TNO innovation for life

STAM: SECURITY TOOL ASSESSMENT METHOD

DR. IR. R.M. SEEPERS

WAAROM SECURITY TECHNOLOGIE EVALUEREN?

Markt voor cybersecurity producten groeit explosief

- Functionaliteit?
- Vergelijkbaar?
- Effectiviteit?
- Volwassenheid?
- Wat heb ik eigenlijk nodig?

STAM: Ontwikkeld sinds 2016 in opdracht van het NBV (Nationaal Bureau voor de Verbindingsbeveiliging)

2019-2020: Beschikbaar stellen voor breder publiek ("de markt")

TNO innovation for life

Zicht op de echte waarde van security producten

STAM

Zicht op de echte waarde van security producten

STAM

STAM: SECURITY TOOL ASSESSMENT METHOD

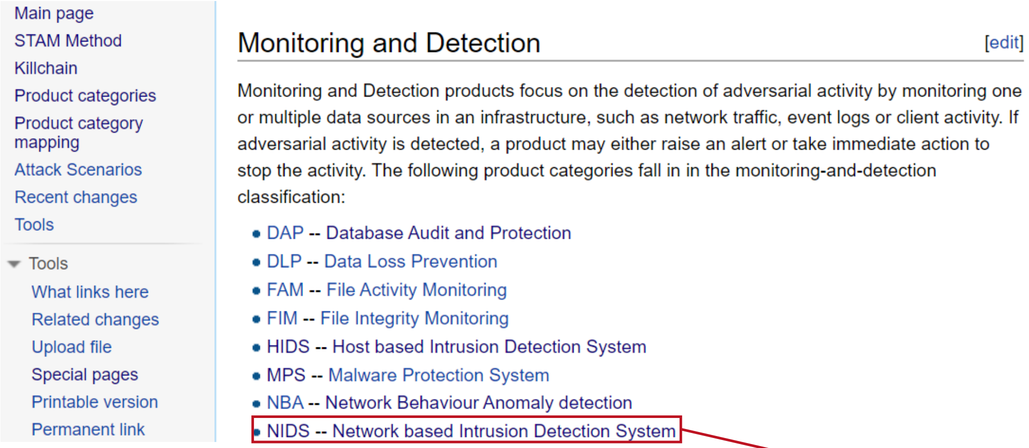
WAT IS STAM?

- STAM is een methode voor het efficiënt beoordelen van security producten
  - Zicht op de werkelijke waarde van cybersecurity technologie
  - Huidige versie met name gericht op monitoring & detectieproducten

- STAM framework
  - Structureren van securityoplossingen en –technologie
  - Structureren van securitybehoeften

  - Versie 2 incorporeert het MITRE ATT&CK framework

STAM FRAMEWORK - STRUCTUREREN VAN SECURITY OPLOSSINGEN EN –TECHNOLOGIE

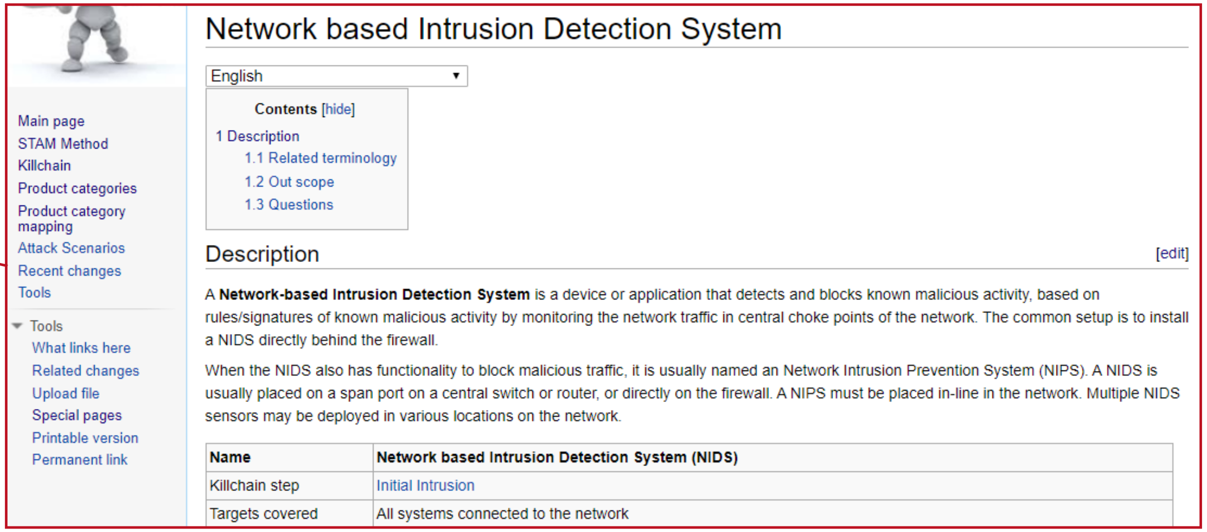


Monitoring and Detection

[edit]

