TIA-942 Rated 3 Facility Certification

epi ®

Protecting your interests

CERTIFICATE OF CONFORMANCE
CONSTRUCTED FACILITY

This is to certify that the constructed data center facilities of

ePLDT Inc
VITRO Clark Data Center

VITRO Clark, Lot 3, Ninoy Aquino Avenue
Clark Freeport Zone, Pampanga
The Philippines

has been independently assessed and found to conform to the requirements of:

ANSI/TIA-942-B-2017
Rated-3

for the following scope:

Architecture	Telecom	Electrical	Mechanical
Rated-3	**Rated-3**	**Rated-3**	**Rated-3**

Certificate Number: TIA942PH220822001
Certificate validity: 22-Aug-2022 until 21-Aug-2025

TIA-942 SM

Certification Manager
EPI Certification Pte Ltd
Technology to Trans...

Surveillance
audits due by:

August 2023   August 2024

epi ®

Protecting your interests

CERTIFICATE OF CONFORMANCE CONSTRUCTED FACILITY

This is to certify that the constructed data center facilities of

ePLDT Inc.
VITRO Makati 2 Data Center

#222 Nicanor Garcia Street, Brgy. Bel-Air
Makati City, The Philippines

has been independently assessed and found to conform to the requirements of:

ANSI/TIA-942-B-2017
Rated-3

for the following scope:

Architecture	Telecom	Electrical	Mechanical
Rated-3	**Rated-3**	**Rated-3**	**Rated-3**

Certificate Number: TIA942PH220901001
Certificate validity: 1-Sep-2022 until 31-Aug-2025

TIA-942 ᴿᴹ

Certification Manager
EPI Certification Pte Ltd

Surveillance audits due by:

August 2023   August 2024

Lack of fulfillment of certification terms and conditions may render this certificate invalid. This certificate can be verified at https://tiaonline.org/942-datacenters/

ePLDT

ePLDT, Inc.
222, N. Garcia St., Bel-Air, Makati, NCR, Fourth
District, Philippines, 1209
VAT REG. TIN 207-762-546-00004
Tel. No : 815-0598 / 515-0803 / 859-0058

Billing Statement

BS-MKT2 142054059

BAN: 900186835

BILL TO:	TRENDS AND TECHNOLOGIES INC.		P.O No.	Date: 09/11/2023
ATTENTION	Renato Velonza		SQ No 16002571	
ADDRESS	6F Trafalgar Plaza, H.V. Dela Costa Street Salcedo Village, Makati City - PH		PAYMENT TERMS: 30 days	
BUSINESS NAME/STYLE			DR No : Tel. No.	
TIN	002-035-961-00000		DUE DATE: 10/11/2023	

Previous Balance	Payments	Adjustments	Past Due Amount	Current Amount
		SENSITIVE INFORMATION REDACTED		

PARTICULARS	QUANTITY	UNIT PRICE	TOTAL AMOUNT
One-Time Charge: For the Period 09/01/2023 to 09/30/2023			
Additional Amps (SQ 16002571)			
Additional Amps (SQ 16002571)			
Full Rack 20A Rated (2F M2001) (SQ 16002571)			
Full Rack 20A Rated (2F M2002) (SQ 16002571)			
Rack basic PDU: 32A IEC309, 20 way C13 + 4 way C19, blah 16002571)			
Copper Cross Connect (SQ 16002452)		SENSITIVE INFORMATION REDACTED	
Copper Cross Connect (SQ 16002452)			
Copper Cross Connect (SQ 16002452)			
Copper Cross Connect (SQ 16002571)			
Copper Cross Connect (SQ 16002571)			
Copper Cross Connect (SQ 16002571)			
LAN Port (SQ 16002571)			
VITRO Internet Access (SQ 16004562)			
SUBTOTAL			

Contract Period: to

VATABLE SALE	PHP	
VAT EXEMPT SALE		SENSITIVE
VAT ZERO RATED SALE		INFORMATION
VAT AMOUNT		REDACTED
TOTAL SALES	PHP	
CURRENT AMOUNT	PHP	
PAST DUE AMOUNT		
TOTAL AMOUNT DUE	**PHP**	

TERMS AND CONDITIONS

1) Due Date: 30 days upon Receipt of Invoice.
2) Late payment shall be subject to a penalty charge of 3% per month.
3) Please submit Creditable Withholding Tax or BIR 2307 and BIR 2306 (if applicable) together with the check payment. Failure to do so will remain an Outstanding Accounts Receivable equivalent to the amount of uncollected CWT.

Please examine the Invoice/statement immediately upon receipt. If no error/discrepancy is reported within seven (7) days from date of receipt, the account will be considered correct.

PAYMENT INSTRUCTIONS

(1) Please make check payable to: ePLDT, Inc.
(2) For direct or wire transfer:
BDO(Ayala Ave Branch) - Peso Acct. No: 5318-013905; (Swift Code): BNORPHMM
DB(Manila Branch) - USD Acct. No. 1009513305; (Swift Code): DEUTPHMM
Send proof of remittance/deposit to: epldt_payments@epldt.com
(3) In case of withholding tax deduction please submit the corresponding withholding tax certificate. Otherwise, the total amount withheld shall be deemed unpaid and demandable.
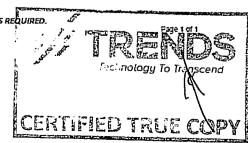(4) For inquiries and clarifications, you may contact us at #ePLDT(#37536) for PLDT landline subscribers and 8 2888 999 for other networks. You can also reach us real-time through CHAT on our website www.epldt.com and click the CHAT ICON or email us at wecare@epldt.com and epldt_payments@epldt.com

BIRCAS Permit No: 2001_0128_PTU_CAS_000751
Date Issued: 01/01/2020
Valid Until: 12/31/2024
Series: BS-MKT2 142000001 - BS-MKT2 142999999

THIS DOCUMENT IS NOT VALID FOR CLAIM OF INPUT TAXES*
THIS BILLING STATEMENT SHALL BE VALID FOR
FIVE (5) YEARS FROM THE DATE OF PERMIT TO USE

THIS IS A SYSTEM-GENERATED DOCUMENT. NO SIGNATURE IS REQUIRED.

Page 1 of 1

TRENDS
Technology To Transcend

CERTIFIED TRUE COPY

ePLDT

ePLDT. Inc.
222. N. Garcia St., Bel-Air. Makati, NCR, Fourth
District, Philippines. 1209
VAT REG TIN 207-762-548-00004
Tel. No.: 815-0598 / 515-0603 / 559-0056

Billing Statement

BS-MKT2 142055275

BAN: 900027842

BILL TO	TRENDS AND TECHNOLOGIES, INC.		P.O No.		Date: 09/29/2023
ATTENTION	Renato Velonza		SO No. 16002571		
ADDRESS	6F Trafalgar Plaza, H.V. Dela Costa Street Salcedo Village, Makati City - PH		PAYMENT TERMS:	30 days	
BUSINESS NAME/STYLE			DR No.	Tel. No.	
TIN	002-035-961-00000		DUE DATE. 10/29/2023		

Previous Balance	Payments	Adjustments	Past Due Amount	Current Amount
		SENSITIVE INFORMATION REDACTED		

PARTICULARS	QUANTITY	UNIT PRICE	TOTAL AMOUNT
FAO: Excess Charges: For the Period 09/01/2023 to 09/30/2023 Excess Power per ampere (rated) (2F M2CD1) (63.33 Amps - 46 Amps) Excess Power per ampere (rated) (2F M2CD2) (60.06 Amps - 46 Amps) SUBTOTAL		SENSITIVE INFORMATION REDACTED	
Contract Period to		VATABLE SALE PHP VAT EXEMPT SALE VAT ZERO RATED SALE VAT AMOUNT TOTAL SALES PHP	SENSITIVE INFORMATION REDACTED
		CURRENT AMOUNT PHP PAST DUE AMOUNT	
		TOTAL AMOUNT DUE PHP	

TERMS AND CONDITIONS	PAYMENT INSTRUCTIONS
(1) Due Date. 30 days upon Receipt of Invoice. (2) Late payment shall be subject to a penalty charge of 3% per month (3) Please submit Creditable Withholding Tax or BIR 2307 and BIR 2306 (if applicable) together with the check payment, failure to do so all remain an Outstanding Accounts Receivable equivalent to the amount of uncollected CWT. Please examine the invoice/statement immediately upon receipt. If no error/discrepancy is reported within seven (7) days from date of receipt, the account will be considered correct.	(1) Please make check payable to: ePLDT, Inc. (2) For direct or wire transfer: BDO(Ayala Ave Branch) - Peso Acct. No: 5318-013905; (Swift Code): BNORPHMM DB(Manila Branch) - USD Acct. No. 1009513305; (Swift Code): DEUTPHMM Send proof of remittance/deposit to: epldt_payments@epldt.com (3) In case of withholding tax deduction please submit the corresponding withholding tax certificate. Otherwise, the total amount withheld shall be deemed unpaid and demandable. (4) For inquiries and clarifications, you may contact us at #ePLDT(#37535) for PLDT landline subscribers and 8 2656 569 for other networks. You can also reach us real-time through CHAT on our website www.epldt.com and click the CHAT ICON or email us at wecare@epldt.com and epldt_payments@epldt.com

BIRCAS Permit No: 2001_0126_PTU_CAS_000751
Date Issued: 01/01/2020
Valid Until: 12/31/2024
Series: BS-MKT2 142000001 - BS-MKT2 142999999

"THIS DOCUMENT IS NOT VALID FOR CLAIM OF INPUT TAXES"
THIS BILLING STATEMENT SHALL BE VALID FOR
FIVE (5) YEARS FROM THE DATE OF PERMIT TO USE

THIS IS A SYSTEM-GENERATED DOCUMENT. NO SIGNATURE IS REQUIRED.

TRENDS
Technology To Transcend

CERTIFIED TRUE COPY

ePLDT

ePLDT, Inc.
5th Floor, LV Locsin Bldg, Ayala Ave. cor Makati
Ave., San Lorenzo, Makati City, Philippines, 1223
VAT REG TIN 207-762-546-00003
Tel. No : 815-0598 / 815-0603 / 559-0059

Billing Statement

BS-CRK 144007045

BAN: 900186843

BILL TO	TRENDS AND TECHNOLOGIES INC.		P.O No.		Date: 09/11/2023
ATTENTION	Renato Velonza		SQ No 16092570		
ADDRESS	6F Trafalgar Plaza, H.V. Dela Costa Street Salcedo Village, Makati City - PH		PAYMENT TERMS 30 days		
BUSINESS NAME/STYLE			DR No.:	Tel. No.	
TIN	002-035-961-00000		DUE DATE 10/11/2023		

Previous Balance	Payments	Adjustments	Past Due Amount	Current Amount
		SENSITIVE INFORMATION REDACTED		

PARTICULARS	QUANTITY	UNIT PRICE	TOTAL AMOUNT
One-Time Charge* For the Period 09/01/2023 to 09/30/2023			
Additional Amps (SQ 16002570)			
Full Rack 20A Rated (GF M1AD7) (SQ 16002570)			
Full Rack 20A Rated (GF M1AD6) (SQ 16002570)			
Rack base PDU 32A IEC309, 20 way C13 + 4 way, C19, BI 16002570)			
Copper Cross Connect (SQ 16002570)	SENSITIVE INFORMATION REDACTED		
Copper Cross Connect (SQ 16002570)			
LAN Port (SQ 16002570)			
VITRO Internet Access (SQ 160004563)			
SUBTOTAL			

Contract Period: to		VATABLE SALE	PHP	
		VAT EXEMPT SALE		SENSITIVE
		VAT ZERO RATED SALE		INFORMATION
		VAT AMOUNT		REDACTED
		TOTAL SALES	PHP	
		CURRENT AMOUNT	PHP	
		PAST DUE AMOUNT		
		TOTAL AMOUNT DUE	**PHP**	

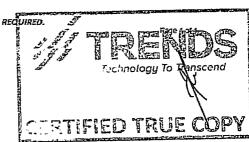| TERMS AND CONDITIONS	PAYMENT INSTRUCTIONS
(1) Due Date 30 days upon Receipt of Invoice. (2) Late payment shall be subject to a penalty charge of 3% per month (3) Please submit Creditable Withholding Tax or BIR 2307 and BIR 2306 (if applicable) together with the check payment. failure to do so will remain an Outstanding Accounts Receivable equivalent to the amount of uncollected CWT. Please examine the Invoice/statement immediately upon receipt. If no error/discrepancy is reported within seven (7) days from date of receipt, the account will be considered correct.	(1) Please make check payable to: ePLDT, Inc. (2) For direct or wire transfer: BDO(Ayala Ave Branch) - Peso Acct No: 5318-013905; (Swift Code): BNORPHMM DB(Manila Branch) - USD Acct. No. 1005513905; (Swift Code): DEUTPHMM Send proof of remittance/deposit to: epldt_payments@epldt.com (3) In case of withholding tax deduction please submit the corresponding withholding tax certificate. Otherwise, the total amount withheld shall be deemed unpaid and demandable. (4) For inquiries and clarifications, you may contact us at ePLDT(#37536) for PLDT landline subscribers and 8 2888 593 for other networks. You can also reach us real-time through CHAT on our website www.epldt.com and click the CHAT ICON or email us at wecare@epldt.com and epldt_payments@epldt.com

THIS DOCUMENT IS NOT VALID FOR CLAIM OF INPUT TAXES*
THIS BILLING STATEMENT SHALL BE VALID FOR
FIVE (5) YEARS FROM THE DATE OF PERMIT TO USE

THIS IS A SYSTEM-GENERATED DOCUMENT. NO SIGNATURE IS REQUIRED.

