

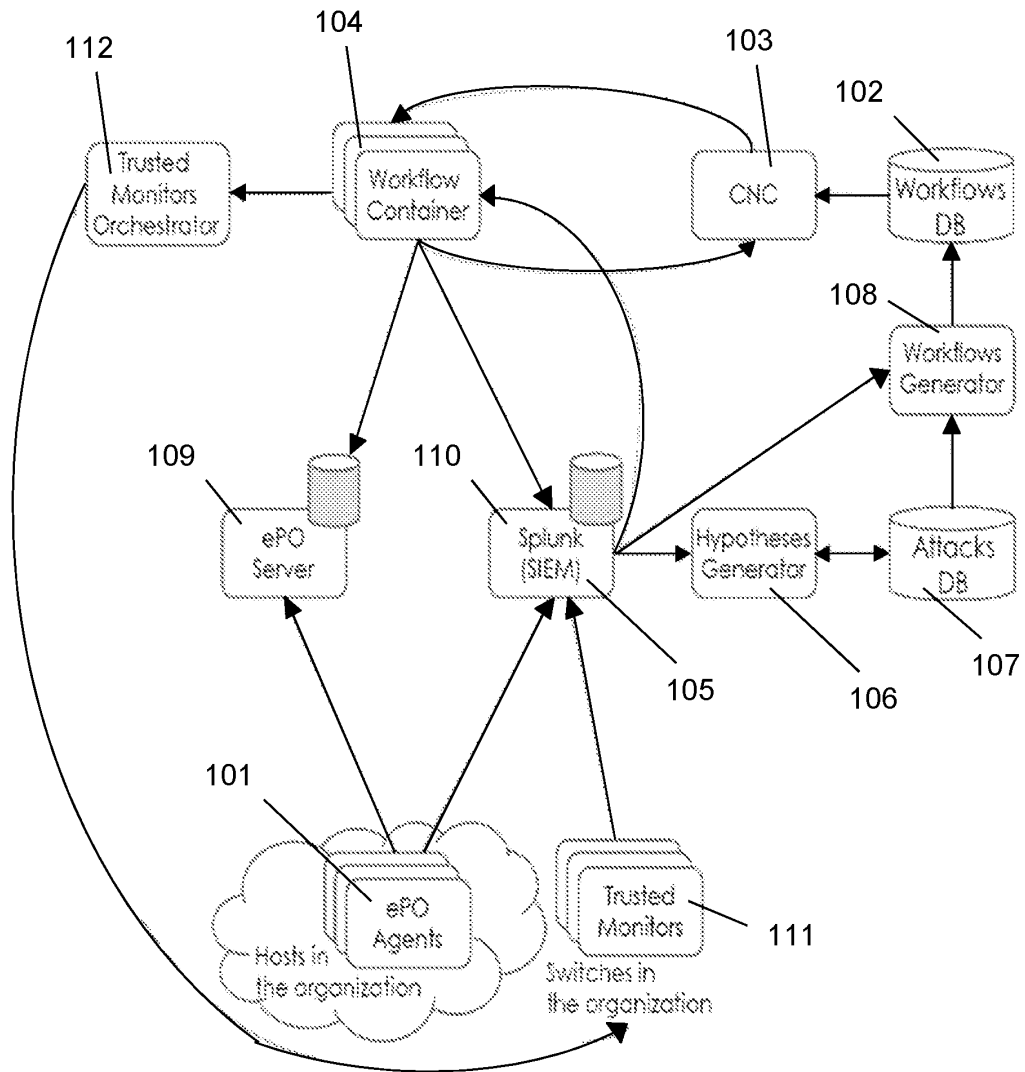


Fig. 1

```

def main():
    iocs = [
        ['FileObjectType', 'Avtask.exe'], ['FileObjectType', 'Wz.exe'],
        ['FileObjectType', 'Alg.exe'], ['FileObjectType', 'tlcrvc.exe'],
        ['FileObjectType', 'svchost.exe'], ['FileObjectType', '104.dll'],
        ['FileObjectType', 'Haslo.dat'], ['FileObjectType', 'Haslo.exe'],
        ['FileObjectType', 'h2.exe'], ['FileObjectType', 'suprv.exe'],
        ['FileObjectType', 'Dcs.exe'], ['FileObjectType', 'Opd.exe'],
        ['FileObjectType', 'GMSD.exe'], ['FileObjectType', 'dofragv.exe'],
        ['FileObjectType', 'port.exe'], ['FileObjectType', 'kabdul']
    ]

    # create a new policy based on the given iocs, assigned to the agent and enforce
    create_and_enforce_policy(iocs)

    # Splunk functionality
    alert_num = 0
    splunkClient.create_alert(alert_num, iocs)
    logger.info("an alert was defined. The container will be notified of any iocs found by src.")
    communicator.bind_handlers_to_alert(alert_num, get_results)
    logger.info("The alert was bound to the get_results handler")

    if name == "main":
        main()