Monitoring and Detection products focus on the detection of adversarial activity by monitoring one or multiple data sources in an infrastructure, such as network traffic, event logs or client activity. If adversarial activity is detected, a product may either raise an alert or take immediate action to stop the activity. The following product categories fall in in the monitoring-and-detection classification:

- DAP -- Database Audit and Protection
- DLP -- Data Loss Prevention
- FAM -- File Activity Monitoring
- FIM -- File Integrity Monitoring
- HIDS -- Host based Intrusion Detection System
- MPS -- Malware Protection System
- NBA -- Network Behaviour Anomaly detection
- NIDS -- Network based Intrusion Detection System



Network based Intrusion Detection System

Contents [hide]
1 Description
1.1 Related terminology
1.2 Out scope
1.3 Questions

Description

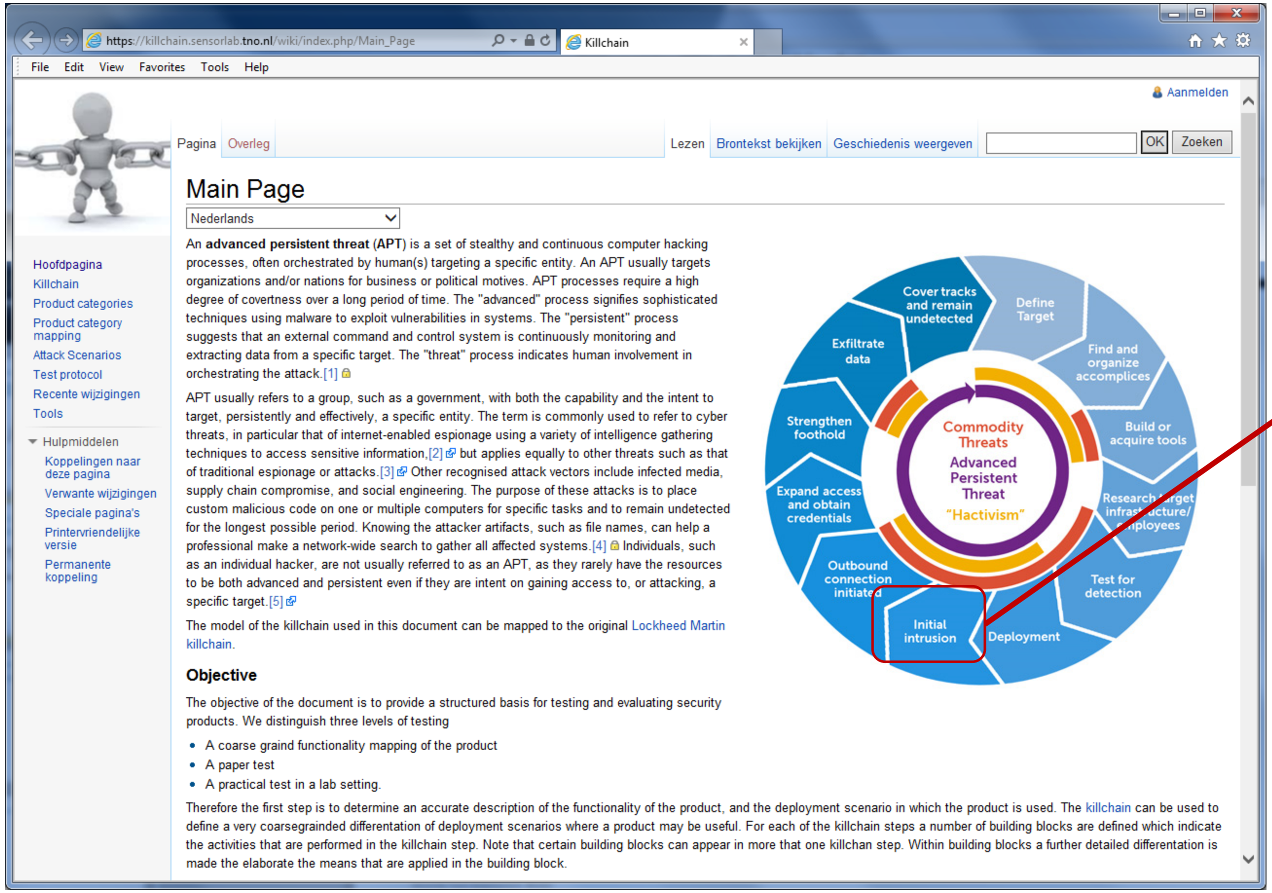
[edit]

A **Network-based Intrusion Detection System** is a device or application that detects and blocks known malicious activity, based on rules/signatures of known malicious activity by monitoring the network traffic in central choke points of the network. The common setup is to install a NIDS directly behind the firewall.