TRENDS
Technology To Transcend

CERTIFIED TRUE COPY

ePLDT

ePLDT, Inc.
6th Floor, LV Locsin Bldg, Ayala Ave cor Makati
Ave., San Lorenzo, Makati City, Philippines, 1223
VAT REG TIN 207-762-546-00003
Tel. No.: 815-0598 / 515-0603 / 559-0059

Billing Statement

BS-CRK 144007107

BAN: 900027834

BILL TO	TRENDS AND TECHNOLOGIES, INC.	P.O No.		Date: 09/29/2023
ATTENTION	Renato Velonza	SO No 16002570	
ADDRESS	6F Trafalgar Plaza, H.V. Dela Costa Street Salcedo Village, Makati City - PH	PAYMENT TERMS. 30 days	
BUSINESS NAME/STYLE		DR No :	Tel. No.
TIN	002-035-961-00000	DUE DATE. 10/29/2023	

Previous Balance	Payments	Adjustments	Past Due Amount	Current Amount

SENSITIVE INFORMATION REDACTED

PARTICULARS	QUANTITY	UNIT PRICE	TOTAL AMOUNT
FAO:			
Excess Charges: For the Period 09/01/2023 to 09/30/2023			
Excess Power per ampere (rated) (GF-M1A-07) (45.27 Amps - 20 Amps)			
Excess Power per ampere (rated) (GF-M1A-08) (28.77 Amps - 20 Amps)			
SUBTOTAL			
		SENSITIVE INFORMATION REDACTED	

Contract Period: to

VATABLE SALE	PHP	
VAT EXEMPT SALE		
VAT ZERO RATED SALE		SENSITIVE INFORMATION REDACTED
VAT AMOUNT		
TOTAL SALES	PHP	
CURRENT AMOUNT	PHP	
PAST DUE AMOUNT		
TOTAL AMOUNT DUE	PH)	

TERMS AND CONDITIONS	PAYMENT INSTRUCTIONS
(1) Due Date: 30 days upon Receipt of Invoice. (2) Late payment shall be subject to a penalty charge of 3% per month (3) Please submit Creditable Withholding Tax or BIR 2307 and BIR 2306 (if applicable) together with the check payment. failure to do so all remain an Outstanding Accounts Receivable equivalent to the amount of uncollected CWT. Please examine the invoice/statement immediately upon receipt. If no error/discrepancy is reported within seven (7) days from date of receipt, the account will be considered correct.	(1) Please make check payable to: ePLDT, Inc. (2) For direct or wire transfer: BDO(Ayala Ave Branch) - Peso Acct No: 5318-015905; (Swift Code): BNORPHMM DB(Manila Branch) - USD Acct. No. 10095113305; (Swift Code): DEUTPHMM Send proof of remittance/deposit to: epldt_payments@epldt.com (3) In case of withholding tax deduction please submit the corresponding withholding tax certificate. Otherwise, the total amount withheld shall be deemed unpaid and demandable. (4) For inquiries and clarifications, you may contact us at #ePLDT(#37536) for PLDT landline subscribers and 8 2886 999 for other networks. You can also reach us real-time through CHAT on our website www.epldt.com and click the CHAT ICON or email us at wecare@epldt.com and epldt_payments@epldt.com

BIRCAS Permit No: 2001_0126_PTU_CAS_000751
Date Issued: 01/01/2020
Valid Until: 12/31/2024
Series: BS-CRK 144000001 - BS-CRK 144999999

THIS DOCUMENT IS NOT VALID FOR CLAIM OF INPUT TAXES
THIS BILLING STATEMENT SHALL BE VALID FOR
FIVE (5) YEARS FROM THE DATE OF PERMIT TO USE

THIS IS A SYSTEM-GENERATED DOCUMENT. NO SIGNATURE IS REQUIRED.

TRENDS
Technology To Transcend

CERTIFIED TRUE COPY

SOCOTEC

CERTIFICATE

No. SCUK001708D

certifies that :

Trends & Technologies, Inc.

20th Trafalgar Plaza, 105 HV Dela Costa, Salcedo Village Makati, Philippines

operates a management system that has been assessed as conforming to :

ISO/IEC 27001:2013

for the scope of activities :

Trends Managed ICT Services- Service Operations Group which consists of
Trends Operations Center, Systems & Platforms, Service Management and
Compliance & Continual Improvement
Statement of Applicability: MICTS-SO-Statement of Applicability Version 6 effective July 20, 2020

Issue date : 14 April 2021
Valid until : 28 October 2023 (Subject to adherence to the agreed ongoing
programme. successful endorsement of certification following each audit and
compliance with the terms and conditions of certification.)
Original date of certification · 29 October 2017

Mo Ghaus Operations Director SOCOTEC Certification UK

SOCOTEC Certification UK Ltd, 6 Gordano Court
Serbert Close, Portishead, Bristol BS20 7FS
UNITED KINGDOM
http://socotec-certification-international.co.uk

TRENDS
Technology To Transcend

CERTIFIED TRUE COPY

99.9% uptime or availability

splunk>

SPLUNK CLOUD SERVICE SERVICE LEVEL SCHEDULE *

Service Level Commitment

The Splunk Cloud Services will be available 100% of the time, as measured by Splunk over each calendar quarter of the Subscription Term, and subject to the exclusions set forth below (the "Service Level Commitment").

A Splunk Cloud Service is considered available if the Customer is able to login to its Splunk Cloud Service account and initiate a search using Splunk Software.

Service Level Credit:

If Splunk fails to achieve the above Service Level Commitment for a Splunk Cloud Service, Customer may claim a credit for such Splunk Cloud Service as provided below, up to a maximum credit per calendar quarter equal to one month's Splunk Cloud Service subscription fees.

PERCENTAGE AVAILABILITY PER CALENDAR QUARTER	CREDIT
100	NO CREDIT
99.99-99.999	2 HOURS
99.9-99.99	4 HOURS

Skip to main content >

splunk>

Exclusions

A Customer will not be entitled to a service credit if it is in breach of its Agreement with Splunk, including payment obligations. The Service Level Commitment does not apply to any downtime, suspension or termination of the applicable Splunk Cloud Service (or any Splunk Content or Splunk Software operating in connection with the Splunk Cloud Service) that results from:

- Account suspension or termination due to Customer's breach of the Agreement.

- Routine scheduled maintenance (Splunk's Maintenance Policy is available at https://www.splunk.com/en_us/legal/splunk-cloud-platform-maintenance-policy.html).

- Unscheduled, emergency maintenance or an emergency caused by factors outside Splunk's reasonable control, including force majeure events such as acts of God, acts of government, flood, fire, earthquake, civil unrest, acts of terror, Customer Content, Third Party Content or Internet Service Provider failures or delays.

- A Customer's equipment, software or other technology, or third-party equipment, software or technology (other than those which are under Splunk's control).

- Failures resulting from software or technology for which Splunk is not responsible under the Agreement.

- Customer's ability or inability to operate the Forwarder software is addressed by Splunk support services. For purposes of the Service Level Commitment, the Forwarder software is excluded from the calculation of the availability of the Splunk Cloud Services.

No Service Level Commitment is provided for free, proof-of-concept or unpaid trial services

Service Credit Claims.

Skip to main content >

splunk>

Cloud Service, by contacting Splunk at splunk-cloud-billing@splunk.com with a complete description of the downtime, how the Customer was adversely affected, and for how long. Splunk reserves the right to deny the service credit if the Customer does not qualify.

The service credit remedy set forth in this Service Level Schedule is the Customer's sole and exclusive remedy for the unavailability of any applicable Splunk Cloud Service.

*All capitalized terms not otherwise defined are as set forth in the Splunk Cloud Terms of Service.

COMPANY ⌄

PRODUCTS ⌄

SPLUNK SITES ⌄

LEARN ⌄

CONTACT SPLUNK ⌄

USER REVIEWS ⌄

Download on the App Store

GET IT ON Google Play

Skip to main content >

splunk>

splunk>

Back to Google Cloud Terms Directory (https://cloud.google.com/product-terms) > Current

Compute Engine Service Level Agreement (SLA)

During the Term of the agreement under which Google has agreed to provide Google Cloud Platform to Customer (as applicable, the "Agreement"), the Covered Service will provide a Monthly Uptime Percentage to Customer as follows (the "Service Level Objective" or "SLO"):

Covered Service	Monthly Uptime Percentage
Instances in Multiple Zones	>= 99.99%
A Single Instance of Memory Optimized family*	>= 99.95%
A Single Instance of all other families**	>= 99.9%
Load balancing	>= 99.99%

* https://cloud.google.com/compute/docs/memory-optimized-machines
(https://cloud.google.com/compute/docs/memory-optimized-machines)

** https://cloud.google.com/compute/docs/machine-resource
(https://cloud.google.com/compute/docs/machine-resource)

If Google does not meet the SLO, and if Customer meets its obligations under this SLA, Customer will be eligible to receive the Financial Credits described below. Monthly Uptime Percentage and Financial Credit are determined on a calendar month basis per Project per Region or, for a Single Instance, per instance. This SLA states Customer's sole and exclusive remedy for any failure by Google to meet the SLO. Capitalized terms used in this SLA, but not defined in this SLA, have the meaning set forth in the Agreement. If the Agreement

authorizes the resale or supply of Google Cloud Platform under a Google Cloud partner or reseller program, then all references to Customer in this SLA mean Partner or Reseller (as applicable), and any Financial Credit(s) will only apply for impacted Partner or Reseller order(s) under the Agreement.

Definitions

The following definitions apply to the SLA:

- **"Covered Service"** means:

  - Instances in Multiple Zones.

  - A Single Instance.

  - Load balancing as part of the Compute Engine Service.

- **"Downtime"** means:

  - For virtual machine instances: loss of external connectivity or persistent disk access for the Single Instance or, with respect to Instances in Multiple Zones, all applicable running instances.

  - For load balancing: loss of external connectivity (via the external IP addresses associated with load balancing forwarding rules with all Healthy Backend Instances) due to the failure of Google's systems.

  - Downtime does not include loss of external connectivity as a result of (i) the Google managed VPN service failing to serve traffic directed to VPN tunnels under that service; that sort of downtime is addressed exclusively in the Cloud VPN SLA; or (ii) <u>Network Service Tiers - Standard Tier</u> (https://cloud.google.com/network-tiers/docs/overview) failing to serve traffic.

