DESIGNING PLAYBOOKS WITH PURPLE TEAM APPROACH

SANS Purple Team Summit 2021

whoami

semanurtg

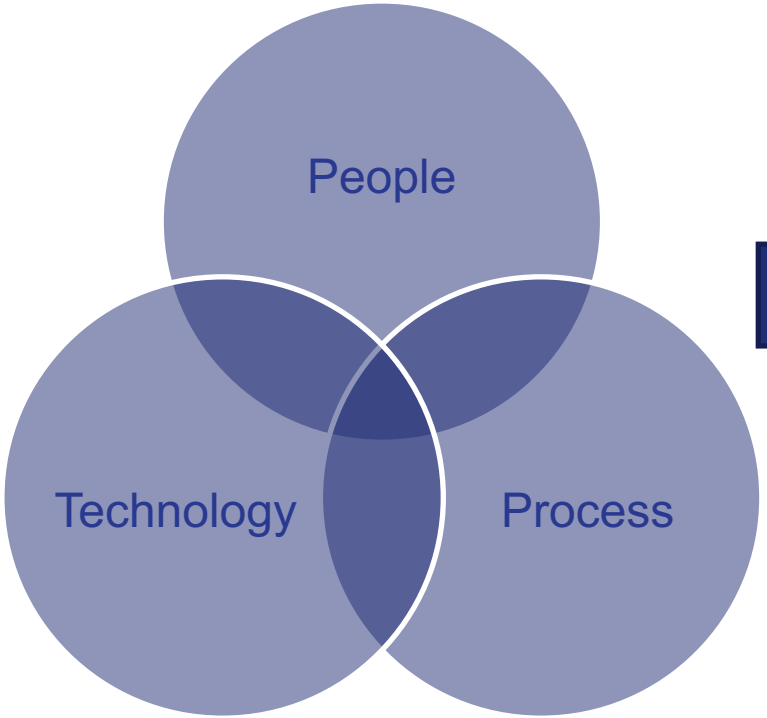
Semanur Guneysu

- 3+ cyber security experience
- SOC Analyst and Team Leader
- Designing MSSP - SOC Services
- Beginner for purple teaming

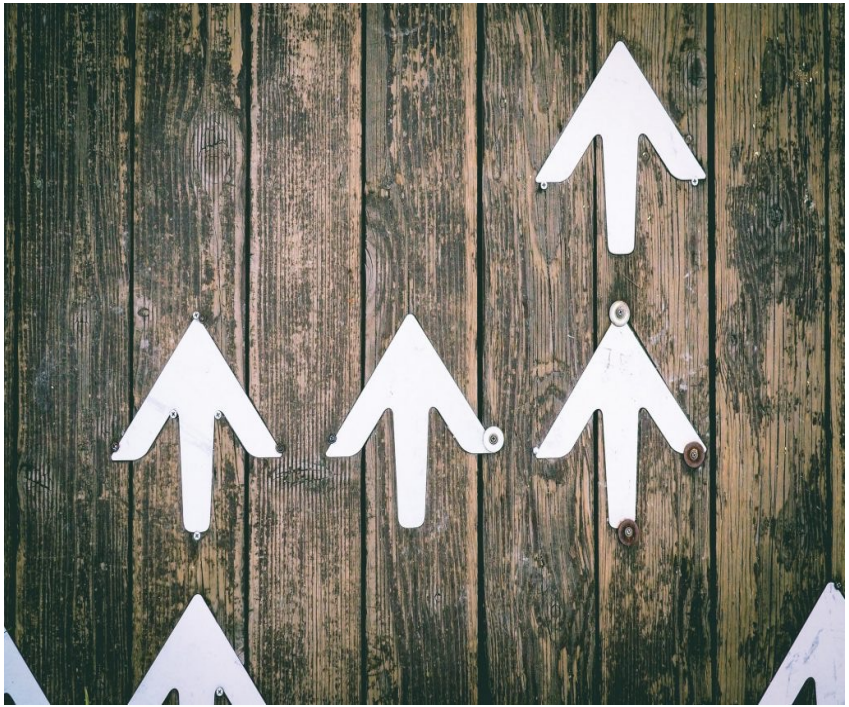
Agenda

- The **5W1H** of Purple Teaming in SOC
- Requirements / Tools
- Take Advantage of Playbooks
- Demo Time

5W1H – Where ?



