Sharing and Automation for
Privacy Preserving Attack Neutralization

(H2020 833418)

D2.1.1 High-impact use case analysis (M3)

Published by the SAPPAN Consortium

Dissemination Level: Public

H2020-SU-ICT-2018-2020 – Cybersecurity

Document control page

Document file: D2.1.1 High-impact use case analysis
Document version: 0.3
Document owner: Josef Niedermeier (HPE)

Work package: WP2
Task: T2.1 Analysis and specification of response and recovery use-cases
Deliverable type: Report
Delivery month: M3
Document status: ☒ approved by the document owner for internal review
☒ approved for submission to the EC

Document History:

Version	Author(s)	Date	Summary of changes made
0.1	Josef Niedermeier (HPE)	2019-07-25	Preliminary draft sent out to partners for approval to publish as public document.
0.2	Josef Niedermeier (HPE)	2019-08-01	Modified version that factors HPE requirements for changes and feedback and corrections from partners integrated into the deliverable.
0.3	Josef Niedermeier (HPE)	2019-08-02	Final correction based on reviews

Internal review history:

Reviewed by	Date	Summary of comments
Jacek Jonczy	2019-07-30	grammar
Christoph Müller	2019-07-30	grammar
Alexey Kirichenko	2019-08-01	formating, comprehensibility and grammar
Christoph Müller	2019-08-02	formal issues,grammar and orthography

Executive Summary

The main goal of this document is to collect requirements from cybersecurity response and recovery domain experts that are relevant for the SAPPAN project. We collected formally structured use cases and analyzed the data and tools used. We also interviewed domain experts about tooling, data requirements and gaps between the optimal and current situation and recorded the findings. We organized a visit to the HPE Cyber Defense Center for the project partners from academia to help understanding how a big company security operation center works.

The main output of this document is a set of use cases that can be used to demonstrate the promised functionality of the SAPPAN platform. The selected use cases are based on collected requirements and address currently trending threats.

Some parts of the collected use cases are confidential. Consequently, these parts are left out in this document. Almost fifty use cases have been collected, but only summarized and sanitized ones are presented it this document. Similarly, the gap analyses contain sensitive information, which could be used by attackers. Therefore, only the extracted requirements are presented.

Table of Contents

1 Use case gathering

In this section, we describe the underlying processes that led to the identification of the SAPPAN use cases relevant for the objectives and areas of application described in the SAPPAN project proposal. Common attributes that are linked to all objectives are cyber threat detection and response to a cyber threat. Hence, the SAPPAN use cases should reflect the current and emerging threat landscape and state-of-the-art approaches to threat modeling and response. At the same time, the SAPPAN use cases should address the state-of-the-art both in the academic research and in practical, real-world environments. Stating this, we divide our use case requirements gathering methodology into two separate, yet highly interconnected, tasks:

- **Threat landscape exploration –** this task includes the exploration of existing data sources to capture relevant trends in the threat landscape, thus identifying the most relevant threats. We believe that a SAPPAN framework built based on use cases reflecting the trending threats will maximize the impact and added value for the intended users of the SAPPAN framework.
- **Collection of high – impact use cases from real-world cyber defense centers –** this task includes personal discussion with potential future users of SAPPAN as well as the collection of their use cases reflecting real-world operations praxis. It helps making sure that the use cases selected for testing the SAPPAN framework are representative for real-world security operations.

1.1 Threat landscape exploration

1.1.1 ENISA Threat Landscape Report 2018

The ENISA Threat Landscape Report by the European Union Agency for Cybersecurity (ENISA) provides an overview of threats including current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends. The specific threat report of 2018 provides a comprehensive compilation of top 15 cyber threats encountered within the time period from December 2017 to December 2018. The 15 top cyber threats reviewed in the report result from the analysis of information collected throughout the aforementioned reporting period. The information collected – mainly from publicly available sources (Open source intelligence, OSINT) and some from commercial providers – covers the majority of the most remarkable events and developments relevant to the study of the top cyber threats. The top 15 cyber threats include malware, web-based attacks – including web application attacks –, phishing, DoS attacks, spam, botnets, data breaches, insider threat, physical manipulation threats, information leakage, identity theft, cryptojacking, ransomware, and cyber espionage. The threat report also provides an overview and comparison of the current threat landscape with the landscape of the previous year (see Fig. 1).

Source: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

Fig. 1 - Overview and comparison of the current threat landscape 2018 with the one of 2017

The most important findings from the report summary are the following:

(1) Skill and capability building are the main focus of defenders. Public organizations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.

(2) Among the many interesting developments in 2018, ransomware and crypto currency attacks have dominated the threat landscape. A further remarkable development is the massive increase in the number of phishing/spear-phishing attacks: it has now covered the gaps created by lawful takedowns of malicious infrastructure components such as botnets and exploit kits, while the role of the latter has been significantly reduced.