- **"Downtime Period"** means a period of one or more consecutive minutes of Downtime. Partial minutes or intermittent Downtime for a period of less than one minute will not count towards any Downtime Periods.

- **"Financial Credit"** means the following for Instances in Multiple Zones and load balancing:

Monthly Uptime   Percentage of monthly bill for the respective Covered Service in the Region that did

Percentage	not meet SLO that will be credited to Customer's future monthly bills
99.00% - < 99.99%	10%
95.00% - < 99.00%	25%
< 95.00%	100%

- ○ **"Financial Credit"** means the following for a Single Instance of Memory optimized family:

Monthly Uptime Percentage	Percentage of monthly bill for a Single Instance in the Region that did not meet SLO that will be credited to Customer's future monthly bills
95.00% - < 99.95%	10%
90.00% - < 95.00%	25%
< 90.00%	100%

- **"Financial Credit"** means the following for a Single Instance of all other families:

Monthly Uptime Percentage	Percentage of monthly bill for a Single Instance in the Region that did not meet SLO that will be credited to Customer's future monthly bills
95.00% - < 99.90%	10%
90.00% - < 95.00%	25%
< 90.00%	100%

- **"Healthy Backend Instances"** means instances that are responding affirmatively to load balancing health checks.

- **"Instances in Multiple Zones"** means virtual machine instances hosted as part of the Compute Engine Service where instances are placed across two or more Zones in the same Region.

- **"Monthly Uptime Percentage"** means total number of minutes in a month, minus the number of minutes of Downtime suffered from all Downtime Periods in a month, divided by the total number of minutes in a month.

- **"Region"** means the applicable region described at https://cloud.google.com/compute/docs/regions-zones/

(https://cloud.google.com/compute/docs/regions-zones), as may be updated by Google from time to time.

- **"Single Instance"** means a single virtual machine instance hosted as part of the Compute Engine Service.

- **"Zone"** means the applicable zone described at https://cloud.google.com/compute/docs/regions-zones/ (https://cloud.google.com/compute/docs/regions-zones), as may be updated by Google from time to time.

Customer Must Request Financial Credit

In order to receive any of the Financial Credits described above, Customer must notify Google technical support (https://support.google.com/cloud/contact/cloud_platform_sla) within 60 days from the time Customer becomes eligible to receive a Financial Credit. Customer must also provide Google with log files showing Downtime Periods and the date and time they occurred. If Customer does not comply with these requirements, Customer will forfeit its right to receive a Financial Credit.

Maximum Financial Credit

The maximum aggregate number of Financial Credits issued by Google to Customer for all Downtime Periods in a single billing month will not exceed the amount due by Customer for the respective Covered Services in the Regions that did not meet SLO for the applicable month. Financial Credits will be in the form of a monetary credit applied to future use of the Covered Service and will be applied within 60 days after the Financial Credit was requested.

SLA Exclusions

The SLA does not apply to any (a) features designated pre-general availability (unless otherwise set forth in the associated Documentation); (b) features excluded from the SLA (in the associated Documentation); or (c) errors (i) caused by factors outside of Google's reasonable control; (ii) that resulted from Customer's software or hardware or third party software or hardware, or both; (iii) that resulted from abuses or other behaviors that violate the Agreement; or (iv) that resulted from quotas applied by the system or listed in the Admin Console. As applicable, Customer will only be entitled to Financial Credit for Downtime of a particular virtual machine instance as either a Single Instance or Instances in Multiple Zones, but not both.

PREVIOUS VERSIONS *(Last modified August 29, 2023)*

April 12, 2021   _ (https://cloud.google.com/compute/sla-20210412)   January 13, 2020

(https://cloud.google.com/compute/sla-20200113)   March 28, 2019

(https://cloud.google.com/compute/sla-20190328)   April 13, 2018

(https://cloud.google.com/compute/sla-20180413)   November 30, 2017

(https://cloud.google.com/compute/sla-20171130)   November 4, 2016

(https://cloud.google.com/compute/sla-20161104)   October 16, 2015

(https://cloud.google.com/compute/sla-20151016)

Splunk Cloud Platform™
Splunk Cloud Platform Service Description 9.0.2305 (latest FedRAMP release)

Splunk Cloud Platform Service Details

Generated: 9/20/2023 5:45 am

Splunk Cloud Platform Service Details

Splunk Cloud Platform introduction

Welcome to the Splunk Cloud Platform service description.

Splunk Cloud Platform delivers the benefits of award-winning Splunk® Enterprise as a cloud-based service. Using Splunk Cloud Platform, you gain the functionality of Splunk Enterprise for collecting, searching, monitoring, reporting, and analyzing all of your real-time and historical machine data using a cloud service that is centrally and uniformly delivered by Splunk to its large number of cloud customers, from Fortune 100 companies to small and medium-size businesses. Unless otherwise noted in Release Notes, Splunk manages and updates the Splunk Cloud Platform service uniformly, so all customers of Splunk Cloud Platform receive the most current features and functionality.

Splunk Cloud Platform provides a complete suite of self-service capabilities for you to ingest data, customize data retention settings, customize user roles and centralized authentication, configure searches and dashboards, update your IP Allow List and perform app management. In addition, you can use the Cloud Monitoring Console (CMC) to holistically monitor the data consumption and health of your Splunk Cloud Platform environment. Finally, ensure your Operational Contacts are kept up-to-date; see Your maintenance responsibilities for more details.

Your subscription to the Splunk Cloud Platform service is workload-based and is sized for resource capacity. By exception, you may be on an ingest-based subscription that is sized for data volume ingested. For more information, see Subscription types.

This document describes the features, capabilities, limitations, and constraints of the Splunk Cloud Platform service and our responsibilities to you as a Software as a Service provider. This document also notes your responsibilities as a subscriber to the service. Be sure to read the complete service description and the service terms and policies documents listed in the following section. If you have questions after reading any of this material, contact your Splunk sales representative.

Service terms and policies

The following links access important terms and policies documents that pertain to the Splunk Cloud Platform service. Be sure to read these documents to have a clear understanding of the service. If you have any questions, contact your Splunk sales representative.

- Splunk General Terms
- Splunk Cloud Service - Service Level Schedule
- Splunk Cloud Platform Maintenance Policy
- Splunk Platform Support Programs
- Splunk Data Security and Privacy
- Splunk Cloud Platform: Shared Responsibility Model: Selecting this link downloads a PDF to your machine or device.

Available regions and region differences

Splunk Cloud Platform is available in the following global regions for new stacks.

Service Component	AWS regions	Google Cloud regions
Victoria Experience	US (Oregon, Virginia) UK (London) Europe (Dublin, Frankfurt, Paris) Asia Pacific (Singapore, Sydney, Tokyo) Canada (Central)	Not currently available
Classic Experience	US (GovCloud US-West, GovCloud US-East) Europe (Stockholm) Asia Pacific (Mumbai, Seoul)	US (Iowa) UK (London) Europe (Belgium, Frankfurt) Asia Pacific (Singapore, Sydney) Canada (Montreal)
Admin Config Service (ACS)	Available	
Data Manager	Available, except GovCloud US-West and GovCloud US-East regions	Not currently available
Edge Processor	US (Oregon, Virginia) UK (London) Europe (Dublin, Frankfurt) Asia Pacific (Singapore, Sydney, Tokyo)	Not currently available
Federated search for Splunk	Available	Available
Federated search for Amazon S3	Available, except GovCloud US-West and GovCloud US-East regions.	Not currently available
Ingest actions	Available, filtering, masking and routing on customer-managed heavy forwarders or Splunk Cloud Platform environment	Available, filtering and masking on customer-managed heavy forwarders
Splunk Secure Gateway	Available, except GovCloud US-West and GovCloud US-East regions	Available
Storage: Customer-managed encryption keys (Preview)	Available	Available, for DDAS

Compliance and certifications

Splunk has attained a number of compliance attestations and certifications from industry-leading auditors as part of our commitment to adhere to industry standards worldwide and part of our efforts to safeguard customer data. The following compliance attestations/certifications are available:

- **SOC 2 Type II:** Splunk Cloud Platform has an annual SOC 2 Type 2 audit report issued. The SOC 2 audit assesses an organization's security, availability, process integrity, and confidentiality processes to provide assurance about the systems that a company uses to protect customers' data. If you require the SOC 2 Type 2 attestation to review, contact your Splunk sales representative to request it.
- **ISO 27001:** Splunk Cloud Platform is ISO/IEC 27001:2013-certified. ISO/IEC 27001:2013 is a standard for an information security management system, specifying the policies and procedures for all legal, physical, and technical controls used by an organization to minimize risk to information. See https://www.splunk.com/pdfs/legal/splunk-ISO-27001-certificate.pdf to access a PDF version of the Splunk ISO

27001 certificate.

For information regarding the availability of service components between the AWS and Google Cloud regions, see Available regions and region differences.

If your data must be maintained in a regulated cloud environment to assist you with meeting your compliance needs, Splunk Cloud Platform provides these optional subscriptions. Not all features may be available in regulated cloud environments. Please see feature-specific Documentation for more details.

- **U.S. Department of Defense (DoD) Impact Level 5 (IL5):** U.S. Defense Information Systems Agency (DISA) has granted the Splunk Cloud Platform U.S. Department of Defense (DoD) Impact Level 5 (IL5) Provisional Authorization (PA). U.S. Government agencies are now able to leverage the power of Splunk Cloud Platform to solve their challenging mission-critical problems, even when working with high sensitivity Controlled Unclassified Information (CUI). This subscription is available in the AWS GovCloud (US) regions, which are isolated regions designed to address specific regulatory and compliance requirements. Cryptographic modules used in the Splunk Cloud Platform FedRAMP offering are FIPS 140-2 validated encryption modules. For information about apps validated by FedRAMP, see FedRAMP Moderate and DoD IL5 validated premium solutions and apps.

- **FedRAMP Moderate:** Splunk Cloud Platform FedRAMP is authorized by the General Services Administration FedRAMP PMO at the Moderate Impact Level. Splunk Cloud Platform FedRAMP addresses the needs of the U.S. Government, State and Local customers, educational institutions, and commercial customers who seek FedRAMP authorized services, and allows them to run sensitive workloads in the cloud. This subscription is available in the AWS GovCloud region, which is an isolated region designed to address specific regulatory and compliance requirements. Cryptographic modules used in the Splunk Cloud FedRAMP offering are FIPS 140-2 validated encryption modules. For information about apps validated by FedRAMP, see FedRAMP Moderate and DoD IL5 validated premium solutions and apps.

- **Health Insurance Portability and Accountability Act (HIPAA):** Splunk Cloud Platform (HIPAA) is compliant with the HIPAA Security Rule and HITECH Breach Notification Requirements. These regulations establish a standard for the security of any entity that accesses, processes, transmits, or stores electronic protected health information (ePHI).

- **Information Security Registered Assessors Program (IRAP):** Splunk attests Splunk Cloud Platform against the PROTECT level of the IRAP standard. The IRAP standard allows the Commonwealth of Australia and commercial customers to run sensitive workloads by using an IRAP assessed Splunk Cloud Platform environment in Australia (AWS Sydney region).

- **Payment Card Industry Data Security Standard (PCI DSS):** Splunk tests Splunk Cloud Platform for compliance with the PCI DSS v4.0 standard. This standard applies to any entity that processes, transmits, or stores payment card data as well as their critical service providers.

The table lists additional information for regulated cloud environments.

Subscription type	Region availability	Encryption at rest	IP Allow List	Certification documents
DoD IL5	GovCloud (US-West and US-East)	Enabled by default. Splunk manages the encryption keys on your behalf and they are regularly rotated.	You must provide IP allow list rules to access your Splunk Cloud Platform IL5 environment located in the splunkcloud.mil domain.	Contact your Splunk sales representative to learn more about Splunk Cloud Platform IL5.