5W1H – Why ?



Goals:

- Self - Assessment
- Improvement
- Learning & Teaching

5W1H – What ?

Purple Teaming

5W1H – When ?

Continuous

On Demand

5W1H – Who ?

Threat Hunters

SOC Analysts

Incident Responders

Red Teamers

...

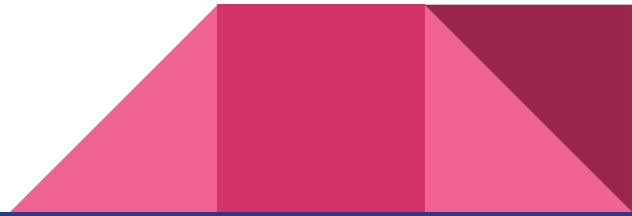
...

5W1H – How ?

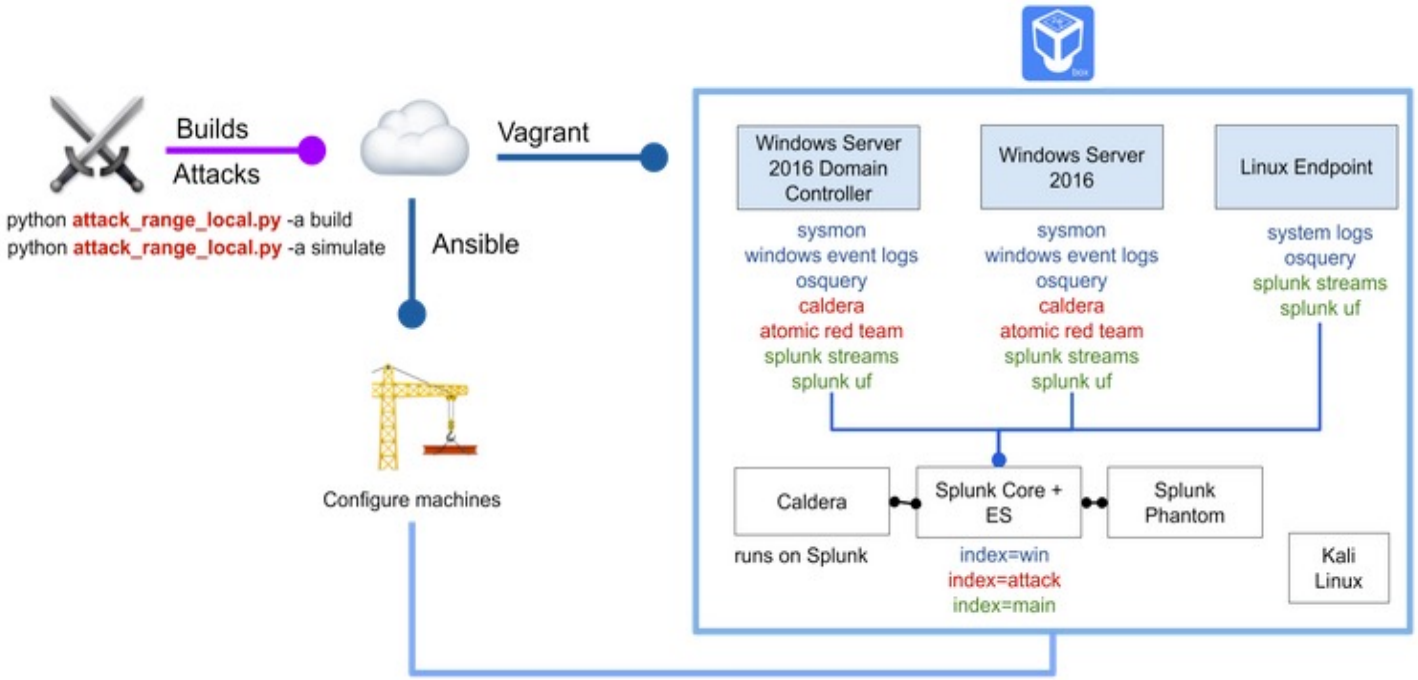
1. Plan scope
2. Decide the tools and requirements
3. Determine the methodology
4. Establish roles and responsibilities

