AutoSecDeploy2

29 Apr 2023

Project manager	
Project dates	21 Nov 2022 - 7 Jul 2023
Completion	5%
Tasks	52
Resources	0

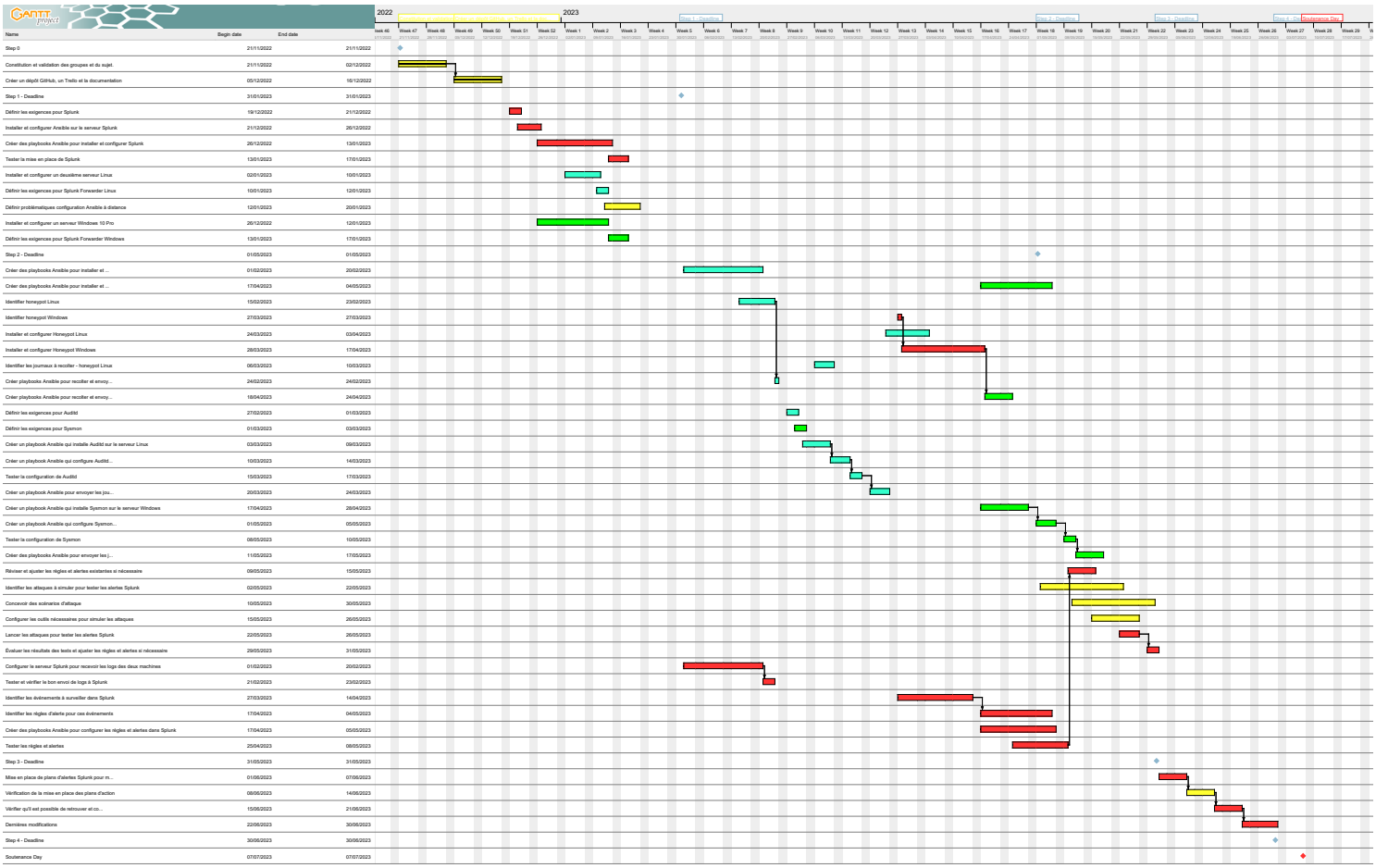
Tasks

Name	Begin date	End date
Step 0	21/11/2022	21/11/2022
Constitution et validation des groupes et du sujet.	21/11/2022	02/12/2022
Créer un dépôt GitHub, un Trello et la documentation	05/12/2022	16/12/2022
Step 1 - Deadline	31/01/2023	31/01/2023
Définir les exigences pour Splunk	19/12/2022	21/12/2022
Installer et configurer Ansible sur le serveur Splunk	21/12/2022	26/12/2022
Créer des playbooks Ansible pour installer et configurer Splunk	26/12/2022	13/01/2023
Tester la mise en place de Splunk	13/01/2023	17/01/2023
Installer et configurer un deuxième serveur Linux	02/01/2023	10/01/2023
Définir les exigences pour Splunk Forwarder Linux	10/01/2023	12/01/2023
Définir problématiques configuration Ansible à distance	12/01/2023	20/01/2023
Installer et configurer un serveur Windows 10 Pro	26/12/2022	12/01/2023
Définir les exigences pour Splunk Forwarder Windows	13/01/2023	17/01/2023
Step 2 - Deadline	01/05/2023	01/05/2023
Créer des playbooks Ansible pour installer et configurer Splunk Forwarder sur Linux	01/02/2023	20/02/2023
Créer des playbooks Ansible pour installer et configurer Splunk Forwarder sur Windows	17/04/2023	04/05/2023
Identifier honeypot Linux	15/02/2023	23/02/2023
Identifier honeypot Windows	27/03/2023	27/03/2023
Installer et configurer Honeypot Linux	24/03/2023	03/04/2023
Installer et configurer Honeypot Windows	28/03/2023	17/04/2023
Identifier les journaux à recolter - honeypot Linux	06/03/2023	10/03/2023
Créer playbooks Ansible pour recolter et envoyer les journaux Linux au serveur Splunk	24/02/2023	24/02/2023
Créer playbooks Ansible pour recolter et envoyer les journaux Windows au serveur Splunk	18/04/2023	24/04/2023
Définir les exigences pour Auditd	27/02/2023	01/03/2023
Définir les exigences pour Sysmon	01/03/2023	03/03/2023
Créer un playbook Ansible qui installe Auditd sur le serveur Linux	03/03/2023	09/03/2023