3

Subscription type	Region availability	Encryption at rest	IP Allow List	Certification documents
FedRAMP Moderate	GovCloud (US-West and US-East)	Enabled by default. Splunk manages the encryption keys on your behalf and they are regularly rotated.	You must provide IP allow list rules to access your Splunk Cloud Platform FedRAMP environment located in the splunkcloudgc.com domain.	If you are a Federal agency, request the Splunk Cloud Platform FedRAMP package from the FedRAMP Marketplace. Otherwise, contact your Splunk sales representative.
HIPAA	All AWS and Google Cloud regions.	Enabled by default. Splunk manages the encryption keys on your behalf and they are regularly rotated. If available in your region, you have the option to manage the encryption keys instead.	You must provide IP allow list rules to access your Splunk Cloud Platform HIPAA environment.	If you require the HIPAA compliance report to review, contact your Splunk sales representative to request a copy.
IRAP	AWS Sydney region	Enabled by default. Splunk manages the encryption keys on your behalf and they are regularly rotated. Optionally, you can choose to manage the encryption keys.	You must provide IP allow list rules to access your Splunk Cloud Platform IRAP environment.	If you require the IRAP attestation of compliance to review, contact your Splunk sales representative to request a copy.
PCI DSS	All AWS regions except GovCloud (US-West and US-East). All Google Cloud regions.	Enabled by default. Splunk manages the encryption keys on your behalf and they are regularly rotated. If available in your region, you have the option to manage the encryption keys instead.	You must provide IP allow list rules to access your Splunk Cloud Platform PCI DSS environment.	If you require the PCI DSS attestation of compliance to review, contact your Splunk sales representative to request a copy.

Data collection

Splunk Cloud Platform provides software and APIs that enable you to ingest data from your applications, cloud services, servers, network devices, and sensors into the service.

Unless otherwise described in feature-specific Documentation, the following sections describe how you can send data to Splunk Cloud Platform.

Using Splunk forwarders

There are two types of forwarder software: universal forwarder and heavy forwarder. In most situations, the universal forwarder is the best forwarder for Splunk Cloud Platform since it includes the essential components that it needs to forward data, uses significantly fewer hardware resources and is inherently scalable. For certain use cases when data needs to be parsed prior to forwarding or data needs to be forwarded based on criteria such as source or type of event, a heavy forwarder is required. Your Splunk Cloud Platform subscription includes a deployment server license for centralized configuration management of your Splunk forwarders. You can request the deployment server license from Splunk support. Setup, enablement, transformation, and sending data from forwarders to your Splunk Cloud Platform environment is your responsibility. This means you are responsible for installing, configuring, and managing your forwarders, including maintaining version compatibility. You can leverage Ingest actions for routing, filtering and masking data while it is streamed to your Splunk Cloud Platform environment. For more information, see Supported forwarder versions. You are responsible for installing the data collection components of any app you wish to use in Splunk Cloud Platform on a Splunk forwarder.

As part of on-boarding to the service, Splunk will provide you the IP addresses that you will use to send data to Splunk Cloud Platform using forwarders. These IP addresses will remain constant and not change during your subscription period. If you increase your subscription level, you may receive additional IP addresses that you will utilize to send data. In the rare occurrence of an IP address change, Splunk will provide you with advanced notification. Most customers will be required to add these IP addresses to their outbound firewall rules to ensure their data is successfully forwarded to Splunk Cloud Platform. To simplify lifecycle management of your outbound firewall rules, Splunk requires that you use the actual IP addresses provided or the DNS mapping.

For more information about scripted and modular inputs, see Experience designations.

For more information, see Upload Data and Use the Ingest Actions page in the *Getting Data In* manual.

Using HTTP Event Collector (HEC)

HEC lets you send data and application events using a token-based authentication mode to Splunk Cloud Platform over the Secure HTTP (HTTPS) protocol. You can generate a token and then configure a logging library or HTTPS client with the token to send data to HEC in a specific format. HEC is enabled by default for your Splunk Cloud Platform environment with a 1 MB size limit on the maximum content length. You are responsible for setup, enablement, transformation, and sending data to your Splunk Cloud Platform environment via HEC. You are also responsible for monitoring and remediation of any HEC error codes that are received from Splunk Cloud Platform to ensure no interruption of your data ingestion. For more information, see the following:

- Use the HTTP Event Collector in the *Getting Data In* manual.
- The Data Collection entry in the Service limits and constraints table.
- The Differences between Splunk Cloud Platform and Splunk Enterprise section, especially the Indexer Discovery and Indexer Acknowledgement entry.

Using AWS Kinesis Data Firehose

For Splunk Cloud Platform in AWS regions, there is an additional data collection option. AWS Kinesis Data Firehose is a fully managed, scalable, and serverless option for streaming data from various AWS services directly into Splunk Cloud Platform. Setup, enablement, transformation, and sending data to your Splunk Cloud Platform environment is your responsibility. If you choose to use the Kinesis Data Firehose service for data ingestion, you are responsible for enabling and configuring AWS Kinesis Data Firehose, and for paying AWS for this service. For more information, see Install and configure the Splunk Add-on for Amazon Kinesis Firehose on a Splunk Cloud Platform deployment in the *Splunk Add-on for Amazon Kinesis Firehose* manual.

Using Edge Processor

Edge Processor provides an intermediate forwarding tier for your Splunk forwarders, with centralized cloud-based control and configuration management. For certain use cases when data needs to be parsed prior to forwarding or data needs to be forwarded based on criteria such as source or type of event, the Edge Processor service is a potential alternative to using heavy forwarder. Additionally, Edge Processor provides filtering, masking, and routing functionality. For more information, see About the Edge Processor solution.

Additional information about data collection

Data compression

Forwarders and HTTP Event Collectors compress data when sending over TLS protocol. The amount of compression varies based on the content, generally at a ratio between 8:1 and 12:1.

5

Valid SOC 2 Type II Attestation Report or ISO27001 Certification for Managed ICT Services or similar services

KPMG

1. Assertion of Trends & Technologies, Inc. Management

1. Assertion of Trends & Technologies, Inc. Management

⫽ TRENDS

Assertion of Trends & Technologies, Inc. Management

We have prepared the accompanying description in section 3 titled "Trends & Technologies, Inc. description of its Managed ICT Services" throughout the period July 31, 2021, to January 31, 2022, based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2®Report* (AICPA, *Description Criteria*), managing access to networks and computing systems for user entities.

The description is intended to provide report users with information about the managed services that may be useful when assessing the risks arising from interactions with Trends & Technologies, Inc. Managed ICT Services, particularly information about system controls that Trends has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*)

We confirm, to the best of our knowledge and belief, that:

a.) The description presents Trends & Technologies, Inc.'s Managed ICT Services that was designed and implemented throughout the period July 31, 2021, to January 31, 2022, in accordance with the description criteria.

b.) The controls stated in the description were suitably designed throughout the period July 31, 2021, to January 31, 2022, to provide reasonable assurance that Trends & Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

c.) The controls stated in the description operated effectively throughout the period July 31, 2021, to January 31, 2022, to provide reasonable assurance that Trends & Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Christine Fard
Chief Operating Officer
Trends and Technologies, Inc.

2. Independent Service Auditor's Report

To: Trends & Technologies, Inc.

Scope

We have examined Trends & Technologies, Inc. accompanying description in section 3 titled "Trends & Technologies Inc. description of its Manage ICT Services " throughout the period July 31, 2021, to January 31, 2022 based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2®Report* (AICPA, *Description Criteria*) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 31, 2021 to January 31, 2022, to provide reasonable assurance that Trends & Technologies, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information included in section 5, "Other Information Provided by Trends & Technologies, Inc. That Is Not Covered by the Service Auditor's Report," is presented by Trends & Technology, Inc.'s management to provide additional information and is not a part of the description. Information about Trends & Technologies, Inc.'s future plans for new systems, other services provided by the service organization that are not included in the scope of the engagement, qualitative information such as marketing claims, that may not be objectively measurable, and responses from management to deviations identified by the service auditor when such responses have not been subject to procedures by the service auditor has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Trends & Technologies, Inc.'s service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

Trends & Technologies, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Trends & Technologies, Inc. service commitments and system requirements were achieved. In section 1, Trends & Technology Inc. has provided its assertion titled "Assertion of Trends & Technologies, Inc. Management" about the description and the suitability of design and operating effectiveness of controls stated therein. Trends is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively

- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria

- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria

- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in section 4, "Trust Services Security Criteria, Related Controls, Test Procedures, and Test results" of this report in columns 1, 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

a.) The description presents Trends & Technologies, Inc.'s Managed ICT Services that was designed and implemented throughout the period July 31, 2021 to January 31, 2022, in accordance with the description criteria.

b.) The controls stated in the description were suitably designed throughout the period July 31, 2021 to January 31, 2022, to provide reasonable assurance that Trends & Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

c.) The controls stated in the description operated effectively throughout the period July 31, 2021 to January 31, 2022, to provide reasonable assurance that Trends & Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of Trends, user entitles of Trends' Managed ICT Services during some or all of the period July 31, 2021, to January 31, 2022, business partners of Trends subject to risks arising from interactions with the practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

R.G. MANABAT & CO.

Jallain Marcel S. Manrique
Partner
CPA License No. 0122094
PTR No. 6615126MD
Issued May 27, 2022, at Makati City

SOCOTEC

CERTIFICATE

No. SCUK001708D

certifies that :

Trends & Technologies, Inc.

20th Trafalgar Plaza, 105 HV Dela Costa, Salcedo Village Makati, Philippines

operates a management system that has been assessed as conforming to :

ISO/IEC 27001:2013

for the scope of activities :

**Trends Managed ICT Services- Service Operations Group which consists of
Trends Operations Center, Systems & Platforms, Service Management and
Compliance & Continual Improvement
Statement of Applicability: MICTS-SO-Statement of Applicability Version 6 effective July 20, 2020**

Issue date : 14 April 2021
Valid until : 28 October 2023 (Subject to adherence to the agreed ongoing
programme, successful endorsement of certification following each audit and
compliance with the terms and conditions of certification.)
Original date of certification : 29 October 2017

Mo Ghaus Operations Director SOCOTEC Certification UK

[signature]

TRENDS
Technology To Transcend

CERTIFIED TRUE COPY

UKAS
7063

SOCOTEC Certification UK Ltd, 6 Gordano Court
Serbert Close, Portishead, Bristol BS20 7FS
UNITED KINGDOM
http://socotec-certification-international.co.uk

TRENDS
Technology To Transcend

CERTIFICATION IN THE INFORMATION TECHNOLOGY

This is to certify that Trends & Technologies, Inc. is a leading Solutions Provider and Systems Integrator for Security and Information and Communications Technology (ICT) in the Philippines for thirty (30) years and more than Three (3) years of experience in providing SOC services. SOC is certified to ISO27001:2013 Information Security Management System (ISMS).

TRENDS offer complete IT Solutions and services to meet our clients' demands. We help clients achieve their business objectives as a total solutions provider. TRENDS' extensive experience has helped over 300 local and global businesses maintain a competitive edge by developing and managing IT network and security infrastructure solutions.

Trends and Technologies SEC details as below;

	Registration Date : 30-Oct-1992
SEC Certificate	SEC Certificate Number AS0920"351

Wilfredo N. Aguilar
Bidder's Representative/Authorized Signatory

Republic of the Philippines

Securities and Exchange Commission

EDSA, Greenhills, Mandaluyong
Metro-Manila

S.E.C. Reg. No. ASO92– C7851

TO ALL TO WHOM THESE PRESENTS MAY COME, GREETINGS

WHEREAS, Articles of Incorporation and By-Laws duly signed and acknowledged for the organization of the

TRENDS & TECHNOLOGIES, INC.

under and in accordance with the provisions of the Corporation Code of the Philippines, Batas Pambansa Blg. 68, approved on May 1, 1980, were presented for filing in this Commission on _____ October 28, 1992 _____, and a copy of said Articles and By-Laws are hereto attached;

NOW, THEREFORE, by virtue of the powers and duties vested in me by law, I do certify that the said Articles of Incorporation and By-Laws were, after due examina- determine whether they are in accordance with law, duly registered in this mission on the _30th_ day of _____ October _____, Anno Domini, Hundred and _Ninety-Two_.

