.ph



TRENDS

Technology To Transcend

2.	MAY 2015 – JAN 2018	ALFAMART	OIC/ STORE LEADER	
3.	SEP 2014 – MAR 2015	EVER PLUS SUPERMARKET	COUNTER HEAD	
4.	SEP 2013 – SEP 2014	ROBINSON'S DEPARTMENT STORE	CASHIER	
5.	MAR – JUL 2012	MANILA INTERNATIONAL AIRPORT AUTHORITY	ADMIN – INTERNAL AUDIT DEPT	ANSWERS PHONE INQUIRIES, ENCODES CORRESPONDENCE, FILES DOCUMENTS

III. EDUCATIONAL BACKGROUND

	DATES	SCHOOL	DEGREE
COLLEGE	2018 - 2019	INFOTECH COLLEGE OR ARTS AND SCIENCES - SUCAT	BS INFORMATION TECHNOLOGY
	2010 – 2012	INFOTECH COLLEGE OR ARTS AND SCIENCES - SUCAT	ASSOCIATE IN COMPUTER SCIENCE TECHNOLOGY
POST GRADUATE STUDIES	N/A		

IV. SEMINARS AND TRAININGS ATTENDED

A. FOREIGN TRAININGS/ SEMINARS

ITEM	COURSE NAME	TRAINING PROVIDER	VENUE	INCLUSIVE DATES
1.	N/A			
2.				
3.				

B. LOCAL TRAININGS/SEMINARS

ITEM	SEMINAR TITLE	TRAINING PROVIDER	VENUE	INCLUSIVE DATES
1.	EC-COUNCIL CERTIFIED THREAT INTELLIGENCE ANALYST CTIA TRAINING	TRENDS	Makati City	SEP 2022
2.	CCNA TRAINING	TRENDS	Makati City	JUL 2022
3.	ITIL 4 FOUNDATION TRAINING	TRENDS	Makati City	JUL 2020

C. CERTIFICATIONS

ITEM	TITLE	INCLUSIVE DATES
1.	NSE1 NETWORK SECURITY ASSOCIATE	AUG 12, 2023 – AUG 12, 2025
2.	NSE2 NETWORK SECURITY ASSOCIATE	AUG 25, 2023 – AUG 25, 2025
3.	NSE3 NETWORK SECURITY ASSOCIATE	AUG 25, 2023 – AUG 25, 2025
4.	CTIA - EC COUNCIL CERTIFIED THREAT INTELLIGENCE ANALYST	NOV 17, 2022 – NOV 16, 2025
5.	CEH - CERTIFIED ETHICAL HACKER	OCT 20, 2021 – OCT 19, 2024
6.	Chronicle Certified SOAR Analyst (CCSA)	SEP 5, 2023
7.	Chronicle SOAR Fundamentals v6 (CSFv6)	SEP 4, 2023
8.	EJPT ELEARNSecurity JUNIOR PENETRATION TESTER	OCT 28, 2022
9.	ECSS - EC COUNCIL CERTIFIED SECURITY SPECIALIST V9	DEC 3, 2021
10.	ITIL® FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT	AUG 3, 2020

Corporate Office
6F Trafalgar Plaza 105 H.V. Dela Costa St.
Salcedo Village, 1227 Makati City Philippines

Email: info@trends.com.ph
Phone: (+632) 811 8181
Fax: (+632) 814 0130

MAKATI | CEBU | DAVAO | HANOI | DA NANG | HO CHI MINH

www.trends.com.ph



TRENDS

Technology To Transcend

D. PROJECT HANDLED

ITEM	COMPANY	ROLE	PROJECT DESCRIPTION	INCLUSIVE DATES
1.	A Mutual Life Insurance Company	SOC Manager	Managed Security Service	2019 - 2021
2.	A Pharmaceutical Company	SOC Manager	Managed IT Security, Managed Wi-Fi, Managed Network	2019 - 2022
3.	A Government Financial Institution	SOC Manager	Managed Security Operations Center	2019 - 2022
4.	A Government Financial Institution	SOC Manager	Managed Security Services	2022 - 2024
5.	A Government Financial Institution	SOC Manager	Managed Security Services	2022 - 2024
6.	A Government Financial Institution	SOC Manager	Managed Security Services	2022 - 2024
7.	A Government Financial Institution	SOC Manager	Managed Security Services	2023 - 2025

Corporate Office
6F Trafalgar Plaza 105 H.V. Dela Costa St.
Salcedo Village, 1227 Makati City Philippines

Email: info@trends.com.ph
Phone: (+632) 811 8181
Fax: (+632) 814 0130

MAKATI | CEBU | DAVAO | HANOI | DA NANG | HO CHI MINH

www.trends.com.ph

EC-Council

Certification Number
ECC3140697852

C | EH
Certified Ethical Hacker

Certified Ethical Hacker

This is to acknowledge that

ERLYN BARREDO

has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

Issue Date: **11 October, 2022**

Expiry Date: **10 October, 2025**



#0732

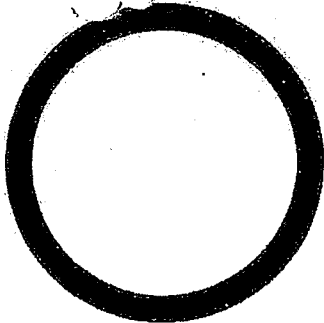
ISO/IEC 17024

Personnel Certification Program

A handwritten signature in black ink, appearing to read "Sanjay Bavisi", is written over a horizontal line.

Sanjay Bavisi, President

CERTIFIED TRUE COPY



CERTIFICATE OF COMPLETION

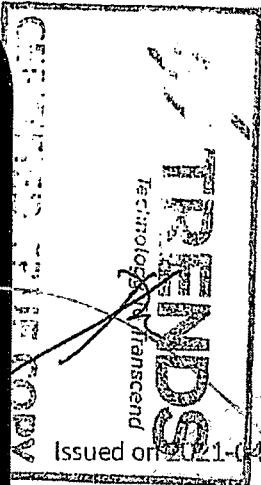


CERTIFIES

Erlyn Barredo

For the successful completion of:

General Platform Knowledge Evaluation (GPKE)

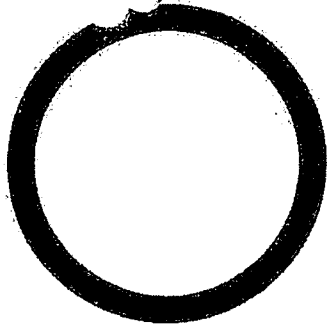


Issued on 2021-04-30

Oleg Siminel, Sr. Security Solutions Architect

Certificate ID: 8gfsu9uqpt





CERTIFICATE OF COMPLETION

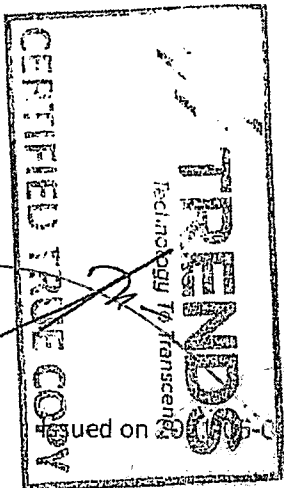
CERTIFIES

Erlyn Barredo



For the successful completion of:

Siemplify Certified SOAR Operator (SCSO)



Oleg Siminel, Sr. Security Solutions Architect

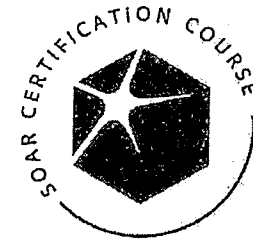


Certificate ID: k1tg8lokrf

CERTIFICATE OF COMPLETION

CERTIFIES

Erlyn Barredo

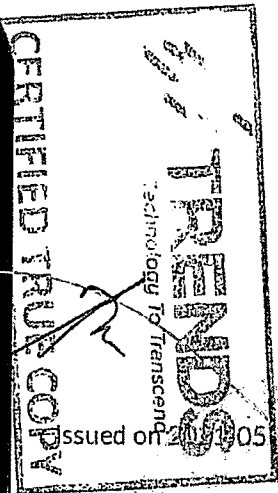


For the successful completion of:

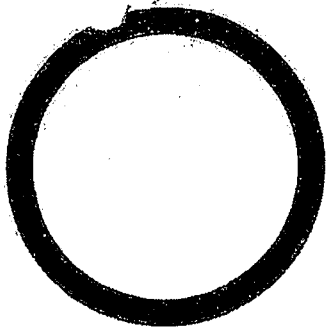
Siemplify Certified SOAR Analyst (SCSA)

A handwritten signature in black ink, appearing to read "O. Siminel", written over a horizontal line.

