

E5 - TICKETING SNOW

**RÉPONDRE AUX INCIDENTS ET AUX DEMANDES
D'ASSISTANCE ET D'ÉVOLUTION**

CONTEXTE

Entreprise

- Sanofi est une entreprise biopharmaceutique qui découvre, développe, fabrique et commercialise une gamme de médicaments et de vaccins.
- 500 employés avec en moyenne 1.7 incident. par personnes.

Objectif

- Analyser les incidents et leur priorité
- Documenté les incidents et effectué un suivi des étapes de résolution
- mettre en relation ou relancer les équipes en charges des incidents



sanofi

METHODOLOGIE

Approche

- Suivi des tickets à haute priorité de manière journalière
- Suivi des tickets “long run” de manière hebdomadaire
- Résolution des tickets locaux à faible impact.
- Relance des équipes en charge du ticket et modification de statut
- Attribution des tickets “perdus” aux équipes correspondantes
- Présentation d’un rapport mensuel à l’équipe

sanofi

EXAMPLES

Incident INC0010616 [Workspace view]

Follow Update Resolve Delete

Number: INC0010616

Caller: Rapid7 InsightConnect

Category: Inquiry / Help

Subcategory: -- None --

Business service:

Configuration item:

Contact type: -- None --

State: New

Impact: 3 - Low

Urgency: 3 - Low

Priority: 5 - Planning

Assignment group:

Assigned to:

Short description: New Vuln "generic-icmp-timestamp" on Asset "r7-orchestrator-1-34.vuln.lax.rapid7.com"

Description: InsightVM has discovered a new vulnerability, "ICMP timestamp response", on host "r7-orchestrator-1-34.vuln.lax.rapid7.com". This ticket should be closed once this vulnerability on this host has been remediated. Closing this ticket will trigger a validation scan in InsightVM to confirm the vulnerability has been removed from the host.

*Vulnerability Details:
 * Severity: 1
 * Solution(s): generic-icmp-timestamp-disable-hpux,generic-icmp-timestamp-disable-ios,generic-icmp-timestamp-disable-irix,generic-icmp-timestamp-disable-linux,generic-icmp-timestamp-disable-nt,generic-icmp-timestamp-disable-openbsd,generic-icmp-timestamp-disable-pix,generic-icmp-timestamp-disable-solaris,generic-icmp-timestamp-disable-w2k,generic-icmp-timestamp-disable-xp-2k3,generic-icmp-timestamp-disable-vista_2k8,generic-icmp-timestamp-disable-via-firewall
 * Affected Architectures:
 * Date Published: 1997-08-01T00:00:00.000Z
 * Description:
 ""
 <p>The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.</p>
 <p>In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.</p>
 ""