```

Fig. 2

```

agent_name = 'AGENT1'

def create_and_enforce_policy(locs):
    policy = epoclient.create_policy(locs)
    logger.info("Policy based on the locs was created successfully...")
    epoclient.import_policy(policy)
    logger.info("Policy was imported to the epo Policies Catalog")

    policy_properties = epoclient.get_policy_properties()
    policy_properties = policy_properties[0]
    epoclient.assign_policy_to_system(agent_name, policy_properties['productid'],
                                     str(policy_properties['typeid']), str(policy_properties['objectid']))
    logger.info("Policy was assigned to the agent")

    epoclient.enforce_policies_using_wakeup_agent(agent_name)
    logger.info("Policy is now enforced at the agent")

def search_network_artifacts():
    logger.info("Searching for network artifacts...")
    network_locs = [['AddressObjectType', '193.16.89.4'], ['AddressObjectType', '46.28.388.132'],
                    ['AddressObjectType', '188.42.233.43'], ['AddressObjectType', '5.19.218.152'],
                    ['AddressObjectType', '93.116.27.87']]
    # create a new policy based on the given locs, assigned to the agent and enforce
    create_and_enforce_policy(network_locs)
    splunkClient.create_alert(alert_name, network_locs)
    logger.info("An alert was defined. The container will be notified of any IOC's found by epo.")

def get_results(**content):
    results = splunkClient.get_splunk_results(content['sid'])
    logger.info("The following IOC's were found:")
    for loc_type, observable in results.items():
        logger.info("Type: {} | Value: {}".format(loc_type, observable))
    search_network_artifacts()