Oleg Siminel, Sr. Security Solutions Architect



Certificate ID: yyndpmk2fa



CERTIFICATE OF COMPLETION

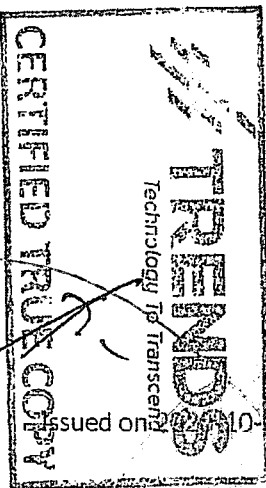
CERTIFIES

Erlyn Barredo



For the successful completion of:

Siemplify Platform Fundamentals



Oleg Siminel, Sr. Security Solutions Architect

Certificate ID: gnbjbozp68



Trends & Technologies, Inc.

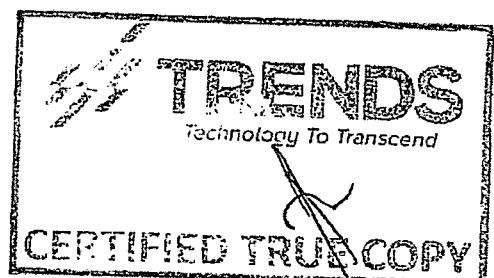
ERL

ERLYN B. BARREDO

RTC-0002



EMPLOYEE'S SIGNATURE






October 12, 2023

CERTIFICATE OF EMPLOYMENT

This certifies that Ms. Eryln B. Barredo is an employee of Trends & Technologies, Inc. from December 03, 2018 up to the present and holds a permanent position of Technology Lead.

This certification is issued to comply with the bidding requirements of the Land Bank of the Philippines.


Grace R. Lorenzo
Human Resources Head

Trends & Technologies, Inc.
23rd Floor Trafalgar Plaza
105 H.V. Dela Costa Street, Salcedo Village
Makati City 1227 Philippines
Phone: +63 2 811 8181 Fax: +63 2 814 0130
www.trends.com.ph



TRENDS

Technology To Transcend

I. PERSONAL INFORMATION

NAME: **BARREDO** **ERLYN** **BARISAL**
 (LAST NAME) (FIRST NAME) (MIDDLE NAME)

GROUP: MANAGED ICT SERVICES POSITION: SECURITY SOLUTIONS SUPPORT TECHNOLOGY LEAD

DIVISION: SERVICES DATE HIRE: DEC 3, 2018

II. WORK EXPERIENCES

ITEM	INCLUSIVE DATES	COMPANY NAME	POSITION	DESCRIPTION OF FUNCTION
1.	DEC 2018 – PRESENT	TRENDS & TECHNOLOGIES, INC	SECURITY SOLUTIONS SUPPORT TECHNOLOGY LEAD	<ul style="list-style-type: none"> • Responsible for implementing and maintaining the security solutions used on our Managed Security Services. • Lead implementation and operational support for Managed Security services • Lead all the activities under the Security Solution Support team. • Responsible for supporting, and maintaining the following solutions: SIEM, SOAR, WAF, EDR/AV, DLP/DE, Vulnerability Management, Threat Intel platform. • Assists with complex projects and assumes ongoing support of security operations. • Solution Architect (Solution Designing & Integration Activities) • Manage resolution, Incident, and Service Request Tickets in accordance with the MICTS Policies and Processes. • Ensure that the appropriate escalation processes are followed in a timely manner, ensuring that high Severity/ Priority incidents are managed according to standards. • Oversee customer implementations, and integration. Become the main point of contract for client's technical issues. • Conduct presentations, simulation, proof-of-concept, implementation, and support to client of assigned product as needed. • Projects handled: <ul style="list-style-type: none"> ○ Managed Security Services in a Mutual Life Insurance Company ○ Managed IT Security, Managed Wi-Fi, Managed Network in a Pharmaceutical Company ○ Managed Security Operations Center in a Government Financial Institution ○ Managed Security Services in four (4) Government Financial Institution
2.	APR 2015 – JUL 2017	CONVERGYS PHILIPPINES, INC.	ASSOCIATE TRAINER	<ul style="list-style-type: none"> • Mentored new trainers. • Acted as SME for new training curriculum. • Facilitated classroom training to teach program product knowledge, call handling

Corporate Office
 6F Trafalgar Plaza 105 H.V. Dela Costa St.
 Salcedo Village, 1227 Makati City Philippines

Email: info@trends.com.ph
 Phone: (+632) 811 8181
 Fax: (+632) 814 0180

MAKATI | CEBU | DAVAO | HANOI | DA NANG | HO CHI MINH
 www.trends.com.ph



TRENDS

Technology To Transcend

				<p>skills, customer service/sales skills and program process and procedures.</p> <ul style="list-style-type: none"> Facilitated continuing education for existing call center staff for new products, services, customer service skills, etc.
3.	APR 2013 – APR 2015	CONVERGYS PHILIPPINES, INC.	PRODUCT READY TRAINER	<ul style="list-style-type: none"> Facilitates classroom training to teach program product knowledge, call handling skills, customer service/sales skills and program process and procedures. Facilitates continuing education for existing call center staff for new products, services, customer service skills, etc. Monitors agent calls and agent performance to identify training gaps. Participates in calibration meetings with the Client, QA and management team to ensure information being trained is up to date
4.	APR 2011 – APR 2013	CONVERGYS PHILIPPINES, INC.	TECHNICAL SUPPORT SPECIALIST	<ul style="list-style-type: none"> WFE POC (collates WFE errors, issues, and reports them. Monitors WFE Compliance report) / Communication Protégé (ensures EOP policy is always observed, collaborates with Comm Coaches) / MRSP POC (blasts updates, recent product promotions, and monitors teams upsells) Diagnose and resolve technical hardware and software issues involving internet connectivity, IPTV, VOIP and more. Interact with customers to provide and process information in response to inquiries, concerns, and requests about products and services. Accurately process and record

III. EDUCATIONAL BACKGROUND

	DATES	SCHOOL	DEGREE
COLLEGE	2006 – 2011, 2017 – 2019	UNIVERSITY OF THE EAST	BS COMPUTER ENGINEERING
POST GRADUATE STUDIES	N/A		

IV. SEMINARS AND TRAININGS ATTENDED

A. FOREIGN TRAININGS/ SEMINARS

ITEM	COURSE NAME	TRAINING PROVIDER	VENUE	INCLUSIVE DATES
1.	N/A			
2.				
3.				

