

CONGRATULATIONS!

EXCLUSIVE SCENARIO INSTRUCTIONS INSIDE

YOU ARE A LEADER THAT IS MOVING
FROM REACTIVE TO PROACTIVE



You have received one of our scenarios.

Now what?

Attached to this document you find one or more of Venation's most recent scenarios that we believe provides you a good example of our scenario content.

In this document we illustrated the 3 most used usecases to demonstrate how this example provides value to your organization. Although specific applications are only limited by your imagination.



Research & Preparation



Education & Awareness



Control Testing & Validation

Scenario Breakdown

...

Objective(s):

The objective of this at

This scenario demonstrat

Summary:

Data from the 2021 Honeywell Industrial USB Threat Report indicates the volume

All malware frameworks relevant to this scenario devised unique ways to reach

Offline frameworks do not involve internet-connected systems at all. In these

Industry Tagging:

#Industry/Manufacturing
#Industry/Energy
#Industry/Government
#Industry/PublicSector
#Industry/FinancialServicesIndustry

Functions and/or systems targeted:

#Solution/System/Microsoft/Windows

Scenario walkthrough:

* **Initial Access (TA0001):** The attacker initially targets victims through

* **Weaponised USB Drive:** Once compromised, the attacker weaponises USB driv

* **Persistence (TA0003):** Once the malware is deployed through its execution

* **Defence Evasion (TA0005):** The attacker formats their USB specially to re

* **Reconnaissance and information stealing:** The payload running on the air-

* **Copy stolen information to USB:** The attacker transfers the output from t

* **Collection (TA0009):** The malware is designed to install and persist in n

* **Copy command results to USB:** The results and output of the commands are

* **Command and Control (TA0011):** The attacker sends commands to the malware

* **Exfiltration (TA0010):** When the USB drive reaches the compromised connec

* **FIN**

Considerations:

* In this scenario we did not no

Adversary playbook

...

**Associated threat actor profil

80%

ready to be customized to your environment

Example

Targeting air-gapped systems through compromised USB drives

<https://github.com/venation-digital/threatscenario>

If you would like to have a sneak peek into materials currently available in our repository, please visit:

<https://content.venation.digital>

Available via

Portal	Github	HTTP REST API/GraphQL

Using a scenario-based approach to Research & Preparation

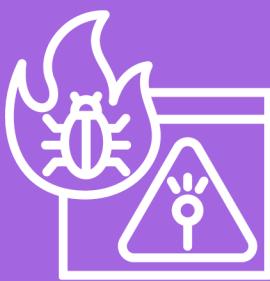


Time is your teams most precious currency.

Both our threat scenarios and academy items provide threat & risk professionals a curated and narrative based starting point. Research time gets reduced significantly, which in turn can be spent on tailoring to your environment.

Other functions that also require curated threat information from your cyber threat intelligence team, are the

Incident Response & Risk Management functions.



Incident Response

Use our templates to get started on IR playbooks & create your process. Integrate with our scenarios to become threat-informed & up to date with threat landscape.



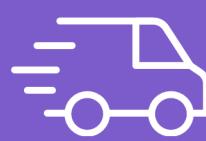
Risk Assessment

Leverage our scenarios to determine what is a threat and what is a risk. Reducing the time to develop questions & control suggestions.



Measurable Value

- Average Turnaround Time of Intelligence deliverable
- Number of Threat Intelligence products contributing to actionable insights
- MTBF, MTTR, MTTF, MTTA



Improve Maturity

- Threat Intelligence Operations
- Program Planning & Requirements

Using a scenario-based approach to Education & Awareness



Sometimes we don't need that much detail. Sometimes you need a quick answer or a nice visual that supports the story your team is telling about threat & risk.

Our content can easily be adjusted to your internal branding, supporting education of your stakeholders or other awareness activities.

Example usecases



Brief your executive stakeholder on 'that thing we read in the Wall Street Journal about Satellite hacking'



Create a simple infographic with 2-row summaries based on a scenario



Trending 'threat' needs a visualization within 48 hours to include in upcoming awareness campaign

COMPANY SECURITY TIPS

- 01 USE STRONG AND UNIQUE PASSWORDS**
Creating strong and unique passwords for each of your online accounts is essential for protecting your information.
- 02 ENABLE TWO-FACTOR AUTHENTICATION**
Two-factor authentication adds an extra layer of security to your online accounts by requiring an additional verification step.
- 03 KEEP YOUR SOFTWARE UP TO DATE**
Keeping software up to date on your corporate laptop is important for maintaining the security of your devices.
- 04 BE CAUTIOUS OF USB DRIVES**
USB drives are used to trick you into plugging them into your device to obtain sensitive information, such as login credentials.
- 05 LIMITING INFORMATION SHARING**
Be mindful of the information you share online, and avoid posting sensitive personal or financial information on social media or other public platforms.

Example

Targeting air-gapped systems through compromised USB drives

Don't want to do this yourself?

We support your team using an Analyst On Demand model.



Measurable Value

- Total Number of curated Intelligence deliverables
- Average Turnaround Time of Intelligence deliverable



Improve Maturity

- Program Planning & Requirements
- Stakeholder engagement

Using a scenario-based approach to Control Testing & Validation



We have significant experience in cyber threat intelligence program build and run. Starting these activities includes performing a threat assessment, where we establish an organization's threat model to identify subsequent controls and understand what needs to be validated against the current threat landscape to determine risk.

Our focus is on building measurable threat-informed defenses, continuously validating your defenses against current and emerging threats. Reporting on this through effective dashboarding.

Tabletop Exercise

We leverage a five week process from signup, to delivery & action plan. Specifically focused on leadership teams. Our templates and scenarios are available to provide stakeholders a realistic experience.

Threat Based Red Teaming

Simplify hypothesis generation & execution for where to start testing. Develop threat landscape based scenarios that test controls using Red teaming or Penetration Testing efforts.

Emulation Packs

Customized scenarios specifically geared towards emulating a given scenario; including a number of procedural level actions. Integrating with your existing tooling.

Our objective is to demonstrate empirical value of the threat & risk function to the overall organization



Measurable Value

- Number of TTPs emulated, not detected by SOC.
- Number of ad-hoc PIRs requested following testing & validation



Improve Maturity

- Program Planning & Requirements
- Governance
- Compliance integrations (e.g. NIS2.0)



About Venation

What happens if you bring together a community of cybersecurity, digital risk, and cyber (threat) intelligence practitioners with the singular focus of building content so you don't have to? Well, that's what Venation is all about.

Venation's team members are experts in cybersecurity, threat intelligence, and risk management frameworks. But beyond technical skills, what sets us apart is our passion and drive. We value traits like optimism, grit, and a growth mindset, ensuring we see every challenge as an opportunity. Whether we're solving problems for Fortune 500 companies or helping small businesses, our global team excels at breaking down complex issues into clear, actionable insights.

Founded in 2021, we run a virtual first company using a distributed team in all continents and time-zones. Diversity is no KPI for us, it's essential to our successful delivery. We are headquartered in Eindhoven, Netherlands, and support clients across the globe.

Your contact

Gert-Jan Bruggink

Founder & CEO

+316-53 59 84 55

gertjanbruggink@Venation.digital

Venation

Eindhoven

Netherlands

Chamber of commerce number: 76555364