CONTOSO Global Security (SGS)

Security Operations

Center of Excellence Guide

05-Sept.-2019

Version 1.0

Document Information

Document Title	Contoso Inc. Center of Excellence Guide
Document Owner	Documentation Team
Review Cycle	Quarterly

Revision History

Date	Description	Version
09-Sept-2019	Initial release, Jackie Emanuele	1.0

Table of Contents

1. Welcome

This Guide has been developed by the SGS Contoso team to assist you in your role in helping protect the company against unwanted cybersecurity threats and attacks. This Guide provides procedures on incident monitoring and handling, procedures on what steps to follow, escalations, and record-keeping best practices, all of which are essential to maintaining effective Security Operations.

Your role is critical to keeping the company one step ahead of increasingly complex attacks.

We hope that this Guide is a useful reference!

This Guide is also an essential training tool that can be used to help onboard new employees as well as a refresher to existing members of the SGS Contoso team.

1.1. Purpose

The purpose of the Contoso, Inc. Center of Excellence Guide is to provide the team (responders, handlers, assignees, IR personnel) with proven, effective capital to help continue to drive success for incident response.

It is our goal to align the team with key learnings and best practices for incident response so they can easily identify, capture, and re-use information if necessary. This capital will help drive success and offer increased value to company. Individual contributors as well as site leadership can use this guide to conduct run-time business, incident response onboarding and offboarding, awareness presentations, and more.

The information in this guide has been vetted by the SGS Contoso Management Team.

As you consult the various pages in this manual, you'll be introduced to different types of material including, but not limited to:

- Reference information
- Best practice learnings
- Intellectual capital
- Contact information
- Templates
- Tools
- And more!

1.2. Audience

If you are…	Then…
New to working with SGS Contoso	You will glance into the Incidence Response world and obtain general suggestions for onboarding, escalations, and coverage times at your site. You will be introduced to the tools the Center of Excellence team uses, and you'll discover conceptual information that may help drive key decision-making.
Skilled at working with SGS Contoso but would like to stay current on processes and general procedures	Look for specific topics that can help you such as templates, reporting, and other tactical run-time procedures. In various sections, you'll peruse content that helps you with day-to-day job duties.

A note from Center of Excellence

The goal of this book is to harvest and provide a single source of information to you so you can do what you do best -- effectively manage incident response. The Guide owner from the SGS Contoso team is committed to creating new sections for inclusions as appropriate. This guide is intended for internal use. Use it to increase your knowledge, visibility, and readiness for all Incident Response activities.

About Center of Excellence

SGS Contoso facilitates and handles all incidents that:

- violate computer security policies, acceptable use policies, or standard security practices for malicious intent.

Some types of activity that are widely recognized as being security incidents are:

- successful attempts to gain unauthorized access to a system or its data.
- unwanted disruption or denial of service (DoS).
- unauthorized use of a system for the processing or storage of data, or changes to system hardware, firmware or software characteristics without the owner's knowledge, instructions, and approval.
- unauthorized processing (including recording, storage, transfer, editing, or erasure) of data (belonging to the company, its personnel, or customers).

Our Organization

The SGS Contoso team lives under the company's Cyber Defense Center (CDC).
Review the contact information periodically to ensure you have the latest information to reach SGS Contoso.

View this link to learn more about the Center of Excellence.

- CoE Documentation {link disabled for purposes of sampling}

Access key documentation for the company's incident response processes.

The Center of Excellence point of view: the company's Incident Response teams *view each suspected event as an information security incident until it has been determined not to be one***.**

2. Incident Escalation Hierarchy Contact Information

Here is a regional table for the organization support team and their numbers throughout the world.


Spreadsheet.xlsx

Escalation Contacts

2.1. Incident Response Partners

Our Suppliers are our valued partners that run our front-line support business. To carry out operations and commitments, the company has set up the following SharePoint sites for continued communication, collaboration, and document control with our internal partners.

Global Support Team

https://wiki.wdf.corp/wiki/display/contoso/CONTOSO+Support

Partners (Network, Systems, etc.)

https://wiki.contoso.com/confluence/display/SO/Contact+Details+-+Other+Teams

Vendors

https://wiki.contoso.com/confluence/display/SO/SecOps+Vendor+Management+Information

For outages or please refer to the Business Continuity Plan. For access, please contact email@Contoso.com.

2.2. Hours of Operation

Regular Hours

Monday - Friday

APAC- 08:00 AM PHT - 17:00 PM PHT

US (BLV) - 08:00 AM- 17:00 PM PST (M-F **+ Saturday and Sunday)**

EMEA - 08:00 AM-17:00 PM CET

Shift Handover Times Map

Shift-Handovers

Bellevue to Manila - 17:00 PM PST (08:00 PM PHT)

Manila to Prague – 16:00 PM PHT (10:00 AM GMT +2)

Prague to Bellevue – 17:00 PM GMT +2 (8:00 AM PST)

2.2.1. Role Definitions

Consult your individual role maps given to you by management within your onboarding packet for more role-specific information.

The following roles are vital to the team and successful incident management at the company. For more information about roles, visit the internal Wiki site.

CDC - (Cyber Defense Center) SIM Team - Responds to cyber incidents and is responsible for addressing, handling, and resolving incidents. CDC works in conjunction with SGS Contoso to contain impacted systems, eradicate threats, recover systems to safe states, and preserve evidence of required-by-law documentation used for forensic purposes. Records decisions, actions, and times for the incident record.