B. LOCAL TRAININGS/SEMINARS

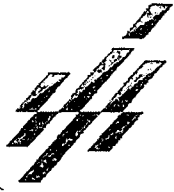
ITEM	SEMINAR TITLE	TRAINING PROVIDER	VENUE	INCLUSIVE DATES
1.	CERTIFIED ETHICAL HACKER TRAINING	TRENDS	VIRTUAL	MAY 10 - 12 & 14 - 15, 2021
2.	CISCO IP TELEPHONY AND ROUTING	RIVAN SCHOOL OF TECHNOLOGY, INC.		SEP 10, 2018

Corporate Office
6F Trafalgar Plaza 105 H.V. Dela Costa St.
Salcedo Village, 1227 Makati City Philippines

Email: info@trends.com.ph
Phone: (+632) 811 8181
Fax: (+632) 814 0130

MAKATI | CEBU | DAVAO | HANOI | DA NANG | HO CHI MINH

www.trends.com.ph



TRENDS

Technology To Transcend

3.	CYBER SECURITY AWARENESS	UE MANILA		JAN 13, 2018
----	--------------------------	-----------	--	--------------

C. CERTIFICATIONS

ITEM	TITLE	INCLUSIVE DATES
1.	CEH - CERTIFIED ETHICAL HACKER	OCT 11, 2022 – OCT 10, 2025
2.	GENERAL PLATFORM KNOWLEDGE EVALUATION - GPKE	APR 30, 2021
3.	SIEMPLIFY CERTIFIED SOAR OPERATOR - SCSO	MAY 2, 2021
4.	SIEMPLIFY CERTIFIED SOAR ANALYST - SCSA	MAY 7, 2021
5.	SIEMPLIFY PLATFORM FUNDAMENTALS	OCT 30, 2020

D. PROJECT HANDLED

ITEM	COMPANY	ROLE	PROJECT DESCRIPTION	INCLUSIVE DATES
1.	A Mutual Life Insurance Company	Security Solutions Support Technology Lead	Managed Security Service	2018 - 2021
2.	A Pharmaceutical Company	Security Solutions Support Technology Lead	Managed IT Security, Managed Wi-Fi, Managed Network	2017 - 2022
3.	A Government Financial Institution	Security Solutions Support Technology Lead	Managed Security Operations Center	2019 - 2022
4.	A Government Financial Institution	Security Solutions Support Technology Lead	Managed Security Services	2022 - 2024
5.	A Government Financial Institution	Security Solutions Support Technology Lead	Managed Security Services	2022 - 2024
6.	A Government Financial Institution	Security Solutions Support Technology Lead	Managed Security Services	2022 - 2024
7.	A Government Financial Institution	Security Solutions Support Technology Lead	Managed Security Services	2023 - 2025

Corporate Office
6F Trafalgar Plaza 105 H.V. Dela Costa St.
Salcedo Village, 1227 Makati City Philippines

Email: info@trends.com.ph
Phone: (+632) 811 8184
Fax: (+632) 814 0130

MAKATI | CEBU | DAVAO | HANOI | DA NANG | HO CHI MINH

www.trends.com.ph

Certification Number
ECC0975281436

E|CIH
EC-Council Certified Incident Handler

EC-Council Certified Incident Handler

This is to acknowledge that

Gemalyn Cabanos

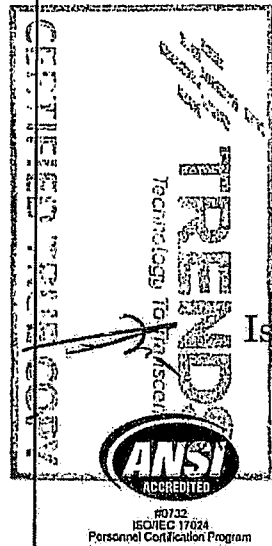
has successfully completed all requirements and criteria for

EC-Council Certified Incident Handler

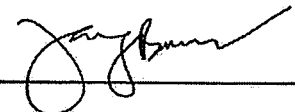
certification through examination administered by EC-Council

Issue Date: **20 July, 2022**

Expiry Date: **19 July, 2025**



EC-Council


Sanjay Bavisi, President



NSE Certification
Program

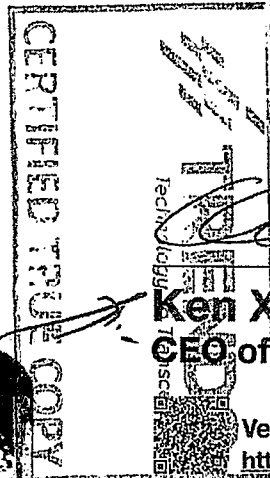


**This certifies that
Gemalyn Cabanos
has achieved
NSE 2 Network Security Associate**

Date of achievement: July 14, 2023

Valid until: July 14, 2025

Certification Validation number: szBFLxoUi7



Ken Xie
CEO of Fortinet

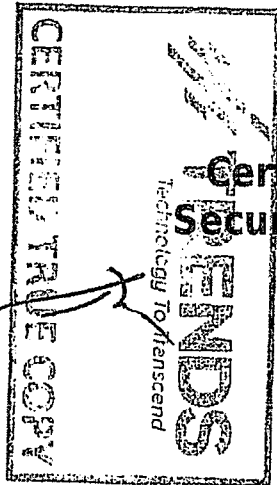
Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

Michael Xie
President and Chief Technology
Officer (CTO), Fortinet

Trellix



Certificate of Completion



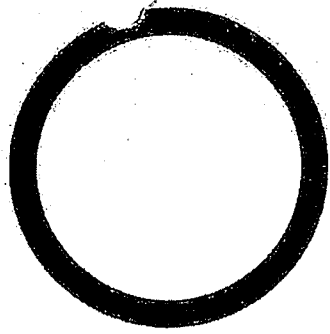
Gem Cabanos

has successfully completed

**Certified Product Specialist:
Security Information and Event
Management (SIEM)**

on 16-MAR-2023

Education Services



CERTIFICATE OF COMPLETION



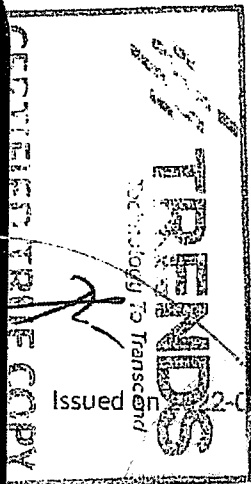
CERTIFIES

Gem Cabanos

For the successful completion of:

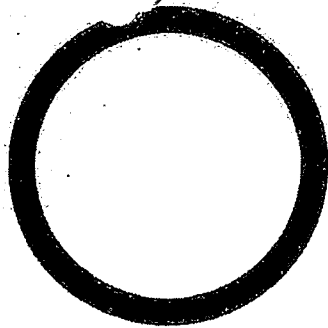
Siemplify Platform Fundamentals - Version 6+ (SPFv6)

Oleg Siminel, Sr. Security Solutions Architect



Certificate ID: rjmhukzdxm





CERTIFICATE OF COMPLETION



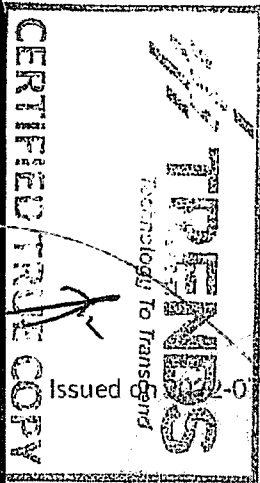
CERTIFIES

Gem Cabanos

For the successful completion of:

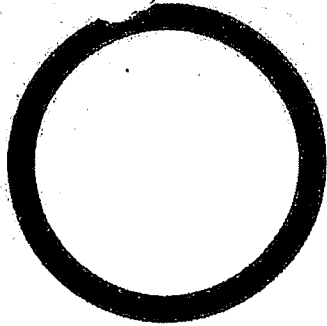
Siemplify Certified SOAR Analyst (SCSA)

Oleg Siminel, Sr. Security Solutions Architect



Certificate ID: molvxc9hfhz





CERTIFICATE OF COMPLETION

CERTIFIES

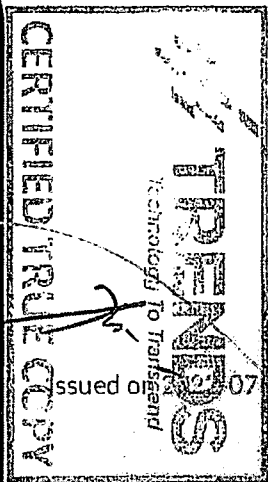
Gem Cabanos



For the successful completion of:

Siemplify Certified SOAR Operator (SCSO)

Oleg Siminel, Sr. Security Solutions Architect



Certificate ID: 1rpi2jdzfo



PeopleCert®

All talents, certified.