When the NIDS also has functionality to block malicious traffic, it is usually named an Network Intrusion Prevention System (NIPS). A NIDS is usually placed on a span port on a central switch or router, or directly on the firewall. A NIPS must be placed in-line in the network. Multiple NIDS sensors may be deployed in various locations on the network.

Name	**Network based Intrusion Detection System (NIDS)**
Killchain step	Initial Intrusion
Targets covered	All systems connected to the network

STAM FRAMEWORK - STRUCTUREREN VAN SECURITYBEHOEFTEN



Main Page

An **advanced persistent threat** (**APT**) is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. An APT usually targets organizations and/or nations for business or political motives. APT processes require a high degree of covertness over a long period of time. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack.[1]

APT usually refers to a group, such as a government, with both the capability and the intent to target, persistently and effectively, a specific entity. The term is commonly used to refer to cyber threats, in particular that of internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information,[2] but applies equally to other threats such as that of traditional espionage or attacks.[3] Other recognised attack vectors include infected media, supply chain compromise, and social engineering. The purpose of these attacks is to place custom malicious code on one or multiple computers for specific tasks and to remain undetected for the longest possible period. Knowing the attacker artifacts, such as file names, can help a professional make a network-wide search to gather all affected systems.[4] Individuals, such as an individual hacker, are not usually referred to as an APT, as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.[5]

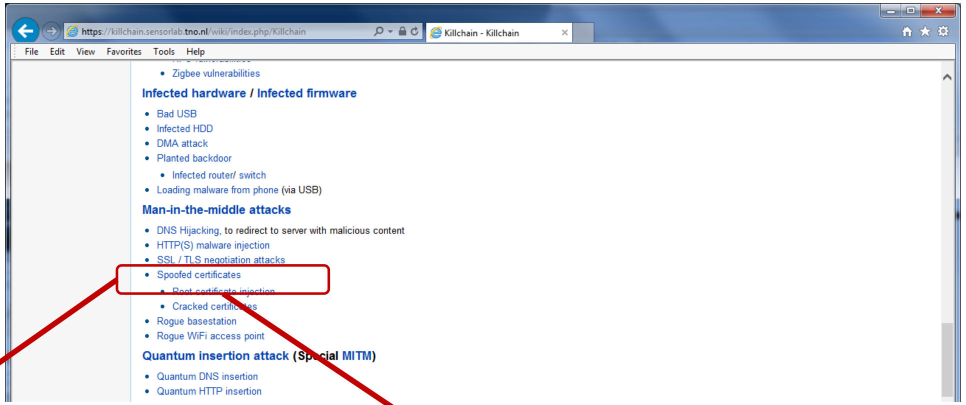
The model of the killchain used in this document can be mapped to the original Lockheed Martin killchain.

Objective

The objective of the document is to provide a structured basis for testing and evaluating security products. We distinguish three levels of testing

- A coarse graind functionality mapping of the product
- A paper test
- A practical test in a lab setting.

Therefore the first step is to determine an accurate description of the functionality of the product, and the deployment scenario in which the product is used. The killchain can be used to define a very coarsegrainded differentation of deployment scenarios where a product may be useful. For each of the killchain steps a number of building blocks are defined which indicate the activities that are performed in the killchain step. Note that certain building blocks can appear in more that one killchan step. Within building blocks a further detailed differentiation is made the elaborate the means that are applied in the building block.



- Zigbee vulnerabilities

Infected hardware / Infected firmware

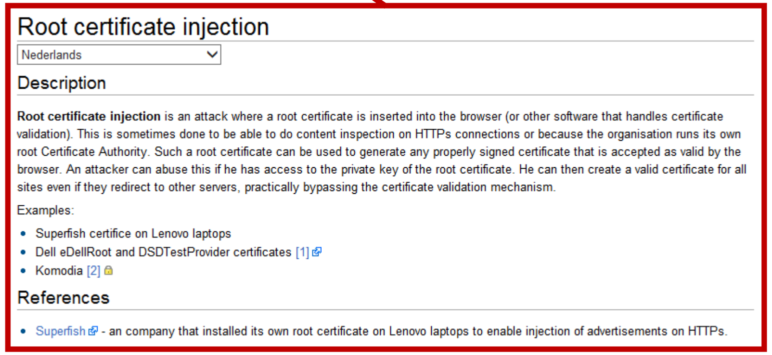
- Bad USB
- Infected HDD
- DMA attack
- Planted backdoor
  - Infected router/ switch
- Loading malware from phone (via USB)

Man-in-the-middle attacks

- DNS Hijacking, to redirect to server with malicious content
- HTTP(S) malware injection
- SSL / TLS negotiation attacks
- Spoofed certificates
  - Root certificate injection
  - Cracked certificates
- Rogue basestation
- Rogue WiFi access point

Quantum insertion attack (Special MITM)

- Quantum DNS insertion
- Quantum HTTP insertion



Root certificate injection

Nederlands

Description

Root certificate injection is an attack where a root certificate is inserted into the browser (or other software that handles certificate validation). This is sometimes done to be able to do content inspection on HTTPs connections or because the organisation runs its own root Certificate Authority. Such a root certificate can be used to generate any properly signed certificate that is accepted as valid by the browser. An attacker can abuse this if he has access to the private key of the root certificate. He can then create a valid certificate for all sites even if they redirect to other servers, practically bypassing the certificate validation mechanism.