(3) Mail and phishing messages have become the primary malware infection vector. Phishing, including malicious e-mail attachments, is the de-facto delivery method for APT groups.

(4) Cyber threat intelligence needs to respond to increasingly automated attacks through novel approaches to utilization of automated tools and skills.

1.1.2 Internet Security Threat Report

The annual Symantec Internet Security Threat Report provides enterprises, small businesses, and consumers with essential information to help secure their systems effectively now and in the future. Symantec builds the report on the data collected from their protection sensors, such as Messaging Gateway, Email Seucrity.cloud, Advanced Threat Protection for Email or Probe Network installed in over 300,000 businesses and organizations worldwide.

The key points from the report from the Internet Security Threat Report Vol. 24 February 2019 are as follows:

(1) Cryptojacking, peaking in December 2017, did fall by 52 % in the course of 2018. Despite the downward trend, more than 3.5 million cryptojacking events were blocked in December 2019. The cryptojacking activity is highly dependent on the price of the cryptocurrencies. The downward trend in cryptojacking contrasts with the upward trend of the formjacking used to steal payment card data.

(2) For the first time since 2013, Symantec observed a decrease in ransomware activity during 2018, with the overall number of ransomware infections on end-points dropping by 20 %. However, within this decrease, one dramatic change comes. Up until 2017, consumers were the hardest hit by ransomware, accounting for the majority of infections. In 2017, the balance tipped towards enterprises. In 2018, that shift accelerated and enterprises accounted for 81 % of all ransomware infections. While overall ransomware infections were down, enterprise infections were up by 12 % in 2018.

(3) Employees of smaller organizations were more likely to be hit by e-mail threats – including spam, phishing, and e-mail malware – than those in large organizations. The report also found that spam levels continued to increase in 2018, with 55 percent of e-mails received in 2018 being categorized as spam. Meanwhile, the e-mail malware rate remained stable, while phishing levels declined, dropping from one in 2,995 e-mails in 2017, to one in 3,207 e-mails in 2018. The phishing rate has declined every year for the last four years. Nevertheless, spear-phishing e-mails remained the most popular avenue for attack and were used by 65 % of all known groups.

1.1.3 McAfee Labs Threats Report

The McAfee Labs Threats Report highlights the notable investigative research and trends in threats statistics and observations gathered by the McAfee Advanced Threat Research and McAfee Labs teams. McAfee is collaborating closely with MITRE Corporation in extending the techniques of its MITRE ATT&CK knowledge base. The MITRE ATT&CK model is projected into the report. Fig. 2 from the report represents techniques used in targeted attacks. The darker the background, the more frequently the method was used.

Source: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-By Compromise	CMSTP	Component Object Model Hijacking	Bypass User Account Control	Bypass User Account Control	Brute Force	Account Discovery	Exploitation of Remote Services	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Create Account	DLL Search Order Hijacking	CMSTP	Credential Dumping	File and Directory Discovery	Logon Scripts	Automated Collection	Data Compressed	Connection Proxy
Replication Through Removable Media	Execution through API	DLL Search Order Hijacking	Exploitation for Privilege Escalation	Code Signing	Credentials in Files	Network Service Scanning	Remote Desktop Protocol	Data from Information Repositories	Data Encrypted	Custom Command and Control Protocol
Spearphishing Attachment	Exploitation for Client Execution	Hidden Files and Directories	Hooking	Component Object Model Hijacking	Hooking	Network Share Discovery	Third-Party Software	Data from Local System	Exfiltration Over Alternative Protocol	Data Encoding
Spearphishing Link	Graphical User Interface	Hooking	New Service	Deobfuscate/ Decode Files or Information	Input Capture	Peripheral Device Discovery	Windows Admin Shares	Data Staged	Exfiltration Over Command and Control Channel	Data Obfuscation
Supply Chain Compromise	LSASS Driver		Process Injection	DLL Search Order Hijacking	Input Prompt	Process Discovery		Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Trusted Relationship	PowerShell	LSASS Driver	Scheduled Task	Exploitation for Defense Evasion		Query Registry		Input Capture		Multiband Communication
	Regsvr32	Modify Existing Service		File Deletion		Security Software Discovery		Man in the Browser		Multilayer Encryption
	Rundll32	New Service		Hidden Files and Directories		System Information Discovery		Screen Capture		Remote Access Tools
	Scheduled Task	Registry Run Keys/ Startup Folder		Indicator Removal from Tools		System Network Configuration Discovery		Video Capture		Remote File Copy
	Scripting	Scheduled Task		Masquerading		System Owner/User Discovery				Standard Application Layer Protocol
	Service Execution	System Firmware		Modify Registry		System Service Discovery				Standard Cryptographic Protocol
	Third-Party Software			Obfuscated Files or Information		System Time Discovery				
	User Execution			Process Doppelgänging						
	Windows Management Instrumentation			Process Injection						
				Regsvr32						
				Rootkit						
				Rundll32						
				Scripting						
				Software Packing						
				Trusted Developer Utilities						
				Valid Accounts						

Fig. 2 - MITRE ATT&CKTM framework. The darker the background, the more frequently the technique was used.