This is to certify that

Gemalyn Cabanos

Has achieved the

**ITIL® Foundation Certificate in
IT Service Management**

Effective from **16 May 2019**

Expiry date **N/A**

Certificate number **GR671016809GC**

Candidate number **9980060002531861**

Mark Basham, CEO, AXELOS

Panoraja Thelarithi, Certification Qualifier, PeopleCert

ITIL 4 Edition

Printed on 17 May 2019

This certificate remains the property of the issuing Examination Institute and shall be returned immediately upon request.



AXELOS, the AXELOS logo, the AXELOS word logo, ITIL®, PRINCE2®, PRINCE2 Agile®, AgileSHIFT®, MSP®, M. & R., P3O®, MoPS and MoV® are registered trademarks of AXELOS Limited. RESILIA™ is a trademark of AXELOS Limited. PeopleCert and 'PeopleCert All talents, certified.' are registered trademarks of PeopleCert International Limited. All rights reserved.

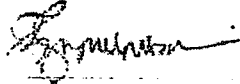


Trends & Technologies, Inc.

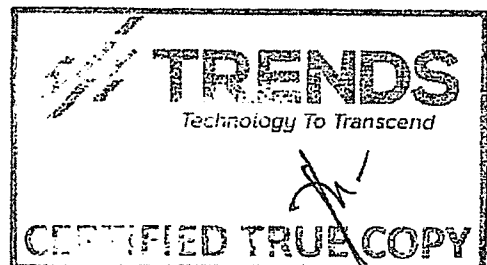
GEM

GEMALYN B. CABANOS

TTI-1475



EMPLOYEE'S SIGNATURE






October 12, 2023

CERTIFICATE OF EMPLOYMENT

This certifies that Ms. Gemalyn B. Cabanos is an employee of Trends & Technologies, Inc. from February 11, 2019 up to the present and holds a permanent position of Senior Correlation Engineer.

This certification is issued to comply with the bidding requirements of the Land Bank of the Philippines.


Grace R. Lorenzo
Human Resources Head

Trends & Technologies, Inc.
23rd Floor Trafalgar Plaza
105 H.V. Dela Costa Street, Salcedo Village
Makati City 1227 Philippines

Phone: +63 2 811 8181 Fax: +63 2 814 0130
www.trends.com.ph



TRENDS

Technology To Transcend

I. PERSONAL INFORMATION

NAME: **CABANOS** (LAST NAME) **GEMALYN** (FIRST NAME) **BERISO** (MIDDLE NAME)

GROUP: MANAGED ICT SERVICES POSITION: SENIOR CORRELATION ENGINEER

DIVISION: SERVICES DATE HIRE: FEB 11, 2019

II. WORK EXPERIENCES

ITEM	INCLUSIVE DATES	COMPANY NAME	POSITION	DESCRIPTION OF FUNCTION
1.	APR 2022 – PRESENT	TRENDS & TECHNOLOGIES, INC	SENIOR CORRELATION ENGINEER	<ul style="list-style-type: none"> Responsible for operationalizing the policy of infra & security solutions, especially the SIEM, NMS, SOAR and other solutions that need use case development on Managed Services. <u>Rule Tuning and Creation</u>. Collaborate with the Correlation Tuning Team to tune or create new SIEM correlation rules based on emerging threats and vulnerabilities. (For such solutions; SIEM, NMS, SOAR) <u>Playbook Tuning and Creation</u>. Work on creating and tuning and optimizing SOAR playbooks to streamline Incident response processes. <u>Assist Team Lead (TL) in Ticket Delivery</u>. Collaborate closely with the Team Lead to ensure that all tickets and requests related to tuning and operational readiness are effectively addressed and delivered within established timelines. <u>Collaborate on Security Solutions Tuning</u>. Work with the Team Lead to ensure that security solutions such as NETWORK MONITORING SYSTEM, WAF Incap-rules, and other security policies are effectively tuned and operationalized. <u>Use Case Development Support</u>. Contribute technical expertise to refine and implement use cases for improved threat detection. <u>Documentation and Tracker Maintenance</u>. Ensure that all relevant documents and trackers, including updates to playbooks, correlation policies, and use cases, are maintained accurately and are readily accessible to the team. <u>Team Support and Collaboration</u>. Collaborate with playbook owners across Infra and security Services Operations to facilitate fine-tuning and operationalization efforts. <u>Additional Support</u>. Collaborate with the Team Lead and other team members to address emerging security challenges and implement proactive solutions. Projects handled: <ul style="list-style-type: none"> Managed Security Services in four (4) government financial institution

Corporate Office
6F Trafalgar Plaza 105 H.V. Dela Costa St.
Salcedo Village, 1227 Makati City Philippines

Email: info@trends.com.ph
Phone: (+632) 811 8181
Fax: (+632) 814 0130

MAKATI | CEBU | DAVAO | HANOI | DA NANG | HO CHI MINH

www.trends.com.ph



TRENDS

Technology To Transcend

2.	FEB 2019 – APR 2022	TRENDS & TECHNOLOGIES, INC.	SECURITY SUPPORT	<ul style="list-style-type: none"> • Experienced on handling McAfee SIEM (Security Information and Event Management) <ul style="list-style-type: none"> ◦ Data Gathering, scrutinizing Supported and Non-Supported Data Sources ◦ Implementation Proper in relevance with Firewall Rules and Troubleshooting Techniques • Associated with TAC Support <ul style="list-style-type: none"> ◦ Correlation Rule Fine Tuning • Creation of Rules which were collaborated with clients • Fine Tuning of Pre-defined rules for the enhancement of monitoring alerts • BeyondTrust (Privileged Account Management) <ul style="list-style-type: none"> ◦ Data Gathering ◦ Implementation Proper • Enrollment of Assets and Accounts <ul style="list-style-type: none"> ◦ Basic Troubleshooting • Associated with Asset owners. <ul style="list-style-type: none"> ◦ Creation of Smart Rules • Projects handled: <ul style="list-style-type: none"> ◦ Managed Security Services in a Mutual Life Insurance Company ◦ Managed IT Security, Managed Wi-Fi, Managed Network in a Pharmaceutical Company ◦ Managed Security Operations Center in a Government Financial Institution
----	---------------------	-----------------------------	------------------	---

III. EDUCATIONAL BACKGROUND

	DATES	SCHOOL	DEGREE
COLLEGE	JUN 2013 – MAR 2018	BICOL STATE COLLEGE OF APPLIED SCIENCES AND TECHNOLOGY	BS ELECTRONICS ENGINEERING
POST GRADUATE STUDIES	N/A	N/A	N/A

IV. SEMINARS AND TRAININGS ATTENDED

A. FOREIGN TRAININGS/ SEMINARS

ITEM	COURSE NAME	TRAINING PROVIDER	VENUE	INCLUSIVE DATES
1.	N/A			
2.				
3.				

B. LOCAL TRAININGS/SEMINARS

ITEM	SEMINAR TITLE	TRAINING PROVIDER	VENUE	INCLUSIVE DATES
1.	EC-COUNCIL CERTIFIED INCIDENT HANDLER (ECIH) TRAINING	TRENDS	MAKATI CITY	DEC 27 - 29, 2021
2.	COMPTIA CYBERSECURITY ANALYST+ TRAINING AND EXAMINATION	TRENDS	MAKATI CITY	MAR 22 – 26, 2021
3.	CERTIFIED ETHICAL HACKER V10	TRENDS	MAKATI CITY	JUN 24-28 2019

Corporate Office
6F Trafalgar Plaza 105 H.V. Dela Costa St.
Salcedo Village, 1227 Makati City Philippines

Email: info@trends.com.ph
Phone: (+632) 811 8181
Fax: (+632) 814 0130

MAKATI | CEBU | DAVAO | HANOI | DA NANG | HO CHI MINH

www.trends.com.ph



TRENDS

Technology To Transcend

4.	ITIL 4	TRENDS	MAKATI CITY	MAY 14-15 2019
5.	COMPTIA SECURITY +	TRENDS	MAKATI CITY	MAR 25-29 2019
6.	13TH IECEP-BSC STUDENT SUMMIT	IECEP		AUG 13, 2016