Examples:

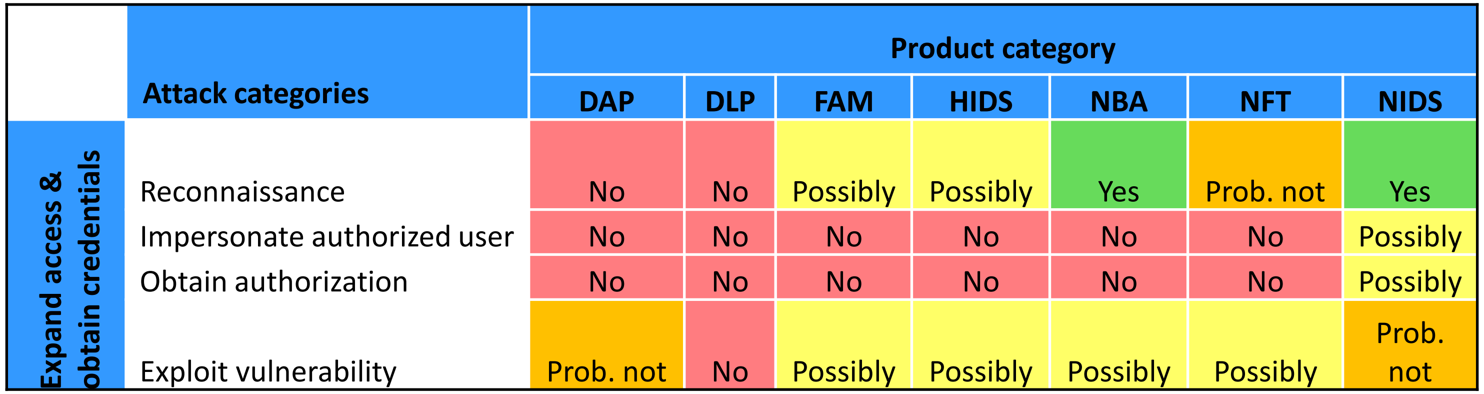
- Superfish certifice on Lenovo laptops
- Dell eDellRoot and DSDTestProvider certificates [1]
- Komodia [2]

References

- Superfish - an company that installed its own root certificate on Lenovo laptops to enable injection of advertisements on HTTPs.

STAM FRAMEWORK

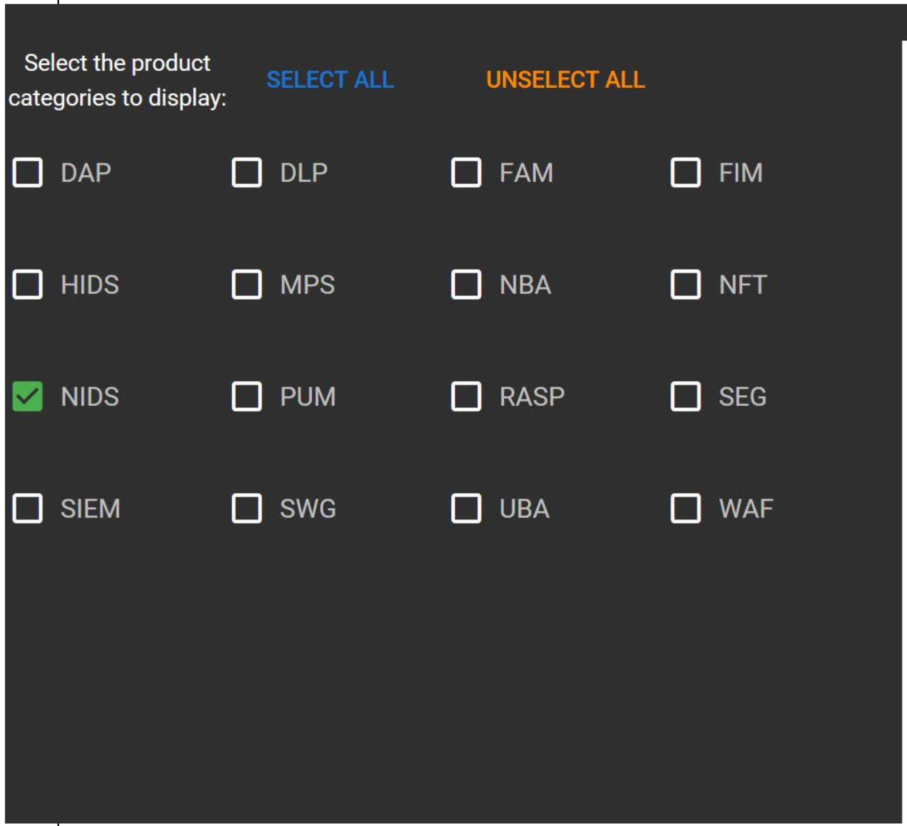
- Mapping om te identificeren welke aanvalscategorieën relevant zijn voor een productcategorie.
  - (51) aanvalscategorieën op (14) productcategorieën (monitoring & detection)