IN TESTIMONY WHEREOF, I have hereunto set my hand and caused the seal of this Commission to be affixed at Mandaluyong, Metro-Manila, Philippines, this _30th_ day of _____ October _____, in the year of our Lord nineteen hundred and _ninety-Two_.

SONIA M. BALEO
Director

CERTIFIED TRUE COPY

Information Security-related certifications of the onsite support engineers

TRENDS
Technology To Transcend

List of Information Security-related certifications of the onsite support engineers

Item	Name	Certifications	Validity
1	Delfin Barquilla, Jr	CEH - CERTIFIED ETHICAL HACKER	MAR 16, 2023 – MAR 15, 2026
		CTIA - EC COUNCIL CERTIFIED THREAT INTELLIGENCE ANALYST	JUN 2, 2023 – JUN 1, 2026
		NSE1 NETWORK SECURITY ASSOCIATE	JUN 15, 2023 – JUN 15, 2025
		NSE2 NETWORK SECURITY ASSOCIATE	JUN 16, 2023 – JUN 16, 2025
		NSE3 NETWORK SECURITY ASSOCIATE	JUN 23, 2023 – JUN 23, 2025
		ITIL® FOUNDATION CERTIFICATE V3	SEP 11, 2012 (No expiration)
2	Jestoni Morales	EC CERTIFIED ETHICAL HACKER (CEH)	JUN 2, 2023 – JUN 1, 2026
		EC CERTIFIED INCIDENT HANDLER (ECIH)	DEC 28, 2022 – DEC 27, 2025
		OFFENSIVE SECURITY WIRELESS PROFESSIONAL (OSWP)	SEP 30, 2018 (No expiration)
3	Mardy Anne Vizcarra	NSE1 NETWORK SECURITY ASSOCIATE	AUG 12, 2023 – AUG 12, 2025
		NSE2 NETWORK SECURITY ASSOCIATE	AUG 25, 2023 – AUG 25, 2025
		NSE3 NETWORK SECURITY ASSOCIATE	AUG 25, 2023 – AUG 25, 2025
		CTIA - EC COUNCIL CERTIFIED THREAT INTELLIGENCE ANALYST	NOV 17, 2022 – NOV 16, 2025
		CEH - CERTIFIED ETHICAL HACKER	OCT 20, 2021 – OCT 19, 2024
		Chronicle Certified SOAR Analyst (CCSA)	SEP 5, 2023 (No expiration)
		Chronicle SOAR Fundamentals v6 (CSFv6)	SEP 4, 2023 (No expiration)
		EJPT ELEARNSECURITY JUNIOR PENETRATION TESTER	OCT 28, 2022 (No expiration)
		ECSS - EC COUNCIL CERTIFIED SECURITY SPECIALIST V9	DEC 3, 2021 (No expiration)
		ITIL® FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT	AUG 3, 2020 (No expiration)
4	Erlyn Barredo	CEH - CERTIFIED ETHICAL HACKER	OCT 11, 2022 – OCT 10, 2025
		GENERAL PLATFORM KNOWLEDGE EVALUATION - GPKE	APR 30, 2021 (No expiration)
		SIEMPLIFY CERTIFIED SOAR OPERATOR - SCSO	MAY 2, 2021 (No expiration)
		SIEMPLIFY CERTIFIED SOAR ANALYST - SCSA	MAY 7, 2021 (No expiration)
		SIEMPLIFY PLATFORM FUNDAMENTALS	OCT 30, 2020 (No expiration)
5	Gemalyn Cabanos	EC CERTIFIED INCIDENT HANDLER (ECIH)	JUL 20, 2022 – JUL 19, 2025
		NSE2 NETWORK SECURITY ASSOCIATE	JUL 14, 2023 – JUL 14, 2025
		TRELLIX CERTIFIED PRODUCT SPECIALIST: SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) 11.3 PROFICIENCY EXAM	MAR 16, 2023 (No expiration)

		SIMPLIFY PLATFORM FUNDAMENTALS - VERSION 6+ (SPFV6)	MAY 26, 2022 (No expiration)
		SIMPLIFY CERTIFIED SOAR ANALYST (SCSA)	JUL 11, 2022 (No expiration)
		SIMPLIFY CERTIFIED SOAR OPERATOR (SCSO)	JUL 11, 2022 (No expiration)
		ITIL FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT	MAY 16, 2019 (No expiration)
6	Madeleine Engua	ECIH - EC COUNCIL CERTIFIED INCIDENT HANDLER	DEC 17, 2021 – DEC 16, 2024
		NSE 1 NETWORK SECURITY ASSOCIATE	NOV 8, 2022 – NOV 8, 2024
		CEH - CERTIFIED ETHICAL HACKER	OCT 20, 2021 – OCT 19, 2024
		ISO/IEC 27001 INFORMATION SECURITY ASSOCIATE	APR 5, 2022 (No expiration)
		ITIL V3 FOUNDATION	SEP 30, 2016 (No expiration)
7	Maria Carla Angela Belen	COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)	FEB 11, 2022 – FEB 10, 2025
		FORTINET NSE 1	FEB 6, 2023 – FEB 6, 2025
		FORTINET NSE 2	MAR 21, 2023 – MAR 21, 2025
		FORTINET NSE 3	SEP 27, 2023 – SEP 27, 2025
8	Christian Ace John Cacot	ITIL® FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT	SEP 16, 2020 (No expiration)
		CEH - CERTIFIED ETHICAL HACKER	JUL 1, 2022 – JUN 30, 2025
		Certified Threat Intelligence Analyst	DEC 2, 2022 – DEC 1, 2025
		Certified Incident Handler	JUL 20, 2022 – JUL 19, 2025
		COMPTIA Security +	APR 1, 2022 – APR 1, 2025
		Recorded Future Certified User	DEC 4, 2020 (No expiration)
		Recorded Future Certified Analyst	NOV 2, 2020 (No expiration)
9	Anthony Michael Borbe	CEH - CERTIFIED ETHICAL HACKER	MAR 15, 2023 – MAR 14, 2026
		ECIH - EC COUNCIL CERTIFIED INCIDENT HANDLER	DEC 29, 2022 – DEC 28, 2025
		CHRONICLE SOAR FUNDAMENTALS V6 (CSFV6)	DEC 3, 2022 (No expiration)
		NATIONAL CYBER DRILL (NCD) INTERMEDIATE LEVEL	NOV 29, 2022 (No expiration)
		NATIONAL CYBER DRILL (NCD) ENTRY LEVEL	NOV 28, 2022 (No expiration)
		TCM PRACTICAL MALWARE ANALYSIS (PMAT)	SEP 26, 2022 (No expiration)
		MITRE FIN6 EMULATION PLANS	SEP 15, 2022 (No expiration)
		MITRE FOUNDATIONS OF OPERATIONALIZING MITRE ATT&CK	SEP 15, 2022 (No expiration)
		ENTERPRISE SECURITY MANAGER (SIEM) DEMO ON-DEMAND TRAINING	JUN 12, 2021 (No expiration)
		ENTERPRISE SECURITY MANAGER 11.0 ESSENTIALS	JUN 12, 2021 (No expiration)
		MCAFEE MVISION EPOLICY ORCHESTRATOR ESSENTIALS	JUN 12, 2021 (No expiration)

TRENDS
Technology To Transcend

		MCAFEE MVISION EPO – OVERVIEW	JUN 11, 2021 (No expiration)
		CROWDSTRIKE SALES & PRODUCT TRAINING	MAY 1, 2021 (No expiration)
10	Chris Ansell Gucon	Fortinet NSE1 Network Security Associate	SEPT 8, 2023 – SEPT 8, 2025
		Fortinet NSE2 Network Security Associate	SEPT 8, 2023 – SEPT 8, 2025
		Qualys Certified Specialist (Vulnerability Management)	OCT 11, 2022 (No expiration)
		Qualys Certified Specialist (Vulnerability Management Detection & Response)	OCT 11, 2022 (No expiration)
		Qualys Certified Specialist (Web Application Scanning)	OCT 11, 2022 (No expiration)
		Acunetix Certified User	SEPT 17, 2018 (No expiration)
11	Rio Perez	TCM SECURITY PRACTIAL MALWARE ANALYSIS & TRIAGE	OCT 3, 2022
		COMPTIA SECURITY +	APR 8, 2021 - APR 8, 2024
		CEH - CERTIFIED ETHICAL HACKER	NOV 18, 2021 - NOV 17, 2024
		CHFI - COMPUTER HACKING FORENSIC INVESTIGATOR	FEB 11, 2022 – FEB 10, 2025
		ECIH - EC COUNCIL CERTIFIED INCIDENT HANDLER	DEC 28, 2022 – DEC 27, 2025
		COMPTIA SECURITY ANALYTICS PROFESSINAL	MAR 17, 2023 – MAR 17, 2026
		COMPTIA CYBERSECURITY ANALYST+ (CySA+)	MAR 17, 2023 – MAR 17, 2026
		GUIDEM DIGITAL FORENSICS & MEMORY ANALYSIS	JUN 11, 2022 (No expiration)
		RECORDED FUTURE CERTIFIED ANALYST	NOV 2, 2020 (No expiration)
		ITIL V4 FOUNDATION	FEB 7, 2020 (No expiration)
12	Dave Phillip Bungag	CISCO CERTIFITED NETWORK ASSOCIATE (CCNA)	OCT 21, 2021 – OCT 21, 2024
		ITIL® FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT	NOV 18, 2022 (No expiration)
		FORTINET NSE 1	APR 3, 2022 – APR 3, 2024
		FORTINET NSE 2	MAR 19, 2022 – MAR 19, 2024
		FORTINET NSE 3	APR 2, 2022 – APR 2, 2024
		FORTINET NSE 4 SECURITY PROFESSIONAL	MAR 30, 2023 – MAR 30, 2025
		COMPTIA + SECURITY CERTIFIED	MAR 14, 2022 – MAR 14, 2025
13	Tyrone Jules Serafico	ITIL® FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT	AUG 3, 2020 (No expiration)
		CEH - CERTIFIED ETHICAL HACKER	OCT 20, 2021 – OCT 19, 2024
		ECSS - EC COUNCIL CERTIFIED SECURITY SPECIALIST v9	DEC 3, 2021 (No expiration
		ISO/IEC 27001 AUDITOR	JUL 12, 2022 – JUL 12, 2025
		NSE 1 NETWORK SECURITY ASSOCIATE	NOV 24, 2022 – NOV 24, 2024
		COMPTIA SECURITY +	JUL 04, 2023 - JUL 04, 2026
		NSE 2 NETWORK SECURITY ASSOCIATE	AUG 13, 2023 – AUG 13, 2025
14	Ahmed Jameel Sia	ELEARNINGSECURITY JUNIOR PENETRATION TESTER	OCT 16, 2020 (No expiration)