C. CERTIFICATIONS

ITEM	TITLE	INCLUSIVE DATES
1.	EC CERTIFIED INCIDENT HANDLER (ECIH)	JUL 20, 2022 – JUL 19, 2025
2.	NSE2 NETWORK SECURITY ASSOCIATE	JUL 14, 2023 – JUL 14, 2025
3.	TRELLIX CERTIFIED PRODUCT SPECIALIST: SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) 11.3 PROFICIENCY EXAM	MAR 16, 2023
4.	SIMPLIFY PLATFORM FUNDAMENTALS - VERSION 6+ (SPFV6)	MAY 26, 2022
5.	SIMPLIFY CERTIFIED SOAR ANALYST (SCSA)	JUL 11, 2022
6.	SIMPLIFY CERTIFIED SOAR OPERATOR (SCSO)	JUL 11, 2022
7.	ITIL FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT	MAY 16, 2019

D. PROJECT HANDLED

ITEM	COMPANY	ROLE	PROJECT DESCRIPTION	INCLUSIVE DATES
1.	A Mutual Life Insurance Company	SECURITY SUPPORT	Managed Security Service	2018 - 2021
2.	A Pharmaceutical Company	SECURITY SUPPORT	Managed IT Security, Managed Wi-Fi, Managed Network	2017 - 2022
3.	A Government Financial Institution	SECURITY SUPPORT	Managed Security Operations Center	2019 - 2022
4.	A Government Financial Institution	SENIOR CORRELATION ENGINEER	Managed Security Services	2022 - 2024
5.	A Government Financial Institution	SENIOR CORRELATION ENGINEER	Managed Security Services	2022 - 2024
6.	A Government Financial Institution	SENIOR CORRELATION ENGINEER	Managed Security Services	2022 - 2024
7.	A Government Financial Institution	SENIOR CORRELATION ENGINEER	Managed Security Services	2023 - 2025

Corporate Office
6F Trafalgar Plaza 105 H.V. Dela Costa St.
Salcedo Village, 1227 Makati City Philippines

Email: info@trends.com.ph
Phone: (+632) 811 8181
Fax: (+632) 814 0130

MAKATI | CEBU | DAVAO | HANOI | DA NANG | HO CHI MINH

www.trends.com.ph

BILL OF MATERIALS

**BILL OF MATERIALS
for Government Insurance Cluster**

Item	Product Description	Qty
1	Dell PowerEdge Server	1 Lot

Item	Product Description	Qty
		Aggregated daily data ingestion
2	Splunk Cloud Set License with twelve (12) months comprehensive searchability and Data Encryption at Rest Subscription for Government Service Insurance System	24 GB
	Splunk Cloud Set License with twelve (12) months comprehensive searchability and Data Encryption at Rest Subscription for Social Security System	48 GB
	Splunk Cloud Set License with twelve (12) months comprehensive searchability and Data Encryption at Rest Subscription for Bureau of the Treasury	17 GB
	Splunk Cloud Set License with twelve (12) months comprehensive searchability and Data Encryption at Rest Subscription for Philippine Deposit Insurance Corporation	15 GB

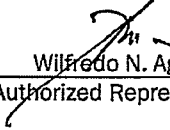
Item	Product Description	Qty	
		Endpoint	Server
3	CrowdStrike Falcon + Spotlight Vulnerability Management License Subscription for Government Service Insurance System	4,000	400
	CrowdStrike Falcon + Spotlight Vulnerability Management License Subscription for Social Security System	7,800	200
	CrowdStrike Falcon + Spotlight Vulnerability Management License Subscription for Bureau of the Treasury	1,450	150
	CrowdStrike Falcon + Spotlight Vulnerability Management License Subscription for Philippine Deposit Insurance Corporation	1,118	82

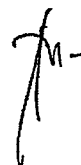
Item	Product Description	Qty
4	Tenable License Subscription for Government Service Insurance System	1 Lot
	Tenable License Subscription for Social Security System	1 Lot
	Tenable License Subscription for Bureau of the Treasury	1 Lot
	Tenable License Subscription for Philippine Deposit Insurance Corporation	1 Lot

Item	Product Description	Qty
5	Google Chronicle SOAR License Subscription for Government Service Insurance System	1 Lot
	Google Chronicle SOAR License Subscription for Social Security System	1 Lot
	Google Chronicle SOAR License Subscription for Bureau of the Treasury	1 Lot
	Google Chronicle SOAR License Subscription for Philippine Deposit Insurance Corporation	1 Lot

Item	Product Description	Qty
6	Cyble License Subscription + Unlimited Takedown Services for Government Service Insurance System	1 Lot
	Cyble License Subscription + Unlimited Takedown Services for Social Security System	1 Lot
	Cyble License Subscription + Unlimited Takedown Services for Bureau of the Treasury	1 Lot
	Cyble License Subscription + Unlimited Takedown Services for Philippine Deposit Insurance Corporation	1 Lot

Item	Product Description	Qty
7	ExtraHop EDA 1200 Subscription for Government Insurance Cluster (per agency)	1 Lot
	For non-supported systems, other means of monitoring must be done, such as network detection and response (NDR) or similar.	
	Network detection and response (NDR) or agency's existing network-based solution shall be integrated with the EDR/MDR and SOC Platform to form the foundation for evolving security operations against both common and advanced threat for endpoints/devices where the agent is not present. This will ensure the agency to have complete coverage and security detection and response capabilities – even for unmanaged or unmanageable (unsupported) endpoints/devices.	


 Wilfredo N. Aguilar
 Authorized Representative



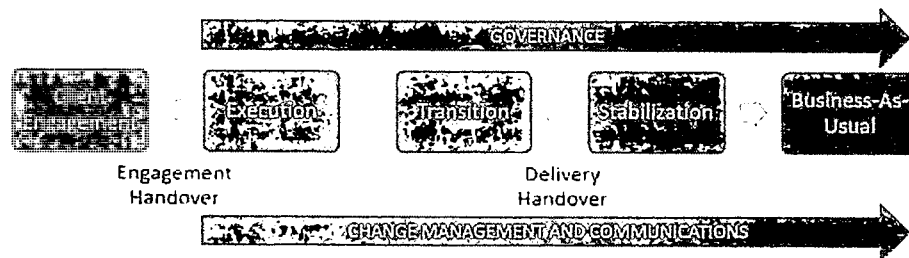
PROJECT MANAGEMENT PLAN



PROJECT MANAGEMENT PROGRAM PLAN FOR GOVERNMENT INSURANCE CLUSTER

To ensure the compliance and delivery of the requirements by the Government Insurance Cluster, **TRENDS** will provide a Project Management Program below:

Trends will use a two-pronged approach for project management. The project phases are planned to use the Waterfall Project Management methodology while the actual tasks execution utilizes Agile Methodology.



1. Client Engagement.

During the Post Qualification Evaluation, Trends will demonstrate the salient features of the proposed Shared Cyber Defense solution at the Project Site or via online.

Trends will assign the needed Project Manager and technical resources and will conduct kickoff activity to ensure that every team member understands the engagement approach. All facets of the project including manner of implementation, scope, requirements, and acceptance criteria will be discussed during the kickoff activity.

2. Execution.

Trends will implement the proposed solution in accordance with the scope of work. All throughout, monitoring of implementation activities will be done by Trend's Project Manager. Weekly project meetings will be conducted to ensure that all issues that may arise will be addressed. Project status updates and reports will be provided to the client in a timely manner. The monthly project monitoring report will be discussed by the Project Manager until the completion of the Phase I

Trends & Technologies, Inc.

6th Floor Trafalgar Plaza
105 H.V. Dela Costa Street, Salcedo Village
Makati City 1227 Philippines

Phone: +63 2 8811 8181 Fax: +63 2 8814 0130
www.trends.com.ph

and Phase II of the project, as defined in the Delivery Time/ Completion Schedule. The Project Manager shall be required to be onsite in any agency, by schedule, if necessary.

3. Transition.

Client onboarding will be done by Trends Service Transition Team to establish the service delivery processes and to ensure completeness of SOC visibility and familiarization with clients' processes and network behaviors.