	Attack categories	Product category						
		DAP	DLP	FAM	HIDS	NBA	NFT	NIDS
Expand access & obtain credentials	Reconnaissance	No	No	Possibly	Possibly	Yes	Prob. not	Yes
	Impersonate authorized user	No	No	No	No	No	No	Possibly
	Obtain authorization	No	No	No	No	No	No	Possibly
	Exploit vulnerability	Prob. not	No	Possibly	Possibly	Possibly	Possibly	Prob. not

Uittreksel van STAM mapping

STAM RAAMWERK V2 (OVERZICHT)



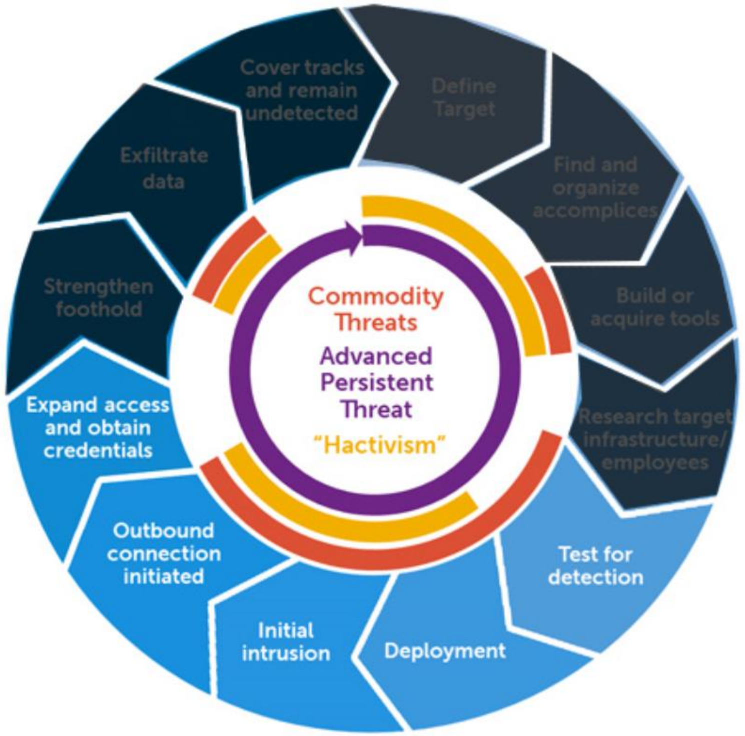
Select the product categories to display: SELECT ALL UNSELECT ALL

☐ DAP ☐ DLP ☐ FAM ☐ FIM

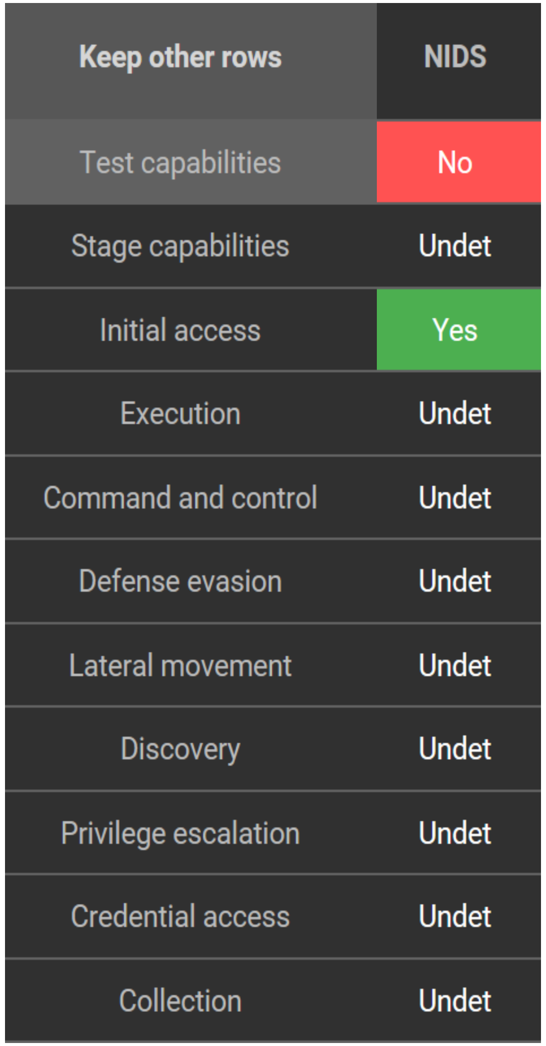
☐ HIDS ☐ MPS ☐ NBA ☐ NFT

☑ NIDS ☐ PUM ☐ RASP ☐ SEG

☐ SIEM ☐ SWG ☐ UBA ☐ WAF


Cover tracks and remain undetected
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Commodity Threats
Advanced Persistent Threat
"Hactivism"