Requirements / Tools

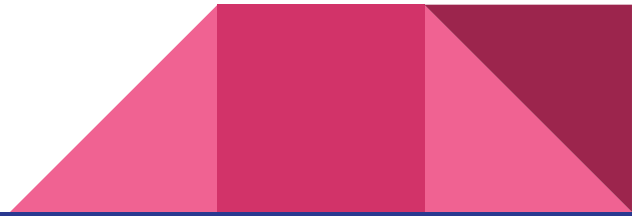
- Data Sources
- Attack Simulation Tools
- Dedicated Blue and Red team
- Time
- Tracking Process
- Threat Intelligence



Attack Range Local



“SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team. … SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.”

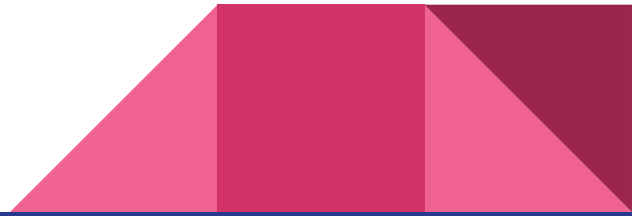


Benefits of Designing Playbooks

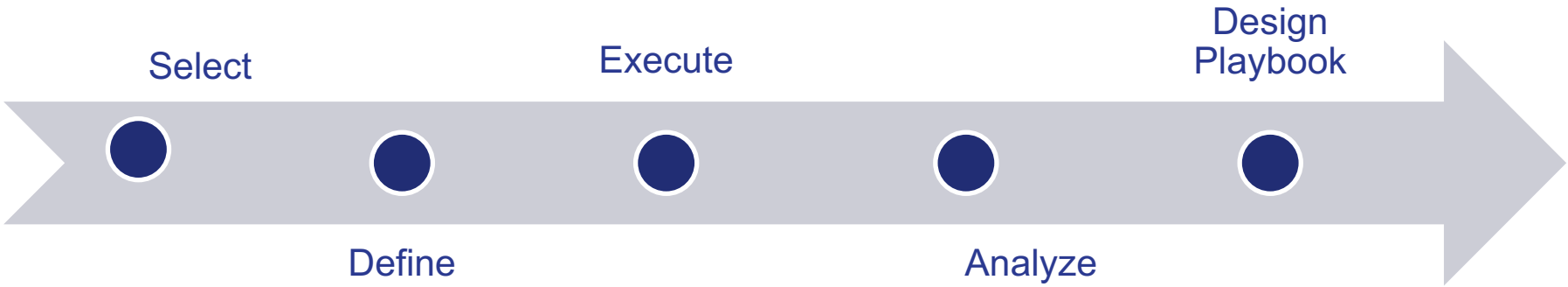
- Standardized workflow for analysts
- Automated repeatable actions
- Enriched incident response procedure