		ICSI CERTIFIED NETWORK SECURITY SPECIALIST	NOV 2, 2020 (No expiration)
		ELEARNINGSECURITY CERTIFIED PROFESSIONAL PENETRATION TESTER	JAN 7, 2021 (No expiration)
		PENTESTER ACADEMY CERTIFIED RED TEAM PROFESSIONAL	JAN 6, 2022 (No expiration)
		FORTINET NSE1 NETWORK SECURITY ASSOCIATE	SEP 7, 2022 – SEP 7, 2024
		FORTINET NSE 2 NETWORK SECURITY ASSOCIATE	SEP 7, 2022 – SEP 7, 2024
		QUALYS CERTIFIED SPECIALIST VULNERABILITY MANAGEMENT	SEP 12, 2022 (No expiration)
		QUALYS CERTIFIED SPECIALIST VULNERABILITY MANAGEMENT DETECTION & RESPONSE	SEP 12, 2022 (No expiration)
		QUALYS CERTIFIED SPECIALIST WEB APPLICATION SCANNING	SEP 12, 2022 (No expiration)
15	Altair Israel Cavida	ELEARNINGSECURITY JUNIOR PENETRATION TESTER	OCT 16, 2020 (No expiration)
		ELEARNINGSECURITY CERTIFIED PROFESSIONAL PENETRATION TESTER	DEC 29, 2020 (No expiration)
		ISO/IEC 27001 INFORMATION SECURITY ASSOCIATE	MAY 1, 2021 (No expiration)
		CERTIFIED RED TEAM PROFESSIONAL	JAN 5, 2022 (No expiration)
		NSE1 NETWORK SECURITY ASSOCIATE	JUL 10, 2022 – JUL 10, 2024
		NSE2 NETWORK SECURITY ASSOCIATE	JUL 10, 2022 – JUL 10, 2024
		NSE3 NETWORK SECURITY ASSOCIATE	JUL 10, 2022 – JUL 10, 2024
		CTIA - EC COUNCIL CERTIFIED THREAT INTELLIGENCE ANALYST	NOV 17, 2022 – NOV 16, 2025
16	Jexler De Leon	ITIL® FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT	FEB 10, 2021 (No expiration)
17	Rolando Agustin	ITIL V4 FOUNDATION	DEC 7, 2019 (No expiration)
18	Paul Daniel Pablo	COMPTIA SECURITY+ CE	JUN 26, 2021 - JUN 26, 2024
19	Maila Calaycay	PECB ISO/IEC 27001 AUDITOR	JANUARY 25, 2023 (3 years)
		COMPTIA SECURITY+	JULY 4, 2023 – JULY 4, 2026
		MICROSOFT CERTIFIED: SECURITY, COMPLIANCE, AND IDENTITY	MAY 20, 2023 (No expiration)
		CERTIFIED ETHICAL HACKER	OCTOBER 20, 2021 – OCTOBER 19, 2024
		EC-COUNCIL CERTIFIED SECURITY SPECIALIST V9	DECEMBER 3, 2021 (No expiration)
		FORTINET NSE 2	MAY 22, 2022 - MAY 22, 2024
		FORTINER NSE 1	JAN 6, 2022 - JAN 6, 2024
		ITIL V4 FOUNDATION	JUL 31, 2020 (No expiration)

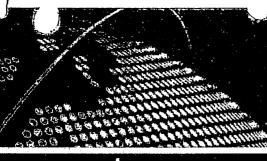| #	Name	Certification	Date
20	Justin Reynel Perez	CrowdStrike Certified Falcon Administrator (CCFA)	Sept. 06, 2023 – Sept. 05, 2026
		Tenable Certified Sales Engineer	Aug 17, 2023 – Aug 17, 2025
		Trellix DLP Certified Specialist	Oct. 05, 2023 – Oct. 05, 2025
		Recorded Future	Tech 101	July 26, 2022 (No expiration)
21	Jethro Cadungon	Microsoft Certified: Security Operations Analyst Associate	Sep 01, 2023 - Sep 02, 2024
		Splunk Core Certified User	Feb 28, 2022 - Feb 28, 2025
		Trellix Certified Product Specialist: Security Information and Event Management (SIEM)	Feb. 22, 2022 - Feb 22, 2024
		Siemplify Certified SOAR Analyst (SCSA)	June 08, 2020 (No expiration)
		Siemplify Certified SOAR Operator (SCSO)	June 04, 2021 (No expiration)
22	Joven Valenzuela III	CrowdStrike Certified Falcon Administrator (CCFA)	Sept. 12, 2023 – Sept. 11, 2026
		Splunk Core Certified User	Feb 28, 2022 - Feb 28, 2025
		Trellix Certified Product Specialist: Security Information and Event Management (SIEM)	Jun 22, 2023 - Jun 22, 2025
		Chronicle Certified SOAR Analyst (CCSA)	Dec. 16, 2022 - Dec. 16, 2024
23	Julio Gabriel Aseron	CrowdStrike Certified Falcon Administrator (CCFA)	Feb 02, 2023 - Feb 01, 2026
		Tenable Certified MSSP Practitioner	May 30, 2023 - May 30, 2025
		Trellix DLP Certified Specialist	Oct 04, 2023 - Oct 03, 2025
		Microsoft Certified: Azure Security Engineer Associate	Mar. 8, 2023 – Mar. 9, 2024
24	Christian Medina	Siemplify Certified SOAR Analyst (SCSA)	Feb 16, 2022 (No expiration)
		Trellix Certified Product Specialist: Security Information and Event Management (SIEM)	Jul 06, 2023 - Jul 06, 2025
		Microsoft Certified: Security Operations Analyst Associate	Sep 01, 2023 - Sep 02, 2024
		Microsoft Certified: Azure Security Engineer Associate	Sep 18, 2023 - Sep 19, 2024
25	John Vincent Yap	Microsoft Certified: Azure Security Engineer Associate	Jul 18, 2023 - Jul 19, 2024
		Chronicle SIEM Fundamentals	Dec. 14, 2023 (No expiration)
		Siemplify Certified SOAR Analyst (SCSA)	Jun 08, 2020 (No expiration)
		Siemplify Certified SOAR Operator (SCSO)	Oct 06, 2020 (No expiration)
26	Pol Dacasin	Tenable Certified Sales Engineer - VM	Jan 04, 2022 - Jan 04, 2024

TRENDS
Technology To Transcend

		Tenable Certified Sales Associate - VM	Jan 02, 2022 - Jan 02, 2024
		Password Safe Administration v22	Sep 02, 2022 - Sep 02, 2024
27		BeyondTrust Certified Implementation Engineer (BCIE)	Dec 09, 2022 - Dec 09, 2024
	Daniel Ada	Sophos Central Endpoint and Server v3.0 - Engineer	Aug. 30, 2022 – Aug. 30, 2024
28	Michael Alfred Encienzo	Tenable Certified Sales Engineer - VM	Sep 25, 2023 - Sep 25, 2025
		Delinea Secret Server Engineer Certification	Apr 04, 2023 - Apr 04, 2025
		Certified Forcepoint DLP Administrator	Nov 03, 2022 - Nov 03, 2023
		Microsoft Certified: Security Operations Analyst Associate	Oct 03, 2023 to Oct 04, 2024
29	Lean Viado	Tenable Certified Sales Engineer (TCSE) - VM Assessment	Sep 27, 2023 to Sep 27, 2025
		MENLO Technical Essentials Course	Sep 07, 2023 (No expiration)
30	Josiah Jose Santos	FORESCOUT CERTIFIED EXPERT (FSCE)	Sep 11, 2023
31	James Ryan Santos	ForeScout Certified Expert (FSCE)	FEBRUARY 1, 2023
32	Giovanni Lojica	BROADCOM PROVEN PROFESSIONAL PROXYSG 6.7	Dec 27, 2022 - Dec 27, 2024
		Trellix Certified Architect: Network Security NX	Sept. 14, 2023 – Sept. 14, 2025
33	Liza Canonoy	Palo Alto Network Certified Security Engineer	Sept. 10, 2023 - Sept. 10, 2025
34	Billy Ray Gamboa	NSE7 Network Security Architect	Sept. 22, 2023 – Sept. 22, 2025
35	Delvin Ray Gamalo	Palo Alto Network Certified Security Engineer	Sept. 8, 2023 - Sept. 8, 2025
		NSE7 Network Security Architect	Sep. 14,2023 – Sep.14, 2025
36	Charice May Moico	Palo Alto Network Certified Security Engineer	Sept. 10, 2023 - Sept. 10, 2025
37	Emmanuel Lacuata	NSE7 Network Security Architect	Sept. 30, 2023 - Sept. 30, 2025

EC-Council

C|EH

Certified | Ethical Hacker

Certified Ethical Hacker

This is to acknowledge that

DELFIN JR BARQUILLA

has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

Issue Date: **16 March, 2023**

Expiry Date: **15 March, 2026**

ANSI
ACCREDITED
#0732
I O/IEC 17024
Personnel Certification Program

Sanjay Bavisi, President

Certification Nu   .lr
ECC6024379518

C|TIA
Certified Threat Intelligence Analyst
(Certified Threat Intelligence Analyst)

This is to acknowledge that

DELFIN JR BARQUILLA

has successfully completed all requirements and criteria for

Certified Threat Intelligence Analyst

certification through examination administered by EC-Council
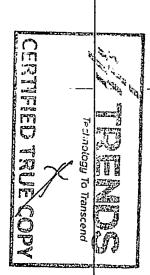
Issue Date: **02 June, 2023**   Expiry Date: **01 June, 2026**

EC-Council

Sanjay Bavisi, President

F RTINET.

NSE Certification
Program

This certifies that
DELFIN JR BARQUILLA
has achieved
NSE 1 Network Security Associate

Date of achievement: **June 15, 2023**

Valid until: **June 15, 2025**

Certification Validation number: **PMFGaadtM9**

Ken Xie
CEO of Fortinet

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

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

F RTINET.

NSE Certification Program

This certifies that
DELFIN JR BARQUILLA
has achieved
NSE 2 Network Security Associate

Date of achievement: **June 16, 2023**

Valid until: **June 16, 2025**

Certification Validation number: **j25IZWWnS5**

Ken Xie
CEO of Fortinet

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

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

CERTIFIED TRUE COPY

Technology to Transcend

FORTINET

NSE Certification Program

This certifies that

DELFIN JR BARQUILLA

has achieved

NSE 3 Network Security Associate

Date of achievement: **June 23, 2023**

Valid until: **June 23, 2025**

Certification Validation number: **BTnWCiKTqe**

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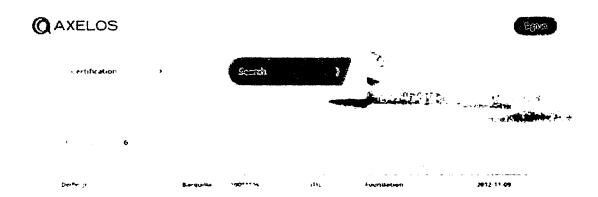
Michael Xie
President and Chief Technology Officer (CTO), Fortinet

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

AXELOS

Trends & Technologies, Inc.

JON
DELFIN JR. I. BARQUILLA
TTI-2163

_____
EMPLOYEE'S SIGNATURE

TRENDS

// TRENDS
Technology To Transcend

October 12, 2023

CERTIFICATE OF EMPLOYMENT
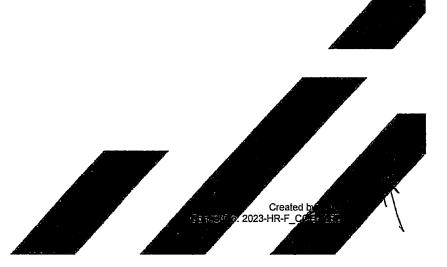
This certifies that Mr. Delfin I. Barquilla Jr. is an employee of Trends & Technologies, Inc. from August 08, 2022 up to the present and holds a permanent position of MICTS Service Operations Head.