```

Fig. 3

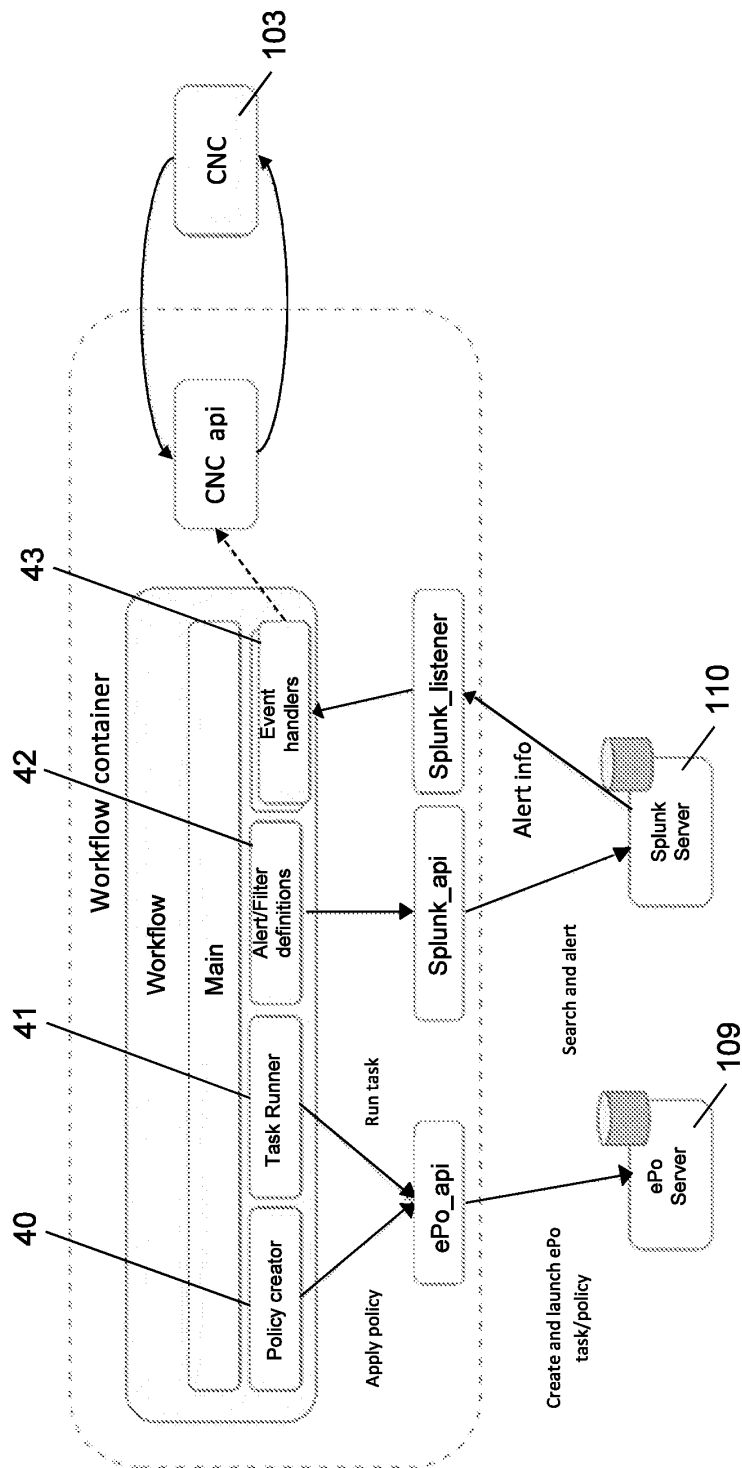


Fig. 4

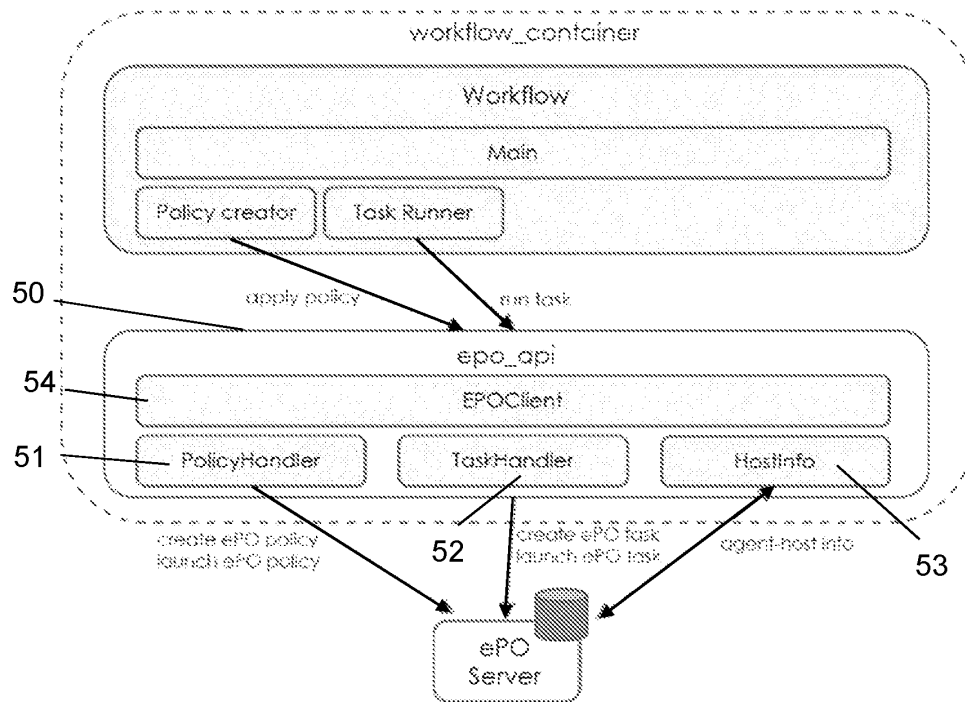