Créer un playbook Ansible qui configure Auditd pour journaliser les événements pertinents	10/03/2023	14/03/2023
Tester la configuration de Auditd	15/03/2023	17/03/2023
Créer un playbook Ansible pour envoyer les journaux Auditd à notre serveur Splunk	20/03/2023	24/03/2023
Créer un playbook Ansible qui installe Sysmon sur le serveur Windows	17/04/2023	28/04/2023
Créer un playbook Ansible qui configure Sysmon pour journaliser les événements pertinents	01/05/2023	05/05/2023
Tester la configuration de Sysmon	08/05/2023	10/05/2023
Créer des playbooks Ansible pour envoyer les journaux sysmon à notre serveur Splunk	11/05/2023	17/05/2023
Réviser et ajuster les règles et alertes existantes si nécessaire	09/05/2023	15/05/2023

Tasks

Name	Begin date	End date
Identifier les attaques à simuler pour tester les alertes Splunk	02/05/2023	22/05/2023
Concevoir des scénarios d'attaque	10/05/2023	30/05/2023
Configurer les outils nécessaires pour simuler les attaques	15/05/2023	26/05/2023
Lancer les attaques pour tester les alertes Splunk	22/05/2023	26/05/2023
Évaluer les résultats des tests et ajuster les règles et alertes si nécessaire	29/05/2023	31/05/2023
Configurer le serveur Splunk pour recevoir les logs des deux machines	01/02/2023	20/02/2023
Tester et vérifier le bon envoi de logs à Splunk	21/02/2023	23/02/2023
Identifier les événements à surveiller dans Splunk	27/03/2023	14/04/2023
Identifier les règles d'alerte pour ces événements	17/04/2023	04/05/2023
Créer des playbooks Ansible pour configurer les règles et alertes dans Splunk	17/04/2023	05/05/2023
Tester les règles et alertes	25/04/2023	08/05/2023
Step 3 - Deadline	31/05/2023	31/05/2023
Mise en place de plans d'alertes Splunk pour mieux cibler les faiblesses de notre infrastructure.	01/06/2023	07/06/2023
Vérification de la mise en place des plans d'action	08/06/2023	14/06/2023
Vérifier qu'il est possible de retrouver et comprendre les attaques qui ont eu lieu sur notre infra.	15/06/2023	21/06/2023
Dernières modifications	22/06/2023	30/06/2023
Step 4 - Deadline	30/06/2023	30/06/2023
Soutenance Day	07/07/2023	07/07/2023