Guided by the CIS Controls Framework, Trends will conduct Information Security Maturity Assessment which is a comprehensive gap analysis and risk assessment of an organization's readiness to detect, prevent, contain, and respond to threats to information systems. This takes on a holistic look on the organization's people, process, and technology to provide insights and understand vulnerabilities, identify, and prioritize remediation activities and demonstrate compliance.

Under CSC Control 17. Incident Response Management for Information Security Maturity Assessment, Trends will review agencies Incident Response Plan (IRP) which would guide the agencies on the creation, enhancement, and documentation of incident response playbooks, policies, and guidelines such as, but not limited to:

- Escalation process
- Incident containment process
- Incident eradication process
- Incident recovery process
- Incident identification process
- Process flow

Once the solution has been implemented, Trends will conduct process discovery and workshop, develop use cases, create playbooks and runbooks, and conduct tabletop exercises with the client. Trends will map security playbook and runbooks for applicable security use cases to guide client on their incident response. The playbooks and runbooks shall be signed off by the client and a signed Certificate of Completion and Acceptance (COCA) shall be issued to Trends by the client.

4. Stabilization.

Trends will validate that the systems are able to detect and respond to potential threats. Trends will perform fine tuning and comprehensive testing to verify the effectiveness of the security measures put in place. During the stabilization period, the SLA will not be in effect. The SLA will become mandatory during the Business-As-Usual (BAU) period.

Once the Stabilization period ends, there should be a signed Certificate of Completion of Stabilization Period issued to Trends by the client.

5. Business-As-Usual.

Once tools and technologies are installed and relevant stakeholders signed off the Certificate of Completion of Stabilization Period, Trends Operation Center will provide proactive monitoring, detection, and response to security incidents and cyber threats of Government Insurance Cluster.

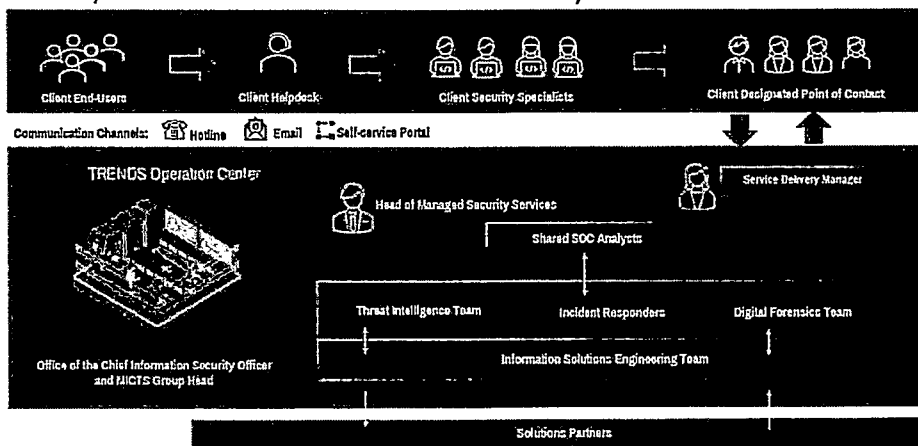


Trends will provide individual agency, web-based dashboards for accessing their agency information about alerts, attacks, track remediation on incidents, generate and extract reports which can be presented near real-time or over a period of time.

Moreover, Trends, through its cloud SIEM platform, will ensure the availability of the ingested raw logs twelve (12) months with comprehensive searchability. The logs, including evidence of security incidents, should be tamper proof and made available for legal and regulatory purposes, as required. The logs beyond the retention period shall be archived and given monthly to the agencies in an agreed format. Agencies will provide a storage repository for the archived logs.

Service Delivery Architecture

During the BAU, the Trends will follow the Service Delivery Architecture below:



Trends Security Operation Center (SOC) team will perform 24x7x365 monitoring services performed remotely at Trends Operations Center (TOC) located in Trends-MICTS Head Office Makati City, Philippines.

Trends will assign a Service Delivery Manager (SDM) to facilitate the delivery of the managed services and serve as the initial point of contact for any escalation. On the other hand, the agencies will also assign their respective SDM as the initial point of contact including tracking and validating of requests.

The agencies can report incidents to their helpdesk support. Only their helpdesk support is allowed to report the incidents to Trends SOC team for verification and authentication purposes.

Should there be any incidents not captured on the monitoring tool, the agency can report the incident through their SDM or helpdesk support, and contact Trends with the following details:

- Hotline: 8811-8181 extn: 8703, 8708, 8710 8715, 8716 and 8727
- Trends-SOC Email: soc@trends.com.ph

- Ivanti ticket: <https://mictsv2-ism.trends.com.ph/HEAT/>

Manpower Resources

Trends will have a dedicated 24x7x365 team assigned to the Government Insurance Cluster, composed of the following with their respective roles and responsibilities:

Personnel	Roles and Responsibilities
SOC Manager or Tier 4 Analyst (1)	In charge of strategy, priorities and the direct management of SOC staff when major security incidents occur. Responsible for the management of the MSOC operations for the agency and cluster.
Tier 3 Analyst (1)	Responsible for managing critical incidents. Responsible for actively hunting for threats and assessing the vulnerability of the business. 1. Manage High Severity Triage 2. Incident Response and Forensics Capabilities 3. Threat Containment (Using Existing EDR or agreed process) 4. Reporting and Post Incident Review 5. Use Case Development 6. Threat Searches 7. New Correlation Rules
Tier 2 Analyst (1)	Responsible for conducting further analysis and deciding on a strategy for containment. 1. Proactive Searches/ Threat Hunting 2. Qualification of Incident Priority/Severity 3. Investigation via SIEM/Analytics Platform and other accessible sources 4. Rule Tuning 5. Ad hoc Vulnerability Advisory & Research 6. Threat Containment (Using Existing EDR or agreed process) 7. Incident Response/Recommendations
Tier 1 Analysts (2)	Responsible for the following tasks: 1. Monitoring via existing SIEM/Analytics Platform 2. Funneling of alerts (noise elimination) 3. Incident Validation 4. Case Management 5. Threat Containment (Using Existing EDR or agreed process) – with guidance from L2 and up 6. General Communication 7. Weekly Summary Reports

Furthermore, Trends will also ensure that there will be alternate personnel deployed to the Insurance Cluster should the primary personnel be unavailable for whatever reason.

Reports and Meetings

- **Monthly Service Performance Report.**

The assigned dedicated local SOC Manager that will oversee that SOC and conduct regular monthly service performance review and reporting to client's management. The monthly service performance report which contains the status of cases and the assistance needed from the client, will be submitted and discussed by the SOC Manager. The monthly service performance report will include the following:

- SLA Performance
- Correlated Events Overview
- Correlated Events Graph Distribution Overtime
- Correlated Events and Rules Triggered Summary
- Summary of Incident Ticker per Use Cases Incident Management

- **Regular Email Advisory and Intelligence Summary Reports**

Trends will also provide regular email advisory and intelligence summary reports on the latest local and international news, latest cyber threats, and updates in Cyber security space, including detected information on the intention to target agencies or other government industries, major activist campaigns, and indications of activism against the agencies, financial and health sector, and the government.

However, a **special report or notice to the agencies** immediately, should there be any information or detection of targeted attacks against the agencies, the government or the sectors of the concerned agencies.

- **Monthly Service Performance Review Meeting.**

Led by the SOC Manager, Trends shall conduct monthly meetings with the agencies IT stakeholders to review SOC performance and discuss the overall IT security posture of the agencies, including fine-tuning of configurations and provision of best practices advice, to aid in continuous improvement.

Furthermore, Trends will also facilitate SOC security briefings to IT and CXOs and key decision-makers to discuss the intelligence summary reports and to share emerging technology trends and the risks associated with it, new regulations, complexity and sophistication of threats, requirement for companies to cyber-resilient among others.



TRAINING PLAN



TRAINING PLAN FOR GOVERNMENT INSURANCE CLUSTER

TRENDS will facilitate at least once a year Continual Service Improvement (CSI) workshop with clients for possible improvement of service through process, people, and technology.