Fig. 5

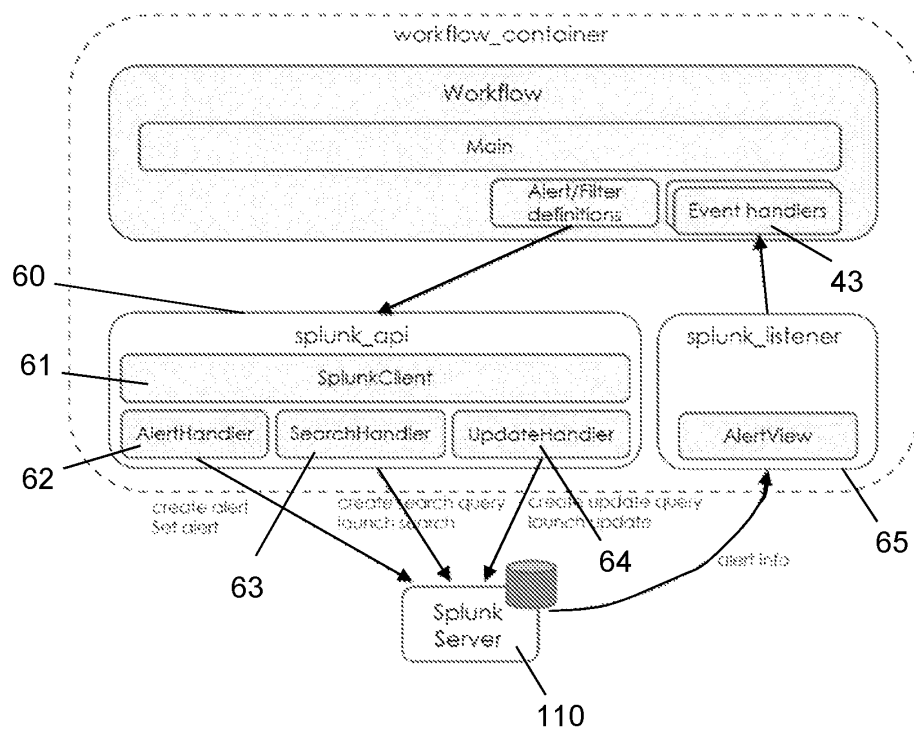


Fig. 6

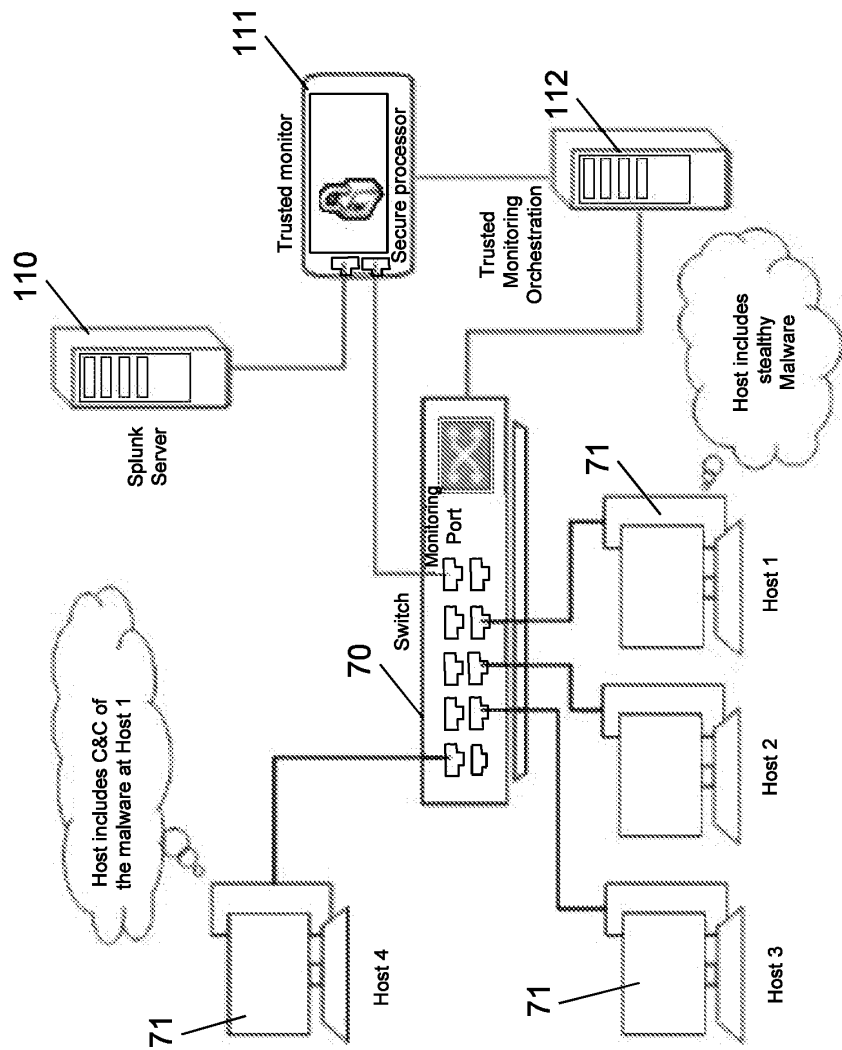


Fig. 7