1.1.4 Cisco Threat Report February 2019

In this report, the cybersecurity specialists from Cisco picked out five key stories that represent treats likely to appear again in the same or a similar way. The five selected stories cover Emotet, VPNFilter, misuse of Mobile Device Management, cryptomining, and Olympic Destroyer. Each story is accompanied by a description of the threat and its consequences narrated to highlight a specific takeaway message. The relevant takeaway messages from our point of view are:

(1) E-mail is the most common threat vector. It remains the most popular infection vector for threat actors to spread their wares, and it will likely remain that way in the near future.

(2) IoT as part of the network will only grow. VPNFilter shows what can happen if security operators do not take proper steps to secure these devices in the future. Unfortunately, while VPNFilter may be a threat of the past, vulnerabilities continue to be discovered in IoT devices. It is all but inevitable that another threat targeting IoT will appear in the future.

(3) By and large, botnets and RATs dominate the security incidents. Included in this category are threats such as Andromeda and Xtrat.

(4) Ransomware has been usurped from its throne, largely by malicious crypto mining. That is not to say ransomware is gone; Cisco saw a few of such threats crop up in 2018. GandCrab continued to make its presence known, and Ryuk was spread via Emotet and Trickbot infections. So while ransomware is no longer king of the hill, it still remains, requiring vigilance to avoid outbreaks.

1.1.5 MITRE ATT&CK

According to the description on its official website, "MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community."

The knowledge base represents a comprehensive and organized collection of adversaries tactics and techniques. The techniques and tactics are accompanied by a summary of the groups that use them and software related to them. Thanks to its organized approach using the attack matrix and its completeness of covering all different steps and techniques used by adversaries, it has been widely adopted by the community as a taxonomy to refer to cyber incidents. The MITRE ATT&CK matrix for enterprises can be found at https://attack.mitre.org/matrices/enterprise/.

Source: https://attack.mitre.org/

1.2 High-impact use cases collection

To support the adoption of the SAPPAN framework by the addressed stakeholders, we collected the information relevant for the definition of use cases also from the SAPPAN consortium members. Since the SAPPAN consortium comprises of different types of organizations operating differently focused cyber defense teams, the information collected from the SAPPAN consortium members enables us to reflect the current needs in various cyber environments. The following paragraph presents a brief overview of the partner cybersecurity operations.

1.2.1 Partner cyber operations overview

Masaryk University

The certified cybersecurity team of Masaryk University (CSIRT-MU) has nine years of experience in incident handling and deals with thousands of incidents a year. It conducts a multitude of research activities focused on large-scale dataset analysis, primarily network traffic and application logs. CSIRT-MU also serves as an example of an organization dealing with ever-changing network topologies where most of the company-wide approaches to cybersecurity are not possible to implement, e.g. per-host profiling, a central application registry or centralized identity management.

CESNET

CESNET-CERT is dealing with a high number of alerts that are related to its connected organizations, the large network infrastructure and its services (constituency). In most cases, the role of CESNET-CERT is to coordinate actions. The high number of alerts as well as the lack of human resources with expert knowledge, demands advanced support for detection, assessment, and handling of incidents in CESNET and in its connected organizations.

Hewlett Packard Enterprise (HPE)

HPE's internal cybersecurity department is responsible for protecting HPE against all forms of cyber threats and attacks. There are two 24 by 7 follow-the-sun Security Operations Centers (SOCs) that the company has across the globe, one in Galway, Ireland, and the other in Roseville, California. The SOC receives over five billion cyber events daily. Specific software assists in turning these events into approximately 500

actionable events that are required to be analyzed extensively. The cybersecurity teams also manage approximately 100 phishing e-mails per day. Indicators from these phishing and malware campaigns are shared with national bodies and law enforcement like the FBI or Interpol.

F-Secure

One of the main ways for F-Secure to deliver its attack detection and response services to the customers is as a fully managed service. cybersecurity experts at the F-Secure Rapid Detection & Response Center (RDC) continuously (24x7x365) monitor alerts, produced by machine learning- and rule-based attack detection engines, filter out false positives, and flag anomalies and signs of data breaches. To confirm anomalies as actual attacks, the RDC experts typically analyze relevant data and contextual information from customer environments, often in an iterative fashion. Confirmed attacks are promptly communicated to affected customers and guidance is provided on the necessary steps to contain the attacks and remediate the affected systems, together with detailed attack information, which can be used as evidence in criminal cases.