Incidents New Search Number Search

1 to 20 of 77

	Number	Opened	Short description	Caller	Priority	State	Category	Assignment group	Assigned to	Updated	Updated by
	INC0010015	2020-12-07 08:31:42	Process Not Running	Barbara Hindley	3 - Moderate	New	Software	L1 Queue	(empty)	2020-12-07 08:32:08	admin
	INC0010014	2020-12-07 08:31:02	Backup Failed	Yhian Brzostowski	4 - Low	New	Hardware	L1 Queue	(empty)	2020-12-07 08:31:36	admin
	INC0010013	2020-12-07 08:30:31	Database utilization exceeds 90% threshold	Vince Etzel	1 - Critical	New	Database	L1 Queue	(empty)	2020-12-10 06:30:56	system
	INC0010012	2020-12-07 08:29:31	Database utilization exceeds 75% threshold	Avery Parbol	2 - High	New	Database	L1 Queue	(empty)	2020-12-07 08:30:19	admin
	INC0010011	2020-12-07 08:28:49	User zz1111 unable to login	Annie Approver	3 - Moderate	New	Software	L2 Queue	(empty)	2020-12-07 08:29:24	admin
	INC0010010	2020-12-07 08:28:20	All user unable to login	Andrew Och	1 - Critical	New	Software	L2 Queue	(empty)	2020-12-10 06:28:45	system
	INC0010009	2020-12-07 08:27:40	Printer Zzz unable to print	Alfonso Griplen	3 - Moderate	In Progress	Software	L2 Queue	(empty)	2020-12-07 08:28:12	admin
	INC0010008	2020-12-07 08:27:08	All Printers Unable to Print	Angelo Ferretz	1 - Critical	New	Software	L2 Queue	(empty)	2020-12-10 06:27:31	system
	INC0010007	2020-12-07 08:26:43	IDOCs unable to send Both Flow	Alex Babeck	1 - Critical	New	Inquiry / Help	L2 Queue	(empty)	2020-12-10 06:27:01	system
	INC0010006	2020-12-07 08:26:00	IDOCs unable to send Outbound	Aileen Mottern	2 - High	New	Software	L2 Queue	(empty)	2020-12-07 08:26:36	admin
	INC0010005	2020-12-07 08:25:24	IDOCs unable to send Inbound	Adela Cervantsz	2 - High	New	Software	L2 Queue	(empty)	2020-12-07 08:25:53	admin
	INC0010004	2020-12-07 08:24:27	Network Outage	Abraham Lincoln	1 - Critical	New	Network	L1 Queue	(empty)	2020-12-10 06:35:59	system
	INC0010003	2020-12-07 08:21:45	Power Outage	Abel Tuter	1 - Critical	New	Inquiry / Help	L1 Queue	(empty)	2020-12-10 06:36:10	system
	INC0009009	2018-08-30 01:06:16	Unable to access the shared folder.	David Miller	4 - Low	New	Inquiry / Help	L2 Queue	(empty)	2020-12-07 08:33:02	admin
	INC0009005	2018-08-31 21:35:21	Email server is down.	David Miller	1 - Critical	New	Software	L2 Queue	(empty)	2020-12-10 06:33:12	system
	INC0009004	2018-09-01 06:13:30	Defect tracking tool is down.	David Miller	3 - Moderate	Closed	Software	(empty)	(empty)	2020-09-24 18:12:19	system
	INC0009003	2018-08-30 02:17:32	Cannot sign into the company portal app	David Miller	3 - Moderate	Closed	Inquiry / Help	(empty)	(empty)	2018-12-12 23:39:53	admin
	INC0009002	2018-09-16 05:49:23	My computer is not detecting the headphone device	David Miller	3 - Moderate	Closed	Hardware	(empty)	(empty)	2020-09-24 18:12:17	system

		IMPACT		
		High	Mid	Low
URGENCY	High	1	2	3
	Mid	2	3	4
	Low	3	4	5



COMPÉTENCES ACQUISES

Compétences Techniques

- Classification des priorités
- Prise en compte des SLA
- Logiciel de ticketing centralisé (ServiceNow)
- Lecture et interprétation de la matrice Impact/Urgence

Compétences Organisationnelles

- Priorisation des tâches selon le niveau de criticité
- Communication inter-équipes pour le suivi des incidents
- Rigueur dans la documentation et le suivi des étapes de résolution

The logo for ServiceNow, featuring the word "servicenow" in a dark teal, lowercase, sans-serif font. The letter "o" is a light teal color.The logo for Sanofi, featuring the word "sanofi" in a bold, black, lowercase, sans-serif font. There are two purple dots: one above the letter "i" and one to the left of the letter "s".

DIFFICULTÉS

Difficultés Techniques

- Prise en main de l'interface ServiceNow, dont la navigation et les filtres peuvent être complexes pour un nouvel utilisateur

Difficultés organisationnelles

- Identification des équipes responsables d'un ticket lorsque l'attribution est manquante ou incorrecte ("tickets perdus")
- Difficulté à obtenir une réponse rapide des équipes sollicitées pour la résolution d'un incident, rendant le suivi et la relance indispensables



sanofi



CONFIDENTIALITÉ

SANOFI

**SANOFI étant une entreprise sensible et stratégique, il m'est
formellement interdit de divulguer
une quelconque documentation technique ou stratégique.**