Key Points

- Threat Intelligence
- Testing
- Tracking
- Documentation
- Team

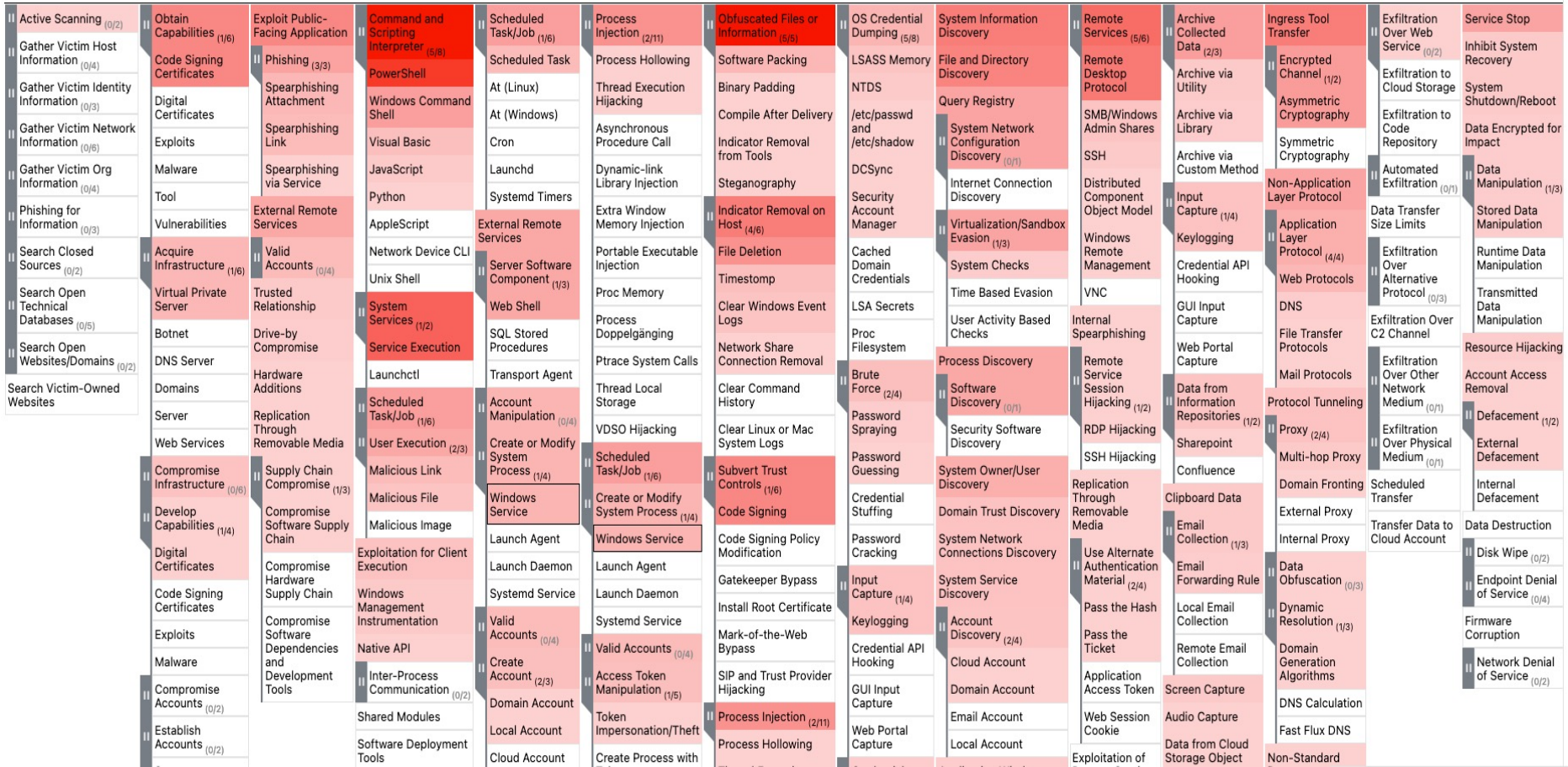


Timeline



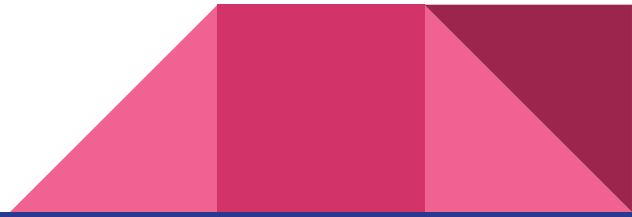
Attack - all x +

selection controls | layer controls | technique controls



Persistence,Privilege Escalation
T1543.003 **Create or Modify System Process: Windows Service**