Dreamlab Technologies

Dreamlab's main activities are focused on cyber defense, cyber forensics, audits, strategic consulting and education. Another focus lies on the conception, realization, integration, operation and maintenance of IT solutions based on open standards. Dreamlab's offensive capabilities should provide SAPPAN with insights about the attacker's perspective. In recent years, Dreamlab also develops defensive solutions for SOCs and is constantly increasing its experience in this area.

1.2.2 Use cases

For the structured collection of use cases, we developed a common template to be used by consortium members. High-level, generalized use cases derived from the ones collected from the paartners are provided below. The use case presentation contains a description of the acting team member in the organization, steps used to respond and recover in the use case and data sources employed by the use case. The use cases are accompanied by the "used data" table, where high-level data source requirements – including sharing and anonymization – are discussed.

End point attack detection

Descriptive name/goal	**Assessment and handling of end point attack detection**
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 1
Steps	1. The central security backend (BE) detects an end point attack and sends relevant alerts to a SIEM. 2. The SOC analyst selects alerts for processing based on severity and priority. 3. When necessary, the SOC analyst: • queries additional information collected, stored and indexed by BE

	• instructs sensors on the end points to collect and pass additional data to BE • tunes BE and SIEM detection and response logic to react to new threats and false positive cases • takes detection and response decisions
Data sources	End point low-level events, operating system events, end point protection data, third-party data
Tools	• The central security backend (BE) that receives, pre-processes, enriches and analyzes data submissions and local detections coming from sensors on end points. It sends alerts to SIEM. • Security information and event management (SIEM) - SOC automation and visualization • End point sensors

Used data

Data	Phase	Can be shared	Should be anonymized
Third-party data types (reputation lists, OSINT data)	detection	yes	no
SIEM events	assessment	yes	yes
Operating system events (e.g. security events logs, Powershell logs)	detection	no	
Low-level end point events (e.g. process creation, module loading, file system access, network connections)	detection	no	
End point protection events (e.g. malware detections)	detection	yes	yes
Detection and response decisions	handling	yes	yes

Intel match egress alert

Descriptive name/goal	Processing "Egress to blacklisted domain or URL or host" alert – decide if true/false positive and decide on corrective action/containment
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 2
Steps	1. Egress to blacklisted domain or URL or host is detected by a firewall, network tap or IDS and an alert is raised. 2. The analyst identifies the computer causing egress, the user and the organizational unit, 3. checks if the computer already fired an alert recently and surrounding traffic 4. The analyst investigates the event: 1. from the detecting device's log, he/she determines if an activity was blocked or successful,

	2. determines what caused egress (web, malware, phishing link, C&C, macro script, torrenting, ...) using web proxy logs, firewall logs, host-based agents, asking an employee, 3. determines malware type (credential harvester, RAT, ...) 5. decides on corrective action (reset browser or password, deploy malware removing tool, engage advanced threat team, apply a quarantine, etc.)
Data sources	Inventory, LDAP, DHCP and DNS logs, inteligence (Crowdstrike, MISP, etc.), IDS, firewalls and web proxy logs, computer-local log
Tools	• Firewall • IDS • web proxy

Used data

Data	**Phase**	**Can be shared**	**Should be anonymized**
Blacklisted host IP or DNS name or URL	detection	yes	no
DHCP logs	assessment	no	
Computer type (server or workstation)	assessment	yes	no
Computer OS including version and patch level	assessment	yes	yes
LDAP user info	assessment	no	
User	assessment	no	
Organizational unit	assessment	no	
Organization unit distance[N1]	assessment	yes	no
Alerts log	assessment	no	
Surrounding/related traffic	assessment	yes	yes
Host log	assessment	no	
Process that caused egress network traffic that was detected	assessment	yes	no
Malware type	handling	yes	no
Corrective action	handling	yes	yes

[N1] organization unit distance can be used to discriminate between targeted and random phishing campaigns.

Handling a phishing campaign that uses an organization's e-mail infrastructure for spamming

Descriptive name/goal	Phishing campaign, mitigation of compromised e-mails accounts that were used for spamming
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 3
Steps	1. An alert about spam originating from the organization is received and its e-mail servers/domains are blocked 2. The analyst identifies the compromised account specific to the alert and contacts the user to change their password 3. The analyst identifies the phishing e-mail and the used link 4. The analyst uses the pieces of information from previous step in order to find other compromised accounts in the organization and contacts the users to change their passwords 5. The analyst makes a request to block the malicious domain and deletes the e-mail from users' inboxes 6. He/she then sends a request to blacklist providers to remove their e-mail server from the blacklist 7. Local administrators are contacted to use backup e-mail servers until the main server is removed from blacklists 8. Affected users are invited for educational training
Data sources	IP flow monitoring, host logs, e-mail logs, inventory, LDAP
Tools	Network monitoring tools, host monitoring tools