Gantt Chart



Name	Begin date	End date
Step 0	21/11/2022	21/11/2022
Constitution et validation des groupes et du sujet.	21/11/2022	02/12/2022
Créer un dépôt GitHub, un Trello et la documentation	05/12/2022	16/12/2022
Step 1 - Deadline	31/01/2023	31/01/2023
Définir les exigences pour Splunk	19/12/2022	21/12/2022
Installer et configurer Ansible sur le serveur Splunk	21/12/2022	26/12/2022
Créer des playbooks Ansible pour installer et configurer Splunk	26/12/2022	13/01/2023
Tester la mise en place de Splunk	13/01/2023	17/01/2023
Installer et configurer un deuxième serveur Linux	02/01/2023	10/01/2023
Définir les exigences pour Splunk Forwarder Linux	10/01/2023	12/01/2023
Définir problématiques configuration Ansible à distance	12/01/2023	20/01/2023
Installer et configurer un serveur Windows 10 Pro	26/12/2022	12/01/2023
Définir les exigences pour Splunk Forwarder Windows	13/01/2023	17/01/2023
Step 2 - Deadline	01/05/2023	01/05/2023
Créer des playbooks Ansible pour installer et ...	01/02/2023	20/02/2023
Créer des playbooks Ansible pour installer et ...	17/04/2023	04/05/2023
Identifier honeypot Linux	15/02/2023	23/02/2023
Identifier honeypot Windows	27/03/2023	27/03/2023
Installer et configurer Honeypot Linux	24/03/2023	03/04/2023
Installer et configurer Honeypot Windows	28/03/2023	17/04/2023
Identifier les journaux à recolter - honeypot Linux	06/03/2023	10/03/2023
Créer playbooks Ansible pour recolter et envoy...	24/02/2023	24/03/2023
Créer playbooks Ansible pour recolter et envoy...	18/04/2023	24/04/2023
Définir les exigences pour Auditd	27/02/2023	01/03/2023
Définir les exigences pour Sysmon	01/03/2023	03/03/2023
Créer un playbook Ansible qui installe Auditd sur le serveur Linux	03/03/2023	09/03/2023
Créer un playbook Ansible qui configure Auditd ...	10/03/2023	14/03/2023
Tester la configuration de Auditd	15/03/2023	17/03/2023
Créer un playbook Ansible pour envoyer les jou...	20/03/2023	24/03/2023
Créer un playbook Ansible qui installe Sysmon sur le serveur Windows	17/04/2023	28/04/2023
Créer un playbook Ansible qui configure Sysmon...	01/05/2023	05/05/2023
Tester la configuration de Sysmon	08/05/2023	10/05/2023
Créer des playbooks Ansible pour envoyer les j...	11/05/2023	17/05/2023
Réviser et ajuster les règles et alertes existantes si nécessaire	09/05/2023	15/05/2023
Identifier les attaques à simuler pour tester les alertes Splunk	02/05/2023	22/05/2023
Concevoir des scénarios d'attaque	10/05/2023	30/05/2023
Configurer les outils nécessaires pour simuler les attaques	15/05/2023	26/05/2023
Lancer les attaques pour tester les alertes Splunk	22/05/2023	26/05/2023
Évaluer les résultats des tests et ajuster les règles et alertes si nécessaire	29/05/2023	31/05/2023
Configurer le serveur Splunk pour recevoir les logs des deux machines	01/02/2023	20/02/2023
Tester et vérifier le bon envoi de logs à Splunk	21/02/2023	23/02/2023
Identifier les événements à surveiller dans Splunk	27/03/2023	14/04/2023
Identifier les règles d'alerte pour ces événements	17/04/2023	04/05/2023
Créer des playbooks Ansible pour configurer les règles et alertes dans Splunk	17/04/2023	05/05/2023
Tester les règles et alertes	25/04/2023	08/05/2023
Step 3 - Deadline	31/05/2023	31/05/2023
Mise en place de plans d'alertes Splunk pour m...	01/06/2023	07/06/2023
Vérification de la mise en place des plans d'action	08/06/2023	14/06/2023
Vérifier qu'il est possible de retrouver et co...	15/06/2023	21/06/2023
Dernières modifications	22/06/2023	30/06/2023
Step 4 - Deadline	30/06/2023	30/06/2023
Soutenance Day	07/07/2023	07/07/2023

Resources Chart