Discovery
T1018 **Remote System Discovery**



ID: T1543.003

Sub-technique of: T1543

ⓘ Tactics: Persistence, Privilege Escalation

ⓘ Platforms: Windows

ⓘ Effective Permissions: Administrator, SYSTEM

ⓘ Data Sources: Command: Command Execution, Process: OS API Execution, Process: Process Creation, Service: Service Creation, Service: Service Modification, Windows Registry: Windows Registry Key Creation, Windows Registry: Windows Registry Key Modification

ⓘ CAPEC ID: CAPEC-478, CAPEC-550, CAPEC-551

Contributors: Matthew Demaske, Adaptforward; Pedro Harrison; Travis Smith, Tripwire

Version: 1.1

Created: 17 January 2020

Last Modified: 16 September 2020

ID: T1018

Sub-techniques: No sub-techniques

ⓘ Tactic: Discovery

ⓘ Platforms: Linux, Windows, macOS

ⓘ Permissions Required: Administrator, SYSTEM, User

ⓘ Data Sources: Command: Command Execution, File: File Access, Network Traffic: Network Connection Creation, Process: Process Creation

ⓘ CAPEC ID: CAPEC-292

Contributors: Daniel Stepanic, Elastic; RedHuntLabs, @redhuntlabs

Version: 3.1

Created: 31 May 2017

Last Modified: 13 April 2021

DEMO TIME

```
(venv) Semanur@STG attack_range_local % python attack_range_local.py -a simulate -st T1543.003 -t attack-range-win10

starting program loaded for B1 battle droid
          ||/__'`.
          |//()'-.:
          |-.||
          |o(o)
          |||\\  .==._
          |||(o)==::'
          `|T  ""
           ()
           |\
           ||\
           ()()
           ||//
           |//
          .'=`=.

attack_range is using config at path attack_range_local.conf
2021-05-18 12:33:20,953 - INFO - attack_range - INIT - attack_range v1

PLAY [all] *********************************************************************

TASK [atomic_red_team : Enable strong dotnet crypto] ***************************
ok: [10.0.1.17] => (item=HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319)
ok: [10.0.1.17] => (item=HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319)

TASK [atomic_red_team : Check installed providers] *****************************
ok: [10.0.1.17]

TASK [atomic_red_team : Install NuGet Provider] ********************************
skipping: [10.0.1.17]

TASK [atomic_red_team : Install Atomic Red Team] *******************************
changed: [10.0.1.17]

TASK [atomic_red_team : set_fact] **********************************************
ok: [10.0.1.17]

TASK [atomic_red_team : include_tasks] *****************************************
included: /Users/Semanur/Documents/GitHub/attack_range_local/ansible/roles/atomic_red_team/tasks/run_art_test.yml for 10.0.1.17

TASK [atomic_red_team : set_fact] **********************************************
ok: [10.0.1.17]

TASK [atomic_red_team : debug] *************************************************
ok: [10.0.1.17] => {
    "technique": "T1543.003"
}

TASK [atomic_red_team : Get requirements for Atomic Red Team Technique] ********
changed: [10.0.1.17]

TASK [atomic_red_team : Run specified Atomic Red Team Technique] ***************
changed: [10.0.1.17]
```

```
(venv) Semanur@STG attack_range_local % python attack_range_local.py -a simulate -st T1018 -t attack-range-win10

starting program loaded for B1 battle droid
          ||/__'`.
          |//()'-.:
          |-.||
          |o(o)
          |||\\  .==._
          |||(o)==::'
           `|T  ""
            ()
            |\
            ||\
            ()()
            ||//
            |//
           .'=`=.

attack_range is using config at path attack_range_local.conf
2021-05-18 13:12:36,187 - INFO - attack_range - INIT - attack_range v1

PLAY [all] ********************************************************************

TASK [atomic_red_team : Enable strong dotnet crypto] **************************
ok: [10.0.1.17] => (item=HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319)
ok: [10.0.1.17] => (item=HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319)

TASK [atomic_red_team : Check installed providers] ****************************
ok: [10.0.1.17]

TASK [atomic_red_team : Install NuGet Provider] *******************************
skipping: [10.0.1.17]

TASK [atomic_red_team : Install Atomic Red Team] ******************************
changed: [10.0.1.17]

TASK [atomic_red_team : set_fact] *********************************************
ok: [10.0.1.17]

TASK [atomic_red_team : include_tasks] ****************************************
included: /Users/Semanur/Documents/GitHub/attack_range_local/ansible/roles/atomic_red_team/tasks/run_art_test.yml for 10.0.1.17

TASK [atomic_red_team : set_fact] *********************************************
ok: [10.0.1.17]

TASK [atomic_red_team : debug] ************************************************
ok: [10.0.1.17] => {
    "technique": "T1018"
}

TASK [atomic_red_team : Get requirements for Atomic Red Team Technique] ********
changed: [10.0.1.17]

TASK [atomic_red_team : Run specified Atomic Red Team Technique] **************
changed: [10.0.1.17]
```