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

Grace R. Lorenzo
Human Resources Head

Created by
2023-HR-F_C

TRENDS
Technology To Transcend

I. PERSONAL INFORMATION

NAME:

BARQUILLA	DELFIN JR.	ICOGO
(LAST NAME)	(FIRST NAME)	(MIDDLE NAME)

GROUP: MANAGED ICT SERVICES **POSITION:** MICTS SERVICE OPERATIONS HEAD

DIVISION: SERVICE OPERATIONS **DATE HIRE:** AUG 8, 2022

II. WORK EXPERIENCES

ITEM	INCLUSIVE DATES	COMPANY NAME	POSITION	DESCRIPTION OF FUNCTION

1.	AUG 2022 – PRESENT	TRENDS & TECHNOLOGIES, INC	MICTS SERVICE OPERATIONS HEAD	• Overall responsible for ensuring that the Service Operations has the optimum organizational structure to support Trends business streams effectively and efficiently.
				 • Ensure the delivery of top-tier services to clients.
				 • Drive process improvements and maintain a high standard of service excellence. Institutionalize metrics as a key indicator for continuous service improvement.
				 • Lead the Service Operations in achieving the highest possible service availability and customer satisfaction rating.
				 • Ensure Service Operations is available and functioning in accordance to commitments and acceptable standards
				 • Ensure Service Operations technology tools & logistical resources are always available in providing.
				 • Projects handled:
				   o Managed IT Security, Managed Wi-Fi, Managed Network in a Pharmaceutical Company
				   o Managed Security Services in four (4) government financial institution

TRENDS

Technology To Transcend

2.	2017 – 2022	COCA-COLA BEVERAGES PHILIPPINES, INC. COCA-COLA FAR EAST LIMITED (CONTINUOUS TENURE)	HEAD OF INFRASTRUCTURE AND CYBERSECURITY	• Technology infrastructure program lead. • Senior infrastructure program management role working within the technology operations & engineering team undertaking analysts, project management and implementation support for large scale transformational change within the Coca-Cola big technology. • Responsible for ensuring end to end service delivery according to agreed SLAs with the designated service provider which covers the planning, designing, managing, and maintaining the corporate it infrastructure, cybersecurity, application development and application support • Project handled: o IT Modernization in a large beverage company
3.	2017	DXT TECHNOLOGY DEPLOYED TO COCA-COLA FEMSA	ACCOUNT SECURITY OFFICER	• Plan, deliver and execute managed security projects and programs for Coca-Cola FEMSA Philippines • Ensuring appropriate resources are mobilized and programs projects portfolios meet operational, contractual, and economic commitments.
4.	2014 – 2016	ACCENTURE INC.	IT OPERATIONS SENIOR MANAGER	• Delivery lead plan, deliver and execute managed security and infrastructure outsourcing programs for multiple Accenture clients. • Ensuring appropriate resources are mobilized and programs projects portfolios meet operational, contractual, and economic commitments.

5.	2009 – 2014	HEWLETT-PACKARD PHILIPPINES CORP	ACCOUNT DELIVERY EXECUTIVE/ SERVICE DELIVERY MANAGER/ NETWORK OPERATIONS LEAD	• Lead and coordinate onshore/ offshore delivery activities for all managed services under contract within plan of record/forecasted cost while achieving contract SLAS, agreed SLOs and other ABS contractual commitments. • Accountable for delivery against cost and margin (DEGM) metrics • Manage relationships with customers. • Supervise network tower. • Responsible for the daily performance and availability of the organization's network. • Analyze network and recommend upgrades/ changes. • Assess organization's current and future network needs. • Oversees the daily operations of network staff
6.	2003 – 2009	ACCENTURE, INC.	NETWORK TEAM LEAD/ NETWORK ENGINEER/ DESKTOP SUPPORT ENGINEER	• Supervise the network engineering team of assigned domain which comprises a team of 13 in the areas of firewall/VPN, LAN/WAN, and network services to ensure the availability of the network to local, remote and/or client resources and professional development of subordinates. • Part of workstation engineering team servicing individuals with laptop and desktops.

III. EDUCATIONAL BACKGROUND

	DATES	SCHOOL	DEGREE
COLLEGE	2001 – 2003	AMA BINAN LAGUNA	BS INFORMATION TECHNOLOGY
POST GRADUATE STUDIES	2017 – 2019	DE LA SALLE LIPA	(MMT) MASTER'S IN MANAGEMENT TECHNOLOGY

IV. SEMINARS AND TRAININGS ATTENDED

A.   FOREIGN TRAININGS/ SEMINARS

ITEM	COURSE NAME	TRAINING PROVIDER	VENUE	INCLUSIVE DATES
1.	MENLO SECURITY	MENLO	NEW YORK	2018
2.	JUNIPER/NETSCREEN FIREWALL AND SWITCHING	JUNIPER	PERTH	2009
3.	CHECKPOINT NOKIA FIREWALL	MTECH	SINGAPORE	2006

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

B. LOCAL TRAININGS/SEMINARS

ITEM	SEMINAR TITLE	TRAINING PROVIDER	VENUE	INCLUSIVE DATES
1.	ACCELERATE TALENT PROGRAM SERIES OF LEADERSHIP TRAININGS FOR SELECT EXECUTIVES	GIBSON HALLMARK	PHILIPPINES – MULTIPLE VENUE	2019 - 2021
2.	VARIOUS SEMINARS ON 1. OPERATIONS SECURITY 2. MODERN WORKPLACE 3. SOC 4. NETWORKING 5. CLOUD	VARIOUS SUPPLIERS	PHILIPPINES – MULTIPLE VENUE	2017 - 2021
3.	PEOPLE, PROJECT, SECURITY AND ACCOUNT DELIVERY MANAGEMENT	ACCENTURE	MANDALUYONG	2014 - 2016
4.	HP ASE NETWORKING	HP	TAGUIG	2012
5.	ITIL V3	HP	TAGUIG	2011
6.	CCNA, CCNP (SWITCHING)	FUJITSU	MAKATI	2005

C. CERTIFICATIONS

ITEM	TITLE	INCLUSIVE DATES
1.	CEH - CERTIFIED ETHICAL HACKER	MAR 16, 2023 – MAR 15, 2026
2.	CTIA - EC COUNCIL CERTIFIED THREAT INTELLIGENCE ANALYST	JUN 2, 2023 – JUN 1, 2026
3.	NSE1 NETWORK SECURITY ASSOCIATE	JUN 15, 2023 – JUN 15, 2025
4.	NSE2 NETWORK SECURITY ASSOCIATE	JUN 16, 2023 – JUN 16, 2025
5.	NSE3 NETWORK SECURITY ASSOCIATE	JUN 23, 2023 – JUN 23, 2025
6.	ITIL® FOUNDATION CERTIFICATE V3	SEP 11, 2012

D. PROJECT HANDLED

ITEM	COMPANY	ROLE	PROJECT DESCRIPTION	INCLUSIVE DATES
1.	A Government Financial Institution	MICTS Service Operations Head	Managed Security Services	2022 - 2024
2.	A Government Financial Institution	MICTS Service Operations Head	Managed Security Services	2022 - 2024
3.	A Government Financial Institution	MICTS Service Operations Head	Managed Security Services	2022 - 2024
4.	A Government Financial Institution	MICTS Service Operations Head	Managed Security Services	2023 - 2025
5.	A Pharmaceutical Company	Security Solutions Support Technology Lead	Managed IT Security, Managed Wi-Fi, Managed Network	2022
6.	A Large Beverage Company	Project Proponent	IT Modernization, Security Transformation, Network Transformation, Cloud migration, virtualization	2017 - 2020

EC-Council

C|EH Certified Ethical Hacker

Certified | Ethical Hacker

This is to acknowledge that

Jestoni Morales

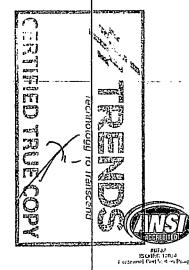has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

Issue Date: **02 June, 2023**

Expiry Date: **01 June, 2026**

ANSI
ACCREDITED
#0732
ISO/IEC 17024
Personnel Certification Program

Sanjay Bavisi, President

E|CIH

EC-Council Certified Incident Handler

EC-Council | Certified Incident Handler

This is to acknowledge that

Jestoni Morales

has successfully completed all requirements and criteria for

EC-Council Certified Incident Handler

certification through examination administered by EC-Council

Issue Date: **28 December, 2022**   Expiry Date: **27 December, 2025**

EC-Council

Sanjay Bavisi, President

OFFENSIVE security

THIS IS TO ACKNOWLEDGE THAT

Jestoni Morales

IS CERTIFIED AS AN

OSWP

(Offensive Security Wireless Professional)

AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY OFFENSIVE SECURITY.

THIS CERTIFICATION, EARNED ON

30th of September 2018

Mati Aharoni
Mati Aharoni

Trends & Technologies, Inc.

JES

JESTONI E. MORALES
TTI-2206

EMPLOYEE'S SIGNATURE

TRENDS

TRENDS
Technology To Transcend

October 5, 2023

CERTIFICATE OF EMPLOYMENT
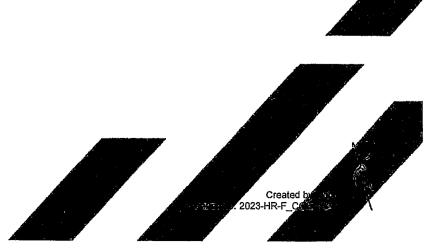
This certifies that Mr. Jestoni E. Morales is an employee of Trends & Technologies, Inc. from October 6, 2022 up to the present and holds a permanent position of SOC Manager.

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

Grace R. Lorenzo
Human Resources Head

Created by
2023-HR-F_CC

TRENDS
Technology To Transcend

I. PERSONAL INFORMATION

NAME:

MORALES	JESTONI	EMNACE
(LAST NAME)	(FIRST NAME)	(MIDDLE NAME)

GROUP: MANAGED ICT SERVICES   **POSITION:** SOC MANAGER

DIVISION: SERVICES   **DATE HIRE:** OCT 6, 2022

II. WORK EXPERIENCES

ITEM	INCLUSIVE DATES	COMPANY NAME	POSITION	DESCRIPTION OF FUNCTION
1.	OCT 2022 – PRESENT	TRENDS & TECHNOLOGIES, INC	SOC MANAGER	**Service Operations Management** • OLA Management and reporting • Recommend and implement technical and operating performance standards. • Execute crisis communication plan. • Address complaints and resolve problems with internal as well as external customers. **Service Operations Management - Incident Management** • Act as an incident manager for P1 and P2 incidents. **Service Operations Management - Problem Management** • Flag recurring incidents and inform Problem Manager of such incidents for proper Problem Management handling. **Service Operations Management - Process Engineering** • Contribute in the establishment of the most effective and efficient processes. • Promote and uphold compliance to agreed standards and processes. • Report inefficiencies and non-compliance to agreed standards and processes. • Propose process and procedure within the Security Operations Center. **Change Management** • Overall responsible for overseeing the correctness of the implementation of changes. **Continuous Improvement** • Collaborate and contribute with other managers in improving workflows, documentations, standards and processes. • Projects handled: o Managed Security Services in four (4) government financial institution
2.	DEC 2013 – AUG 2022	NEXT GENERATION TECHNOLOGIES GLOBAL INC.	TECHNICAL MANAGER	**Security Solutions Implementation** • Data loss protection solution • Endpoint protection solution • Vulnerability management solution

				• Security awareness training and simulation solution
				IT Security Services
				• Vulnerability Assessment and Penetration Testing (VAPT) services
				• Security awareness training and phishing simulation
				• PCI-DSS Pre-audit and red teaming exercises
				• Wi-Fi Audit
				• Project handled:
				  o A Property Management Company – Vulnerability Assessment and Penetration Testing of Web Applications, Wireless Network, Phishing Simulation and System Exploitation and Overall Internal Network
				  o A Financing Company – Managed Vulnerability Assessment Services
				  o A Financing Company – Implementation of Vulnerability Assessment for internal/external systems and web application scanning

3.	2012 – 2013	SWEDA SYSTEMS PHILIPPINES	SYSTEM ENGINEER	PDS Specialist for Jollibee Branches nationwide

III. EDUCATIONAL BACKGROUND

	DATES	SCHOOL	DEGREE
COLLEGE	2008 – 2012	UNIVERSITY OF CALOOCAN CITY	BS INFORMATION TECHNOLOGY
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.	ISACA CERTIFIED INFORMATION SECURITY MANAGER (CISM) TRAINING	TRENDS		JAN 2023
2.	CERTIFIED ETHICAL HACKER TRAINING	NGT GLOBAL	MAKATI	2017

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

Email: Info@trends.com.ph
Phone: (+632) 911 8181
Fax: (–632) 814 0130

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

TRENDS
Technology To Transcend

C. CERTIFICATIONS

ITEM	TITLE	INCLUSIVE DATES
1.	EC CERTIFIED ETHICAL HACKER (CEH)	JUNE 2, 2023 – JUNE 1, 2026
2.	EC CERTIFIED INCIDENT HANDLER (ECIH)	DEC 28, 2022 – DEC 27, 2025
3.	OFFENSIVE SECURITY WIRELESS PROFESSIONAL (OSWP)	SEPT 30, 2018

D. PROJECT HANDLED

ITEM	COMPANY	ROLE	PROJECT DESCRIPTION	INCLUSIVE DATES
1.	A Government Financial Institution 1	SOC Manager	Managed Security Services	2022 - 2024
2.	A Government Financial Institution 2	SOC Manager	Managed Security Services	2022 - 2024
3.	A Government Financial Institution 3	SOC Manager	Managed Security Services	2022 - 2024
4.	A Government Financial Institution 4	SOC Manager	Managed Security Services	2023 - 2025
5.	A Property Management Company	Project Manager	VAPT for Web Applications, Wireless Network, Phishing Simulation and System Exploitation and Overall Internal Network	2018 – 2021
6.	A Financing Company	Project Manager	Managed Vulnerability Assessment Services	2018 – 2021
7.	A Financing Company	Project Manager	Implementation of Vulnerability Assessment for internal/ external systems and web application scanning	2017 - 2021

F RTINET.