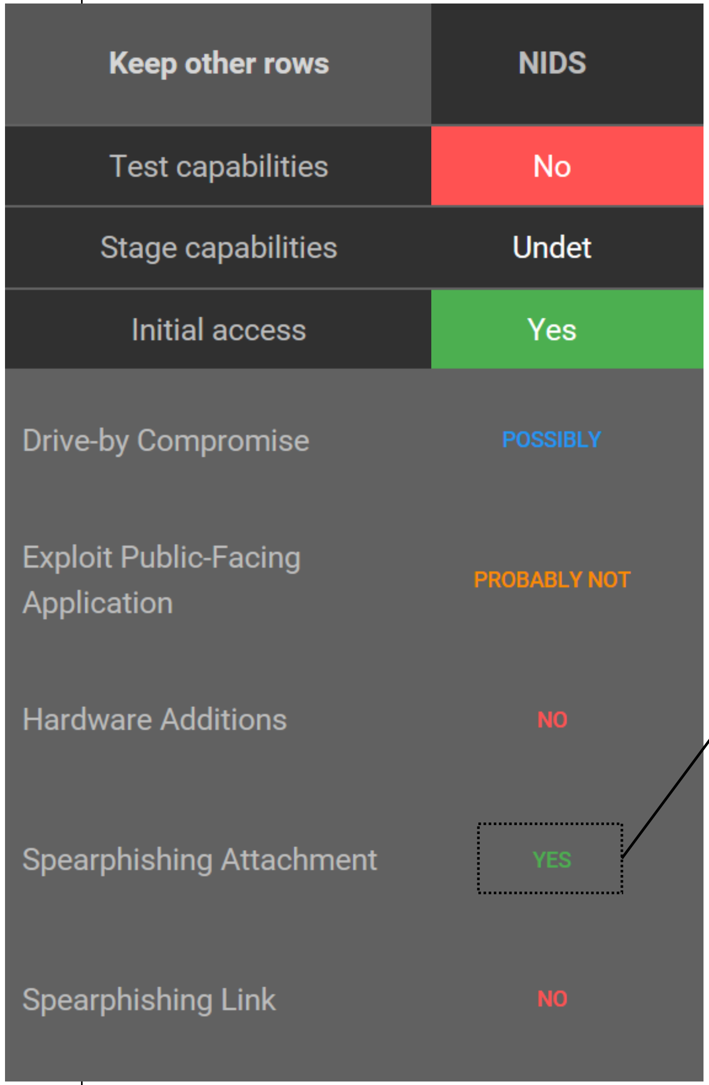
integratie ATT&CK



Keep other rows	NIDS
Test capabilities	No
Stage capabilities	Undet
Initial access	Yes
Execution	Undet
Command and control	Undet
Defense evasion	Undet
Lateral movement	Undet
Discovery	Undet
Privilege escalation	Undet
Credential access	Undet
Collection	Undet