TRENDS will provide security advisories with the client for cybersecurity news and updates like the latest viruses, trojans, worms, or other malicious programs.

TRENDS will conduct an annual cyber security maturity assessment (i.e., people, process, and technology) on each Government Agency based on the NIST or CIS controls.

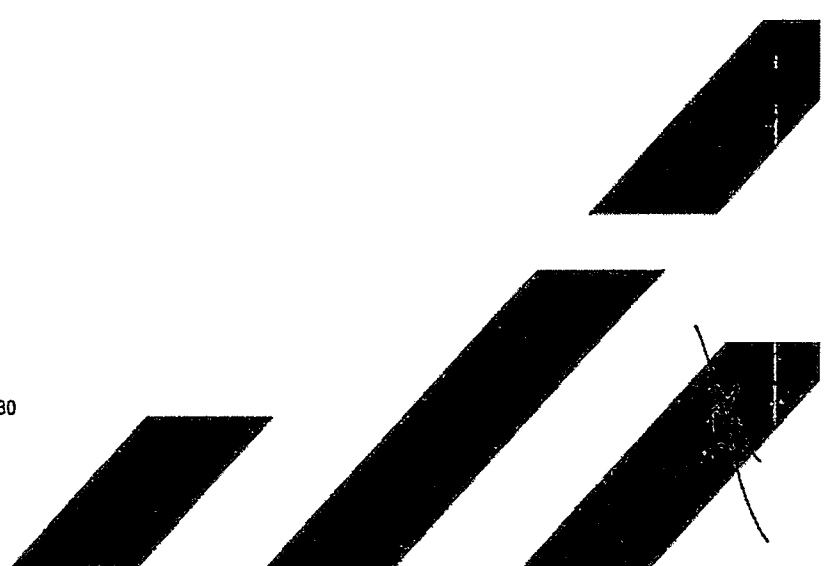
TRENDS will conduct an annual, or as needed, IR readiness training to the agencies Computer Security Incident Response Teams (CSIRT), including IT security awareness training to both technical and non-technical audiences of the agencies. The readiness training shall include best practices recommendation in isolation, containment, and remediation activities of the security incident.

TRENDS will conduct an annual, or as needed, incident response drill or simulation exercises with the agencies-CSIRTs to improve detection and internal readiness for cyber security incidents. This will include internal and external incident communications, reduced impact on operation continuity, reporting to regulators (e.g., NPC, DICT), CSIRT readiness, blue team capability, tabletop exercises, among others.

Trends & Technologies, Inc.

6th Floor Trafalgar Plaza
105 H.V. Dela Costa Street, Salcedo
Village Makati City 1227 Philippines

Phone: +63 2 8811 8181 Fax: +63 2 8814 0130
www.trends.com.ph



ANNEX 9 – Cybersecurity Daily Digest



Managed ICT Services
Service Delivery with Flexibility

THREAT HUNTING DAILY DIGEST

JAN 27 2022

TOP 5 SUSPICIOUS IP Address

1	23.94.159.201	Hits 39
Risk Score: 35 Related to: Phishing		
2	92.255.85.135	Hits 38
Risk Score: 64 Related to: Brute Force Blocking		
3	46.161.27.133	Hits 37
Risk Score: 45 Related to: Brute Force Blocking		
4	212.70.149.72	Hits 19
Risk Score: 69 Related to: Brute Force Blocking		
5	92.255.85.237	Hits 16
Risk Score: 60 Related to: Brute Force Blocking		

You can block IP addresses with the risk score of 40 and higher in your network. Otherwise, add to watchlist.

TOP 5 GLOBAL Vulnerabilities

1	CVE-2021-33742	Hits 1093
NIST Severity: High Related to: CVE-2021-27308		
2	CVE-2021-44228	Hits 576
NIST Severity: Critical Related to: Log4j, Ransomware		
3	CVE-2021-4034	Hits 557
NIST Severity: Medium Related to: HTTPS		
4	CVE-2021-27308	Hits 309
NIST Severity: Medium Related to: HTTPS		
5	CVE-2016-10045	Hits 5
NIST Severity: High Related to: HTTPS		

Remember to check if these exploited vulnerabilities are already patch in your system.

TOP MALWARE IN GLOBAL CYBER ATTACKS

Pegasus

Classification: Spyware
Attack Vector: Spam Campaigns
Target: Vulnerable Organizations
Hits: 132

Description:
Pegasus is a spyware developed by the Israeli cyberarms firm NSO Group that can be covertly installed on mobile phones (and other devices) running most versions of iOS and Android. The spyware is named after Pegasus, the winged horse of Greek mythology. It is a Trojan horse computer virus that can be sent "flying through the air" to infect cell phones.

LATEST INFORMATIONAL NOTES

A bug lurking for 12 years gives attackers root on most major Linux distros

The link for this article is included in this email. Stay tuned for more Cybernews update daily.

Prepared by TRENDS Operation Center

ANNEX 10 – Threat Hunting Advisory

THREAT HUNTING ADVISORY
OCT 20 2021

ADVISORY FROM SECURITY PROFESSIONALS

Conti/Lockbit MalSpam Campaign

Ransomware • MalSpam
▲ Spike in Cyber Reference

THE THREAT

Through sensitive source reporting, our threat intelligence partner, Insikt Group, recently identified an ongoing TrickBot malspam campaign targeting a large number of personal and corporate email addresses. In this campaign, TrickBot is used as the first stage for initial access to victim networks, with the subsequent deployment of the Conti ransomware variant.



In total, Insikt Group are aware of several million email addresses listed as targets in this campaign. The presence of an email address in this dataset does not imply active TrickBot or Conti infection, but indicates that these recipients are being actively targeted by email spearphishing attempts to initiate an attack.

WHAT'S IN IT FOR YOU?

Per checking, after a broader search for any emails with ".com.ph" or ".ph" in the list, none of such domains were found. Do note that this does not mean that the Philippines is free from Trickbot infection, but rather indicates that there is no known active targeting or spearphishing attempts to initiate an attack.

RECOMMENDATIONS

- The Threat Hunting Team recommends the following next actions:
- Use YARA rules to hunt for Conti/Lockbit Ransomware (if applicable).
 - Keep the antimalware, firewalls, and machines updated.
 - Fortify email security with strong spam filters.
 - Keep email security policy in check (DKIM, DMARC, SPF, etc.)



Handwritten signature

ANNEX 8 – Cybersecurity Maturity Assessment Sample

CIS

CONTROLS V8 ASSESSMENT

EXECUTIVE REPORT

PRESENTED BY

ALLAN JHAY M. LIBARIO
MADELEINE G. ENGUA
INFORMATION SECURITY CONSULTANT
ADVISORY AND AUDIT

TECHNOLOGY MANAGEMENT GROUP

CIS ID	Control Name	Compliance
CIS 01	Inventory and Control of Enterprise Assets	85%
CIS 02	Inventory and Control of Software Assets	85%
CIS 03	Data Protection	75%
CIS 04	Secure Configuration of Enterprise Assets and Software	75%
CIS 05	Account Management	85%
CIS 06	Access Control Management	75%
CIS 07	Information Governance Management	85%
CIS 08	Auditing Management	75%
CIS 09	Incident and Event Detection, Protection, and Response	85%
CIS 10	Malware Defense	85%
CIS 11	Data Recovery	85%
CIS 12	Network Architecture Management	75%
CIS 13	Network Monitoring and Defense	85%
CIS 14	Security Assessment and Scoping	85%
CIS 15	Service Provider Management	85%
CIS 16	Application Software Security	85%
CIS 17	Vendor Supplier Management	85%
CIS 18	Security Training	75%

Figure 8: Controls Data for CIS V8

CONFIDENTIAL

7

BID BULLETIN



LANDBANK

SERVING
THE NATION

**SUPPLEMENTAL/BID BULLETIN NO. 2
For LBP-HOBAC-ITB-GS-20230725-01**

PROJECT : Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster


IMPLEMENTOR : HOBAC Secretariat Unit

DATE : October 6, 2023

This Supplemental/Bid Bulletin is issued to modify, amend and/or clarify certain items in the Bid Documents. This shall form an integral part of the Bid Documents.