NSE Certification Program

This certifies that

Mardy Vizcarra

has achieved

NSE 1 Network Security Associate

Date of achievement: **August 12, 2023**

Valid until: **August 12, 2025**

Certification Validation number: **hPFOTL2yeu**

Ken Xie
CEO of Fortinet

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

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

FORTINET.

**NSE Certification
Program**

NSE
ASSOCIATE

This certifies that
Mardy Vizcarra
has achieved
NSE 2 Network Security Associate

Date of achievement: **August 25, 2023**

Valid until: **August 25, 2025**

Certification Validation number: **cqDDsPDQ6E**

Ken Xie
CEO of Fortinet

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

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

FORTINET

NSE Certification Program

This certifies that

Mardy Vizcarra

has achieved

NSE 3 Network Security Associate

Date of achievement: **August 25, 2023**

Valid until: **August 25, 2025**

Certification Validation number: **OdAJT3lCob**

Ken Xie
CEO of Fortinet

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

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

CTIA
(Certified Threat Intelligence Analyst)

Certified Threat Intelligence Analyst

This is to acknowledge that

Mardy Anne Vizcarra

has successfully completed all requirements and criteria for

Certified Threat Intelligence Analyst
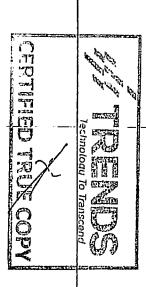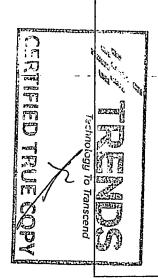
certification through examination administered by EC-Council

Issue Date: **17 November, 2022**   Expiry Date: **16 November, 2025**

EC-Council

Sanjay Bavisi, President

EC-Council

C|EH
Certified Ethical Hacker

Certified Ethical Hacker

This is to acknowledge that

Mardy Anne Vizcarra

has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

Issue Date: **20 October, 2021**

Expiry Date: **19 October, 2024**

Sanjay Bavisi, President
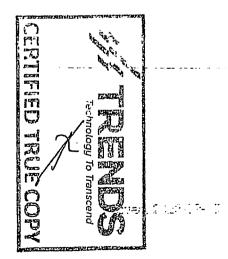
Certificate
of Completion

Certifies

Mardy Anne Vizcarra
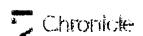
For the successful completion of:

Chronicle Certified SOAR Analyst (CCSA)

Oleg Siminel, Sr. Security Solutions Architect

TRENDS
Technology To Transcend

CERTIFIED TRUE COPY

Chronicle
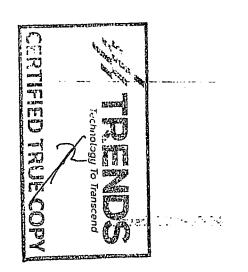
Certificate
of Completion

Certifies
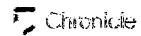
Mardy Vizcarra

For the successful completion of:

Chronicle SOAR Fundamentals V6 (CSFv6)

Oleg Siminel, Sr. Security Solutions Architect

Chronicle

CERTIFICATE OF COMPLETION

PROUDLY PRESENTED TO

Mardy Anne Vizcarra

eJPT eLearnSecurity
Junior Penetration Tester

eJPT V1.0

28th of October 2022

2313273
CERTIFICATION ID

Jack Reedy

Richard McLain

CERTIFIED TRUE COPY

TRENDS
Technology To Transcend

eLearn Security

E C S S

EC-Council Certified Security Specialist

(EC-Council) (Certified) (Security) (Specialist)

This is to acknowledge that

Mardy Anne Vizcaura

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

People

All talents, certified.

AXELOS
GLOBAL BEST PRACTICE

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

TRENDS
Technology To Transcend

CERTIFIED TRUE COPY

Trends & Technologies, Inc.

MARDY
MARDY ANNE M. VIZCARRA
TTI-1623

EMPLOYEE'S SIGNATURE

TRENDS

TRENDS

Technology To Transcend

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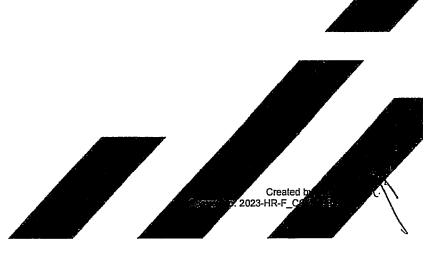
This certification is issued to comply with the bidding requirements of the Land Bank of the Philippines.

Grace R. Lorenzo
Human Resources Head

Created by
2023-HR-F_C

TRENDS

Technology To Transcend

I. PERSONAL INFORMATION

NAME:

VIZCARRA
(LAST NAME)

MARDY ANNE
(FIRST NAME)

MANAYSAY
(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	**Service Operations Management** • 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. **Service Operations Management - Event & Monitoring Management** • 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. **Service Operations Management - Incident Management** • 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: o Managed Security Services in a Mutual Life Insurance Company o Managed IT Security, Managed Wi-Fi, Managed Network in a Pharmaceutical Company o Managed Security Operations Center in a Government Financial Institution o 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 8191
Fax: (+632) 814 0130

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

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 INTERNATINAL 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

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

EC-Council

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
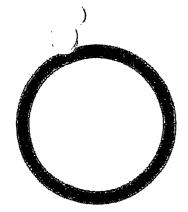
certification through examination administered by EC-Council

Issue Date: **11 October, 2022**

Expiry Date: **10 October, 2025**

Sanjay Bavisi, President

ANSI
ACCREDITED
#0732
ISO/IEC 17024
Personnel Certification Program

CERTIFICATE
OF COMPLETION

CERTIFIES

Erlyn Barredo
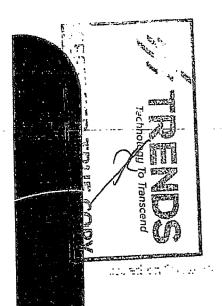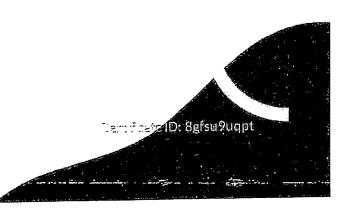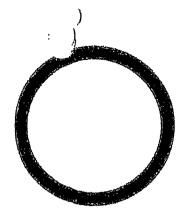
For the successful completion of:

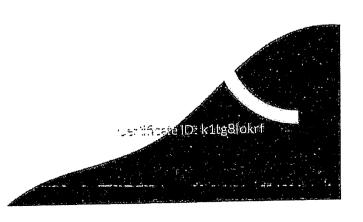## General Platform Knowledge Evaluation (GPKE)
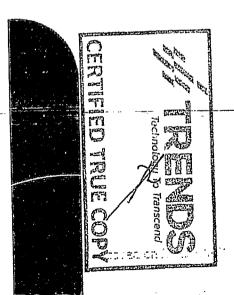
SOAR CERTIFICATION COURSE
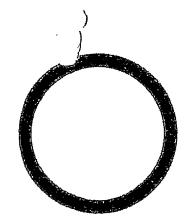
Oleg Siminel, Sr. Security Solutions Architect

Certificate ID: 8gfsu9uqpt

Siemplify

CERTIFICATE
OF COMPLETION

CERTIFIES

Erlyn Barredo

For the successful completion of:

Siemplify Certified SOAR Operator (SCSO)

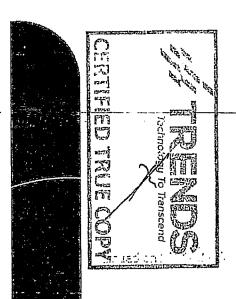SOAR CERTIFICATION COURSE
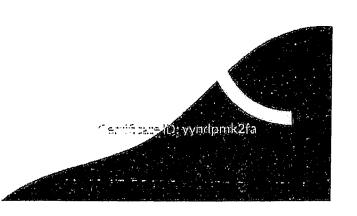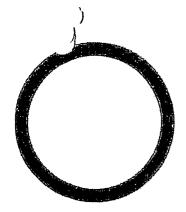
Oleg Siminel, Sr. Security Solutions Architect

✳ Siemplify

Certificate ID: k1tg8lokrf

CERTIFICATE
OF COMPLETION

CERTIFIES

Erlyn Barredo

For the successful completion of:

Siemplify Certified SOAR Analyst (SCSA)
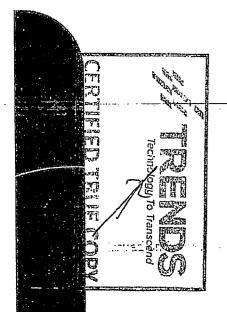
Oleg Siminel, Sr. Security Solutions Architect

SOAR CERTIFICATION COURSE

Certificate ID: yyndpmk2fa

Siemplify

CERTIFICATE
OF COMPLETION

CERTIFIES

Erlyn Barredo
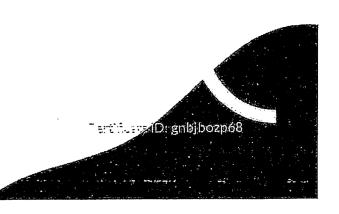
For the successful completion of:

Siemplify Platform Fundamentals

Oleg Siminel, Sr. Security Solutions Architect

SOAR CERTIFICATION COURSE

TRENDS
Technology To Transcend

CERTIFIED TRUE COPY

Certificate ID: gnbjbozp68

Siemplify

Trends & Technologies, Inc.

ERL

ERLYN B. BARREDO
RTC-0002

EMPLOYEE'S SIGNATURE

TRENDS

TRENDS
Technology To Transcend

October 12, 2023
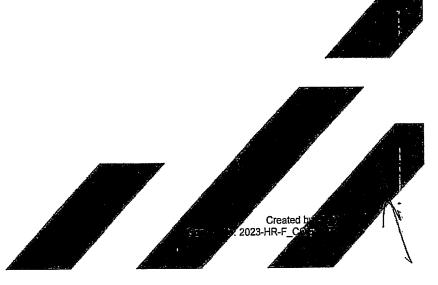
CERTIFICATE OF EMPLOYMENT

This certifies that Ms. Erlyn 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

Created by
2023-HR-F_C

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	• 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: o Managed Security Services in a Mutual Life Insurance Company o Managed IT Security, Managed Wi-Fi, Managed Network in a Pharmaceutical Company o Managed Security Operations Center in a Government Financial Institution o Managed Security Services in four (4) Government Financial Institution
2.	APR 2015 – JUL 2017	CONVERGYS PHILIPPINES, INC.	ASSOCIATE TRAINER	• Mentored new trainers. • Acted as SME for new training curriculum. • Facilitated classroom training to teach program product knowledge, call handling skills, customer service/sales skills and program process and procedures.

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

TRENDS
Technology To Transcend

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

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

FORTINET.

NSE Certification Program

NSE

ASSOCIATE

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

_____ Xie
CEO of Fortinet

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

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