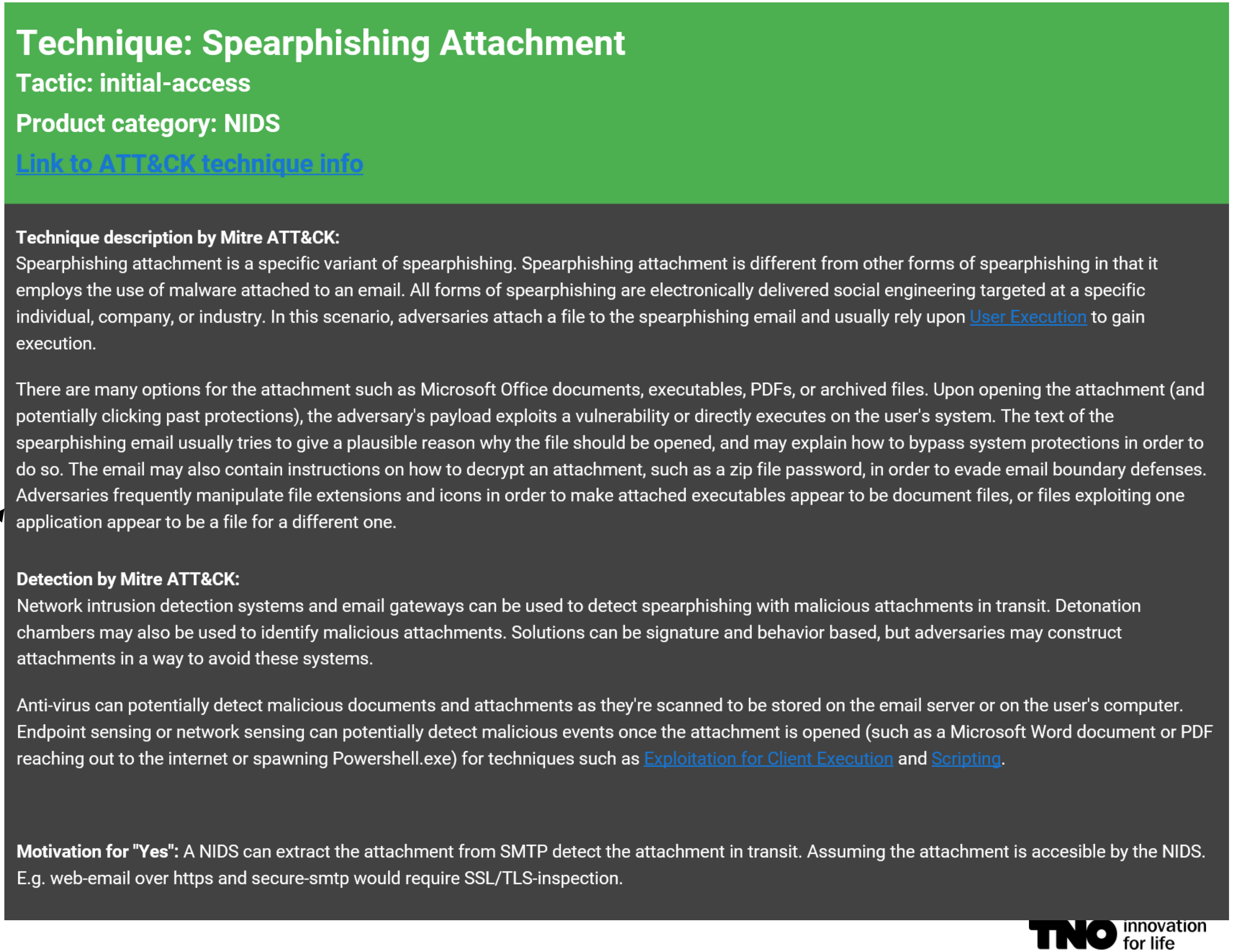
TNO innovation for life

STAM RAAMWERK V2 (OVERZICHT 2)



Keep other rows	NIDS
Test capabilities	No
Stage capabilities	Undet
Initial access	Yes
Drive-by Compromise	POSSIBLY
Exploit Public-Facing Application	PROBABLY NOT
Hardware Additions	NO
Spearphishing Attachment	YES
Spearphishing Link	NO

click



Technique: Spearphishing Attachment

Tactic: initial-access

Product category: NIDS

Link to ATT&CK technique info

Technique description by Mitre ATT&CK:
Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

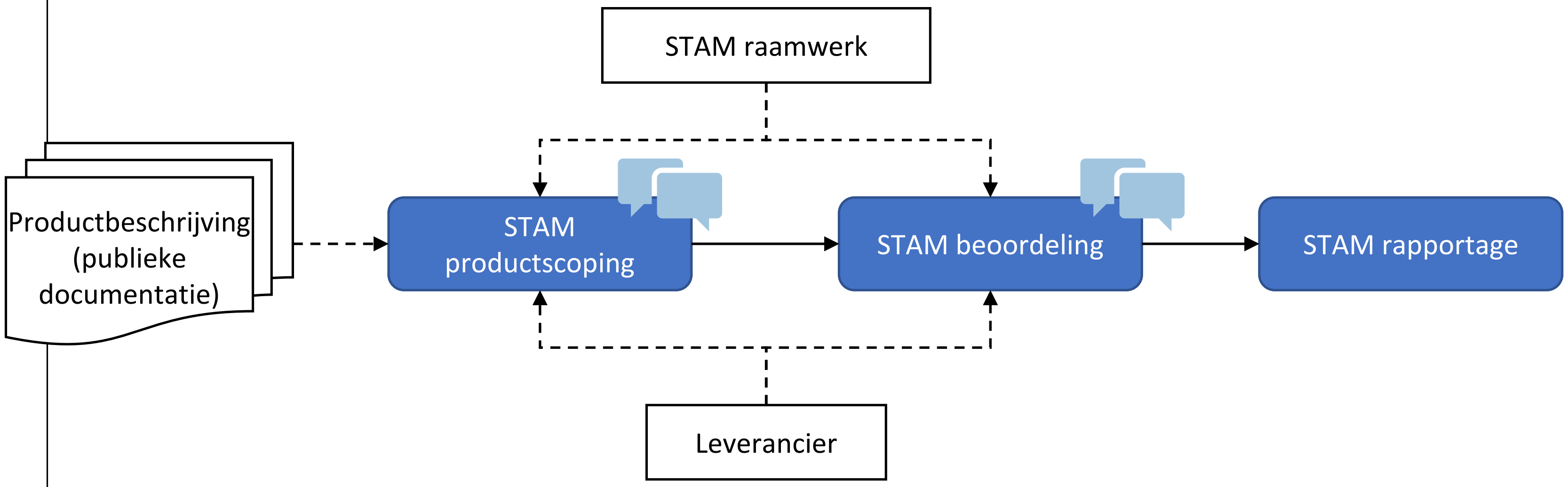
Detection by Mitre ATT&CK:
Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. Detonation chambers may also be used to identify malicious attachments. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Anti-virus can potentially detect malicious documents and attachments as they're scanned to be stored on the email server or on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the attachment is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning Powershell.exe) for techniques such as Exploitation for Client Execution and Scripting.