Used data

Data	Phase	Can be shared	Should be anonymized
Corrective action	handling	yes	yes
Host info	assessment	no	
Initial phishing e-mail	assessment	yes	yes
Phishing URL	detection	yes	no
SMTP relay info	detection	yes	no
Surrounding traffic	assessment	yes	yes
User info	assessment	no	

Possible phishing e-mail evaluation

Descriptive name/goal	Assess possible phishing e-mails, mitigate phishing, and share intelligence
Team member	SOC analyst
Unique use	SAPPAN-generalized 4

case ID	
Steps	1. The analysts get an e-mail with a suspicious link from a user to analyze 2. They check if the link or domain is already present in threat intelligence 3. If not, they open the link in a safe environment and classify it (benign, credential harvester, malware, ...) 4. If not benign, the analysts make a request to block the domain and delete the e-mail from the users' inboxes 5. The analysts find users that have already egressed to the phishing link and contact them for corrective actions 6. Intelligence on the URL and additional pieces of information are shared
Data sources	Threat intelligence, link from the e-mail
Tools	Safe environment, antivirus

Used data

Data	Phase	Can be shared	Should be anonymized
Category of phishing	preparation	yes	no
Intelligence	detection	yes	no
Number of targeted employees	preparation	yes	no
Organization distance	preparation	yes	no
Phishing e-mail	detection, preparation	yes	yes

Anomalous traffic peak assessment and handling

Descriptive name/goal	Anomalous traffic peak assessment; decide if true/false positive; decide on corrective action
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 5
Steps	1. The analyst receives an alert reporting an outbound anomalous traffic peak from a network monitoring system. 2. The analyst identifies source computers and looks for a common denominator. 3. He/she checks if the computers have fired alerts recently and their surrounding traffic 4. He/she determines what caused the egress (web browser, malware, phishing link, C&C, macro script, torrenting, ...) 5. The analyst decides about a corrective action and executes it
Data sources	Flow data, alerts, host log
Tools	Rule- or UEBA-based, network monitoring alert system

Used data

Data	Phase	Can be shared	Should be anonymized
Flow data	detection, assessment	yes	yes
Alerts	assessment	yes	yes[N2]
History of blacklisted host IPs	assessment	yes	no
Computer type (server, printer, router, etc.)	assessment	yes	no
DNS	assessment	yes	no
Inventory	assessment	no	
Behavioral pattern	handling	yes[N3]	no
Network monitoring alert system rules	handling	yes[N4]	no
Data from UEBA analytics	detection, assessment	yes	yes

[N2] Contains identifiers that might be considered personal, such as IPs, domains, e-mail addresses.

[N3] If the behavioral pattern is not specific for the given network, it makes sense to share it.

[N4] If the rule does not contain an IP address, it can be shared without restrictions.

Detecting a connection to a command and control server

Descriptive name/goal	**Detection of connections to command and control severs by searching for long-term TCP connections** Malicious activity like reverse shells could be detected by analyzing the time since a TCP connection began. It is common to find reverse shells connected to remote servers on ports like 445, 80 with a duration longer than ten minutes.
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 6
Steps	1. The analyst regularly queries network flows for long TCP sessions on specified ports 2. The analyst determines the process that made the connection and checks for malware 3. If malicious code is found, the analyst decides on corrective action (deploy malware removing tool, engage advanced threat team, apply a quarantine, etc.) 4. Intelligence is updated
Data sources	Netflow and network taps data, host and firewalls logs

Used data

Data	Phase	Can be shared	Should be anonymized
Incoming and outgoing network traffic (unencrypted and encrypted) of servers	preparation, detection	no	
Best practices of other organizations	assessment	yes	no
IP addresses[N5]	handling	yes	depends on traffic
IP address to user mapping	handling	no	
corrective action	handling	yes	yes

[N5] Compare with RAT databases.

Assessment of suspicious account activity

Descriptive name/goal	Assess failed attempts to login into account, decide if benign or malicious
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 7

Steps	1. A failed attempt to login alert appears in the SIEM and the analyst starts to analyze it
	    1. He or she checks if the login attempt was local or remote
	        1. If local, the person attempting the login must have physical access to the server
	        2. If remote, determine network location from source IP and compare with the account owner office location
	2. If it looks like a human error, the analyst engages with the user to confirm it.
	3. He or she raises an alert for further investigation if the attempt is not the human error.