SecOps Team (Security Operations) - SGS Contoso's internal security team that acknowledge, handle, and resolve security incidents being dispatched by the SIM Team.

Analyst Lead - Operates as a member of the SGS Contoso to review logs and alerts and lead security analysts to augment processes, procedures for log and alert review. The On-call Lead ensures that investigations and compliance tasks are properly evidenced in the security system. On point to escalate issues about processes and technology. 100% coverage of Sec Incident Management process for P1 cases.

Analyst III - Drives Playbook creation (see Section 10); conducts gap analysis and incident analysis escalations. Mentors analysts and reviews incident process. The escalation point for Analyst II. Handles analysis and triage of Security P1 incidents. Conducts review of submitted SIEM use cases.

Analyst II - Leads use case creation (see Section 9). Leads incident analysis. Escalation point for Analyst I. Handles 100% of analysis and triage of security incidents (from P2 to P1 incidents); generates Root Cause Analysis report and other reports. Secures at least 10 approved use cases per year.

Analyst I - Monitors lead; primary security alerts responder for triage. Incidents from SIEM and other security tools and channels. Handles 100% of coverage incidents including analysis and triage of security incidents (up to P2 incidents).

Engineer - As a key part of the SecOps team, the Sec Engineer works with Splunk search, SIEM, and log managers and other security platforms. The exposure and engagement to incident response and threat hunting helps to ensure that that operational incidents are understood and reviewed for investigations. Access-management-related tasks are common for Sec Engineer duties.

2.3. Incident Prioritization Matrix

"When in doubt, treat any incident as an information security incident until it has been determined not to be."
~ SGS Contoso Management

In the matrix below, the "X" axis conveys severity. The "Y" axis conveys urgency. The initial severity rating given to an incident may be adjusted during execution.

Severity

Urgency	Critical	High	Medium	Low
Critical	P0	P1	P2	P3
High	P1	P1	P2	P3
Medium	P1	P2	P3	P3
Low	P2	P3	P3	P4

P0/P1 = highest priority to attend to ASAP
P2 = medium priority
P3 = low priority
P4 = lowest priority

Incident Prioritization Guideline

Within the company, information security incidents are grouped in different risk categories based on impact, severity, and urgency. The category tables in this section are used to measure the over-all incident priority.

Incident Urgency (Categories of Urgency)

The below categories help determine the Incident's urgency; choose the *highest* relevant category for your incident.

Category	Description
Critical	• Damage caused has stopped all business functions • No customer transactions are coming through • Company executive members are affected
High	• Business functions and operations are being disrupted from doing work • Most customers are not able to do transactions
Medium	• Business functions is slowed down due to incident • Some customers are being disrupted from doing transactions
Low	• Only a few people are affected • Only 1 customer is being affected

Incident Impact (Categories of Impact)

This section establishes categories of impact. To determine the Incident's impact, choose the *highest* relevant category:

Category	Description
Critical	Asset or assets have been accessed in an unauthorized manner with privileged access and secret data has been accessed/modified or can be accessed
High	Asset(s) have been accessed/modified by in an unauthorized manner and privileged access has been gained but no secret data has been accessed/modified or service is not available
Medium	Asset(s) have been accessed/modified in an unauthorized manner, but no privileged access has been gained and no secret data has been accessed
Low	Intruder attempted access/modified in an unauthorized manner against contoso assets, but no sensitive data has been accessed and no privileged access was gained

2.4. Communications

When reporting an information security incident or information security vulnerability to Cyber Defense Center (CDC) or SGS Contoso, personnel must do their best to report incidents timely and completely in all circumstances.

Incidents must be reported within:

- *one operational hour* of a suspected security incident by internal personnel
  -or-
- as determined by *specific contractual requirements* by external personnel or external agency policy

When SGS Contoso receives the report, it has already been delivered to the CDC (Cyber Defense Center) SIM Team via email or the GSIM ticketing system. In extenuating circumstances—or if neither email nor ticketing systems function properly—reports are made via phone or personal communication, such as Slack or Skype or other instant messaging tool.

External parties

Aside from the Cyber Defense Center (CDC) SIM Team, only designated SGS Contoso personnel, such as the SGS Contoso Management Team and/or their delegates, with the presence of the Compliance and Legal Team, are permitted to report information security incident updates and summary to external parties. Such parties may include law enforcement and external information security teams.

In the event of a breach of confidential information, such as with personally identifiable information (PII), designated SGS Contoso personnel must communicate with the company's senior management, governmental liaisons, and attorneys before creating external information security incident reports. This process greatly facilitates the company's meeting its contractual and legal responsibilities.

There are various Communication Incident Response communication paths within the IR ecosystem.

SGS Contoso Communications - E-mails sent by SGS Contoso to Partners whenever an alert is necessary (e.g. - informing of an outage; planned maintenance; etc.).

Vendor Communications - E-mails sent by SGS Contoso to Partners whenever process, launch, or new tool information needs to be distributed. Vendor Comms get posted to the Vendor Comm Wiki for support personnel to review.

Updates and Release Notifications – Emails sent by SGS Contoso management team about new Training and any new release tools information to SGS Contoso personnel.