Motivation for "Yes": A NIDS can extract the attachment from SMTP detect the attachment in transit. Assuming the attachment is accesible by the NIDS. E.g. web-email over https and secure-smtp would require SSL/TLS-inspection.

STAM BEOORDELINGEN

- STAM beoordelingen zijn kwalitatief op basis van desk-studie en leveranciersinterviews
  - Snel, efficiënt (enkele dagen), het security-kaf van het -koren scheiden
  - Enige manier om moderne oplossingen generiek te beoordelen (UEBA, NBA, …)
- 5 succesvolle assessments tot dusver

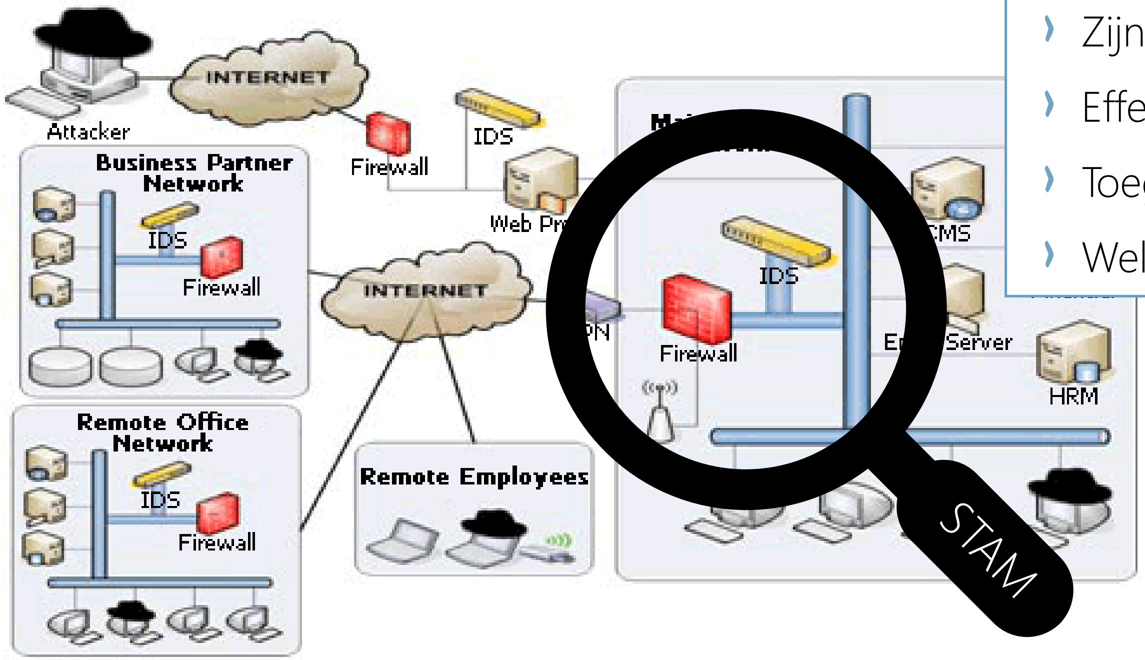


Zicht op de echte waarde van security producten

BEOORDELEN BEVEILIGINGSARCHITECTUUR

- Doorlichten van beveiligingsarchitectuur met STAM om
  - Blinde vlekken te identificeren
  - Effectiviteit oplossing te bepalen

- Worden aanvalsvectoren voldoende afgedekt?
- Zijn alle assets voldoende beschermd?
- Effectiviteit van IDS?
- Toegevoegde waarde introductie UEBA product?
- Welk product is voor mij het meest doeltreffend?



TOT SLOT

- “STAM organisatie” nu in de maak
  - Betrekken assessoren, coördinatie, etc.

- Toekomst: Veel kansen voor toepassing en doorontwikkeling STAM
  - STAM voor OT
  - Overige types securityproducten
  - Uitbreiden beoordelingsmethode beveiligingsarchitectuur

Interesse? Ideeën? Meedenken?

Laat het graag weten!

En tot zo op de stand ☺

Zicht op de echte waarde van security producten

BEDANKT VOOR UW AANDACHT

TNO innovation for life