Data sources	LDAP, AD, host logs, SIEM

Used data

Data	Phase	Can be shared	Should be anonymized
Login attempts in access logs	preparation, detection, assessment	yes	yes
LDAP, AD, host logs	assessment	yes	yes
Best practices from other organizations	assessment	yes	no
Corrective action	handling	yes	yes

Detecting malicious activity by examining files with specific extensions

Descriptive name/goal	**Detection of malicious activity by examination of files from HTTP GET requests with uncommon file extensions like .mips, .conf, .config, .exe, .bat, .sh, .bash, etc.**
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 8
Steps	1. The analyst regularly queries the WEB proxy log for HTTP GET requests with files with specific extensions. 2. The analyst tries to download files identified in the previous step and analyze if those are malicious. 3. He or she checks intelligence for known related attacks 4. If positive he or she generates an alert
Data sources	Web server access logs, downloaded files

Used data

Data	**Phase**	**Can be shared**	**Should be anonymized**
HTTP requests	preparation, detection	yes	no
Application info	assessment	yes	yes
File hash	assessment	yes	no
Best practices from other organizations	assessment	yes	no
Corrective action	handling	yes	yes

Scanning alert

Descriptive name/goal	**Decide if unauthorized port scanning alert is true/false positive; decide on corrective action/containment**
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 9
Steps	1. The firewall raises an alert. 2. The analyst determines the nature of the source computer and identifies the user and organizational unit, 3. checks if the computer already fired an alert recently and surrounding traffic, 4. checks the destination port for the scanning activity from the firewall log. 5. If the source system has a local agent, the analyst finds the source process causing activity from the local agent log; otherwise, he/she engages with the system owner to determine if he/she is aware of the activity and the reason for it. 6. The analyst decides on corrective action: system re-image, deploy

	of malware removing tool, engage advanced threat team, apply quarantine.
Data sources	Inventory, LDAP, DHCP logs, DNS logs, firewall logs, computer-local log
Tools	Firewall

Used data

Data	**Phase**	**Can be shared**	**Should be anonymized**
DHCP logs	assessment	no	
Computer type (server or workstation)	assessment	yes	no
Computer OS including version and patchlevel	assessment	yes	yes
LDAP user info	assessment	no	
User	assessment	no	
Organizational unit	assessment	no	
Network distance	assessment	yes	no
Alert log	assessment	no	
Surrounding/related traffic	assessment	yes	yes
Host log	assessment	no	
Process that caused detected network traffic	assessment	yes	no
Malware type	handling	yes	no
Corrective action	handling	yes	yes

Spamming alert

Descriptive name/goal	**Possible spamming alert processing; decide if true/false positive; decide on corrective action/containment**
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 10

Steps	1. The firewall raises an alert.
	2. The analyst checks if this system raised another alert previously as the alert may be related to an ongoing case.
	3. The analyst checks the volume of outbound SMTP events from firewall log,
	4. checks the destination IPs over SMTP ports
	  1. If destinations are antivirus tool-owned etc., this is indicative of a misconfiguration (false positive for spamming) and an e-mail is sent to the owner to correct it.
	  2. If destinations are known SMTP (e.g. Google, Yahoo, etc.), the user is contacted to determine if a personal mail client is

	installed. 3. If destinations are known spam-related relays or unknown infrastructure, the system owner is engaged. A quarantine may be required if spamming is confirmed. The analyst determines the process that caused SMTP network traffic from computer logs if available and analyzes the executable for malware.
Data sources	Inventory, LDAP, DHCP logs, DNS logs, firewall logs, SMTP logs, computer-local log
Tools	Firewall

Used data

Data	**Phase**	**Can be shared**	**Should be anonymized**
DHCP logs	assessment	no	
Computer type (server or workstation)	assessment	yes	no
Computer OS including version and patchlevel	assessment	yes	yes
LDAP user info	assessment	no	
User	assessment	no	
Organizational unit	assessment	no	
Network distance	assessment	yes	no
Alert log	assessment	no	
Surrounding/related traffic[N6]	assessment	yes	yes
Host log	assessment	no	
Process that caused SMTP traffic	assessment	yes	no
Malware type if detected	handling	yes	no
Corrective action	handling	yes	yes

[N6] For detection models

Infection via forgotten account

Descriptive name/goal	**Handling an infection via a forgotten account** A forgotten account with a weak password gets compromised and used as an entry point to the internal network. In case of reused password, it allows for lateral movement across the organization services.
Team member	SOC analyst
Unique use-case ID	SAPPAN-generalized 11

Steps	1. An attacker obtains access to an account with weak password using a dictionary attack 2. The attacker identifies other services in the organization, accessible with obtained credentials and uses them for lateral movement 3. An incident handler or an automated system detects an unusual behavior (e.g. log in at midnight, too many failed login attempts) 4. The analyst identifies the account and either removes or disables it 5. The recovery team identifies assets accessible with compromised credentials and performs an additional audit
Data Sources	IP flow monitoring, host logs, e-mail logs, case management system, contacts, LDAP, ...
Tools	Network monitoring tools, host monitoring tools, case management system

Used data

Data	**Phase**	**Can be shared**	**Should be anonymized**
Dictionary enumeration attempts	handling	yes	no[N7]
User info	assessment	no	
Host info	assessment	no	
Surrounding traffic	assessment	yes	yes
Adversary movement patterns	handling	yes	yes[N8]
Corrective action	handling	yes	yes

[N7] Only if the dictionary is not personalized (generated per user).