T1543.003

2-Service Installation CMD	win10	Windows Service Windows Service	https://attack.mitre.org/techniques/T1543/003 https://attack.mitre.org/techniques/T1543/003	TA0003 TA0004	T1543.003	Service Installation CMD	win10\vagrant
1-Modify Fax service to run PowerShell	win10	Windows Service Windows Service	https://attack.mitre.org/techniques/T1543/003 https://attack.mitre.org/techniques/T1543/003	TA0003 TA0004	T1543.003	Modify Fax service to run PowerShell	win10\vagrant

Executed simulations

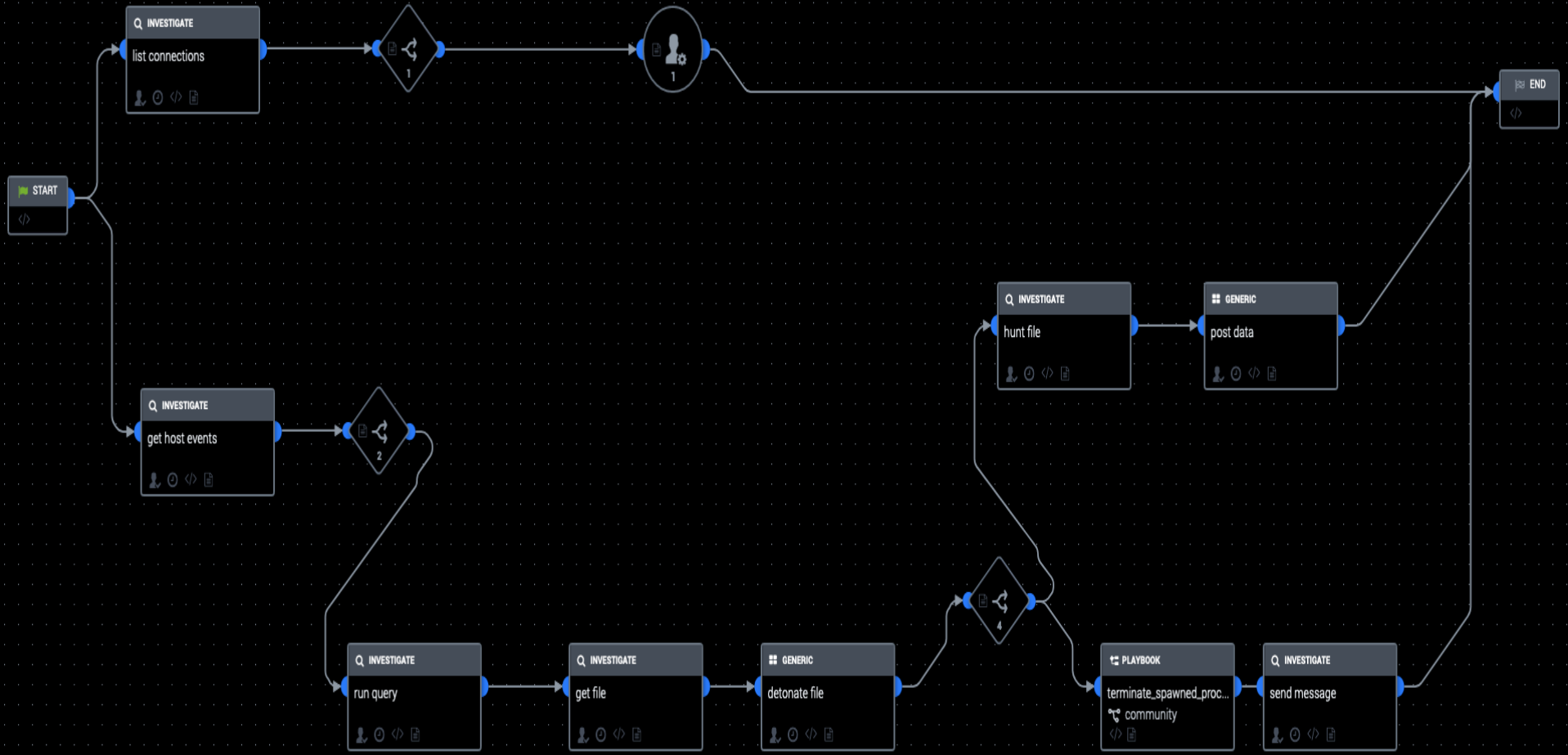
atomic_test	Hostname	mitre_id
1-Remote System Discovery - net	win10	T1018 - Remote System Discovery
3-Remote System Discovery - nltest	win10	T1018 - Remote System Discovery
2-Remote System Discovery - net group Domain Computers	win10	T1018 - Remote System Discovery
5-Remote System Discovery - arp	win10	T1018 - Remote System Discovery
4-Remote System Discovery - ping sweep	win10	T1018 - Remote System Discovery

T1543.003

Type	Field	Value	Actions
Selected	host	win-client-7637484	
	source	XmlWinEventLog:Security	
	sourcetype	XmlWinEventLog	
Event	Caller_Domain	WIN10	
	Caller_User_Name	vagrant	
	Channel	Security	
	CommandLine	sc config Fax binPath= "C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe -noexit -c \"write-host 'T1543.003 Test'\""	
	Computer	win10	

T1018

Type	Field	Value	Actions
Selected	host	win-client-7637484	
	source	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	
	sourcetype	xmlwineventlog	
Event	Channel	Microsoft-Windows-Sysmon/Operational	
	CommandLine	"C:\Windows\system32\cmd.exe" /c "nltest.exe /dclist:domain.local"	
	Company	Microsoft Corporation	
	Computer	win10	


INVESTIGATE
list connections
1
1
END
START
INVESTIGATE
hunt file
GENERIC
post data
INVESTIGATE
get host events
2
INVESTIGATE
run query
INVESTIGATE
get file
GENERIC
detonate file
4
PLAYBOOK
terminate_spawned_proc...
community
INVESTIGATE
send message

Resources

1. https://github.com/splunk/attack_range_local
2. https://github.com/rabobank-cdc/DeTTECT/tree/master/threat-actor-data/ATT%26CK-Navigator-layers/20210413-FireEye-Mandiant
3. https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

Q & A

semanurtg