Modifications, amendments and/or clarifications.

- 1) The bidder/s are encouraged to use the Bid Securing Declaration as Bid Security
- 2) The Terms of Reference (Annexes D-1 to D-25), Technical Specifications (Section VII) and Checklist of Bidding Documents (Item No. 12 of Technical Documents and Item Nos. 26 to 28 of Other Documents to Support Compliance with Technical Specifications) have been revised. Please see attached revised Annexes D-1 to D-25 and specific sections of the Bidding Documents.
- 3) The submission and opening of bids is re-scheduled on October 13, 2023 at 10:00 A.M. through videoconferencing using Microsoft (MS) Teams.
- 4) Responses to bidder's queries/clarifications per Annex H-1 to H-21.


ATTY. HONORIO T. DIAZ, JR.
Head, HOBAC Secretariat Unit

Technical Specifications

Specifications	Statement of Compliance								
<p align="center">Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster</p> <table border="1" data-bbox="276 1458 826 1639"> <tr> <td>1. Bureau of Treasury</td> <td>1,600 endpoints</td> </tr> <tr> <td>2. Government Service Insurance System</td> <td>4,400 endpoints</td> </tr> <tr> <td>3. Social Security System</td> <td>8,000 endpoints</td> </tr> <tr> <td>4. Philippine Deposit Insurance Corporation</td> <td>1,200 endpoints</td> </tr> </table> <p>Phase 1.</p> <ul style="list-style-type: none"> ▪ Threat Intelligence ▪ Security Monitoring and Management ▪ Incident Response <p>Phase 2:</p> <ul style="list-style-type: none"> ▪ Vulnerability Management 	1. Bureau of Treasury	1,600 endpoints	2. Government Service Insurance System	4,400 endpoints	3. Social Security System	8,000 endpoints	4. Philippine Deposit Insurance Corporation	1,200 endpoints	<p align="center">Please state here either "Comply" or "Not Comply"</p>
1. Bureau of Treasury	1,600 endpoints								
2. Government Service Insurance System	4,400 endpoints								
3. Social Security System	8,000 endpoints								
4. Philippine Deposit Insurance Corporation	1,200 endpoints								

Bidders must state below either "Comply" or "Not Comply" against each of the individual parameters of each Specification preferably stating the corresponding performance parameter of the product offered.

Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.

<p>Notes:</p> <ol style="list-style-type: none">1. Technical specifications and other requirements per attached Terms of Reference (TOR) – revised Annexes D-1 to D-25.2. The documentary requirements enumerated in Items 3.II.C and D of the TOR shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements. <p>Non-submission of the above requirements may result to post-disqualification of the bidder.</p>	
---	--

Conforme:

Name of Bidder

Signature over Printed Name of
Authorized Representative

Position



Checklist of Bidding Documents for Procurement of Goods and Services

The documents for each component should be arranged as per this Checklist. Kindly provide guides or dividers with appropriate labels.

Eligibility and Technical Components (PDF File)

- *The Eligibility and Technical Component shall contain documents sequentially arranged as follows:*

- **Eligibility Documents – Class “A”**

Legal Eligibility Documents

1. Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages).

Technical Eligibility Documents

2. Duly notarized Secretary's Certificate attesting that the signatory is the duly authorized representative of the prospective bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the prospective bidder in the bidding, if the prospective bidder is a corporation, partnership, cooperative, or joint venture or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder. (sample form - Form No. 7).
3. Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid, within the last five (5) years from the date of submission and receipt of bids. The statement shall include all information required in the sample form (Form No. 3).
4. Statement of the prospective bidder identifying its Single Largest Completed Contract (SLCC) similar to the contract to be bid within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the sample form (Form No. 4).

Financial Eligibility Documents

5. The prospective bidder's audited financial statements, showing, among others, the prospective bidder's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission.



6. The prospective bidder's computation for its Net Financial Contracting Capacity (NFCC) following the sample form (Form No. 5), or in the case of Procurement of Goods, a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.
- o **Eligibility Documents – Class “B”**
7. Duly signed valid joint venture agreement (JVA), in case the joint venture is already in existence. In the absence of a JVA, duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful shall be included in the bid. Failure to enter into a joint venture in the event of a contract award shall be ground for the forfeiture of the bid security. Each partner of the joint venture shall submit its legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance, provided, that the partner responsible to submit the NFCC shall likewise submit the statement of all its ongoing contracts and Audited Financial Statements.
 8. For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos, Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.
 9. Certification from the DTI if the Bidder claims preference as a Domestic Bidder.
- o **Technical Documents**
10. Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
 11. Section VI – Schedule of Requirements with signature of bidder's authorized representative.
 12. Revised Section VII – Technical Specifications with response on compliance and signature of bidder's authorized representative.
 13. Duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).

Note: During the opening of the first bid envelope (Eligibility and Technical Component), only the above documents will be checked by the BAC if they are all present using a non-discretionary “pass/fail” criterion to determine each bidder's compliance with the documents required to be submitted for eligibility and the technical requirements.



- o **Other Documents to Support Compliance with Technical Specifications [must be submitted inside the first bid envelope (Eligibility and Technical Component)]**
 - 14. Current Certifications from the manufacturer that Service Provider is a certified/authorized reseller of the brands being offered.
 - 15. Data Sheets and Documentations of the brands and/or services being offered.
 - 16. Latest Forrester Leaders and Gartner Magic Quadrant report for brands offered that has such requirement.
 - 17. List of local sales and technical offices in the Philippines.
 - 18. TIA-942 Rated 3 Facility Certification.
 - 19. Valid SOC 2 Type II Attestation Report or ISO27001 Certification for Managed ICT Services or similar services.
 - 20. Information Security-related certifications of the onsite support engineers.
 - 21. Certifications of the SOC analysts.
 - 22. Certifications of the network and security engineers.
 - 23. List of Local Certified Engineers for the (i) SOAR, (ii) SIEM and (iii) Vulnerability Management, including their respective Certifications on the brand/solution being proposed.
 - 24. List of names of the dedicated 24x7x365 team that will be assigned to the Insurance Cluster, which shall be composed of the following:
 - a. Tier 1 Analyst
 - b. Tier 2 Analyst
 - c. Tier 3 Senior Analyst/Team Lead
 - d. Tier 4 Analyst/SOC Manager
 - 25. Documents regarding the Project Manager:
 - Company ID
 - Certificate of employment
 - List of projects handled.
 - End-User/Client company name of the projects handled.
 - Project Name and Project Duration (Start date and end date).
 - Project Management Certification



26. Documents regarding the SOC Manager/Tier 4 Analyst:
 - Company ID
 - Certificate of employment
 - List of engagements
 - Any two (2) of the unexpired professional certifications in the Insurance Cluster revised Terms of Reference

27. Documents regarding the Team Lead/Tier 3 Analyst:
 - Company ID
 - Certificate of employment
 - List of engagements
 - Any two (2) of the unexpired professional certifications in the Insurance Cluster revised Terms of Reference

28. Documents regarding the Team Member/Tier 2 or Tier 1 Analyst:
 - Company ID
 - Certificate of employment
 - List of engagements
 - Any one (1) of the unexpired professional certifications in the Insurance Cluster revised Terms of Reference

- **Post-Qualification Documents/Requirements – [The bidder may submit the following documents/requirements within five (5) calendar days after receipt of Notice of Post-Qualification]:**
 1. Business Tax Returns per Revenue Regulations 3-2005 (BIR No.2550 Q) VAT or Percentage Tax Returns for the last two (2) quarters filed manually or through EFPS.
 2. Latest Income Tax Return filed manually or through EFPS.
 3. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
 4. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).
 5. Duly notarized Secretary's Certificate designating the authorized signatory in the Contract Agreement if the same is other than the bidder's authorized signatory in the bidding (sample form – Form No. 7).