[N8] For use with machine learning models.

Infection via a vulnerable application

Descriptive name/goal	**Handling of infection via a vulnerable application** An unpatched vulnerability in an application is used as an entry point to internal infrastructure, which may be used for other forms of attack, e.g. ransomware deployment.
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 12
Steps	1. A vulnerable (unpatched/outdated/0-day/default configuration) application in an organization (e.g., ICS controller, terminal server) is compromised. 2. An attacker moves laterally within the local network (e.g. move via shared folders, printers) 3. The attacker uses access to files for execution of ransomware. 4. A ransomware request appears in the organization. 5. The analyst identifies damage. 6. Prevention measures from further spread are applied. 7. Possibilities of data recovery are investigated (decryption

	possibilities, backup data availability). 8. The initial compromise is identified. 9. Vulnerable service/host is patched and security audit of the whole company is executed (patch services, …)
Data sources	IP flow monitoring, host logs, case management system, LDAP, open source intelligence, ...
Tools	Network monitoring tools, host monitoring tools, case management system

Used data

Data	**Phase**	**Can be shared**	**Should be anonymized**
Application info	assessment	yes	no
Vulnerability info	assessment	yes	no
Malware sample/info	handling	yes	no
Surrounding traffic	assessment	yes	yes
Adversary movement patterns	handling	yes	yes[N9]
Corrective action	handling	yes	yes

[N9] For use with machine learning models.

Man-in-the-middle – illicit network gateway

Descriptive name/goal	**Handling MITM, illegal network gateways** Sensitive pieces of information are being harvested using a MITM attack launched on a publicly available access point.
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 13
Steps	1. An attacker gets access to a network, e.g. physical access/wifi access (old protocols/unsecured network/WPA2 vulnerabilities) and sets up a man-in-the-middle device (MITM). 2. The attacker re-routes traffic via MITM device (e.g. ARP/DHCP spoofing). 3. The attacker collects information/access credentials and uses them for lateral movement. 4. The analyst regularly tries to identify misused access points to the network by analyzing logs. 5. A MITM device is identified. 6. The analyst finds out what data has been compromised. 7. Network access policies are reviewed/checked.
Data sources	IP flow monitoring, host logs, case management system, LDAP, open source intelligence, ...
Tools	Network monitoring tools, host monitoring tools

Used data

Data	Phase	Can be shared	Should be anonymized
Network logs	detection	yes	yes
Initial PoC info	assessment	yes	yes
Malicious CA cert	assessment	yes	no
Adversary network profile	handling	yes	no
Surrounding traffic	assessment	yes	yes
Corrective action	handling	yes	yes

DNS queries to non-trusted DNS servers

Descriptive name/ goal	**Detecting and assessment of DNS queries to non-trusted DNS servers.** Malicious activity like DNS poisoning could be detected comparing the destination IP to a source of black/whitelist of DNS servers.
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 14
Steps	1. The analyst regularly compares DNS requests against a whitelist/blacklist and checks TLS properties. 2. He or she generates an alert if the real time activity exceeds predetermined parameters.
Data sources	Intelligence (whitelist/blacklist of DNS servers), DNS traffic, TLS traffic

Used data

Data	Phase	Can be shared	Should be anonymized
DNS traffic	preparation, detection	no[N11]	
Benign public key certificates	preparation, detection	no	
Malicious public key certificates	preparation, detection	yes	no
Benign TLS client hello messages	preparation, detection	no	
Malicious TLS client hello messages	preparation, detection	yes	yes
Suspicious domain, host	assessment	yes	no
Best practices of other organizations	assessment	yes	no

IP addresses	handling	no	
IP address to user mapping	handling	no	

N11 Sharing of extracted features or whole machine learning models might be possible.

Remote Desktop Protocol (RDP) exploits

Descriptive name/ goal	**Detection and assessment of Remote Desktop Protocol (RDP) vulnerability exploitation**
Team member	SOC analyst
Unique use case ID	SAPPAN-generalized 15
Steps	1. The analyst regularly checks firewall, IDS and IPS logs for unusual activity of malicious IPs and domains. 2. He or she detects connections to command and control servers like chained RDP connections, multiple RDP communication from same host in short time. 3. The analyst compares findings with known databases of indicators of compromise 4. correlates information with other systems 5. compares active models vs. real-time activity 6. He or she generates an alert if the real-time activity exceeds predetermined parameters.
Data sources	Firewall logs, IDS logs, IPS logs, SIEM logs

Used data

Data	**Phase**	**Can be shared**	**Should be anonymized**
TCP traffic	preparation, detection	yes	
UDP traffic	preparation, detection	yes	
Session numbers	assessment	yes	no
Best practices of other organizations	assessment	yes	no
IP addresses	handling	no	
IP address to user mapping	handling	no	
Corrective action	handling	yes	yes

Enabling local attack detection logic

This is a special use case reflecting the customer's decision making with respect to local attack detection capabilities, which are one of the key elements in the SAPPAN plan. In that sense, the use case can be considered a part of the customer validation of the project outcomes.

Descriptive name/goal	**Deciding on the use of the local anomaly detection system (enable/disable)** CISO, as a person responsible for InfoSec policies, technologies, and processes, has to decide on enabling/disabling the local anomaly detection systems.
Team member	Chief Information Security Officer (CISO)
Unique use case ID	SAPPAN-generalized 16
Steps	1. The CISO considers consequences of switching on the local anomaly detection system: ◦ less data are sent to and processed in the central security backend (BE), potential cost savings ◦ reduced privacy concerns ◦ increase of the load of the end-points 2. The CISO decides if the local anomaly detection system will be enabled on all commuters or only on a part and about its settings. 3. The SOC implements the decision and specifies needed SIEM events. 4. CISO regularly reviews reports on the key performance indicators to monitor the impact of local anomaly detection and to evaluate its configuration.
Data sources	Predefined KPIs for system monitoring, organizational IT infrastructure description, value/criticality of various resources, past cybersecurity incidents in the organization, specifications for the available local anomaly detection system
Tools	The local anomaly detection system, monitoring tools for system performance

Used data

Data	Phase	Can be shared	Should be anonymized
Local anomaly detection system non-functional requirements and specification	preparation	yes	yes
Local anomaly detection system functional requirements and specification	preparation	yes	yes
Organizational IT infrastructure description	preparation	no	
Reports on the key performance indicators for SOC	preparation	yes	yes
Reports on the key performance indicators for local anomaly detection system	preparation	yes	yes

1.3 Identified areas for improvements

The following table presents opportunities for possible improvements discovered during the analysis of the collected use cases and discussions with the cybersecurity professionals.

Step	Current data/functionality	Required data/functionality
Selection of alerts for processing	Alerts are displayed in tabular form ordered by priority.	Showing alerts as points in a two-dimensional plane where the distance between the points is proportional to similarity of the alerts and the priority and severity are expressed by size and color is a presentation that allows analysts to pick up alerts that are related.
Identification of the computer and its type (workstation/ server), user and organization	Information should be looked up in several applications	Enriching of the alerts by consolidated data about a computer, user, location and organizational unit would reduce the analysts' effort during the assessment phase. Adding the confidence level for the match to identified host would add clarity in specific cases (eg. DHCP).
Analyze surrounding/related traffic	• Manual search in firewall and other logs, no possibility to save filters • There is only tabular representation of traffic	• Show similar computers that raised the same alert type recently • Show changes in the computer's behavior close to the alert time • Show data filtered specifically for alert type • A visual graph showing communication between computers
Detecting compromised computers	Manual search to get users info	Show the distance between users that logged to a certain computer and show outlines
Assessment of suspicious account activity	Manual approach is time consuming	Authentication: • High-fidelity classifier that assesses failed login attempts • Adaptive authentication techniques Authenticated session: • High-fidelity classifier that assesses suspicious activities • Trigger immediate action such as killing session, etc. ML-based or CEP-based techniques may come into play.
High-fidelity "change in a computer behavior" detection	Alerts are usually based on thresholds, either set manually or computed from past data for the computer or group of computers with similar users, etc. Such a	A novel approach with high-fidelity with minimum false positive alerts

	logic produces a lot of false positives.	
Automatic clustering of alerts	Alerts are not automatically correlated, so it is difficult for the analysts finding similar events	Automatic clustering of with listing of common features/patterns
Threat hunting	Network and host-based data are separated, no possibility to make a query that correlates them	Both, network and host-based data, in one system that allows making a correlated query
Threat hunting	Case data is logged by analysts into a case system that is not connected with security data management	It should be possible to correlate case data to host data to allow analyst to see if a host has been referenced in previous cases
Threat hunting	Manual queries to multiple systems are required to establish context	Contextual data should be gathered for events relevant to the alert and presented to the analyst with the alert. The contextual data for different alert types will vary but may include time-based before and after network data and host log process tree data.
Threat hunting	Alert generating intelligence often arrives months after the first cases are detected in the wild. Manual process is used to do historical search for selected intelligence.	Tool should be available to automatically scan historical data for cases when new intelligence arrives
Threat hunting	Different levels of data retention cause problems for threat hunt teams.	Consistent data retention across sources with some levels of "smart" aggregation/filtration acceptable to reduce volume. Aggregation and filtration can be based both on domain knowledge and statistical/machine learning processing.
Detecting phishing domain/url	Phishing domains and URLs can be generated, which makes traditional approach with blacklists inefficient	A machine learning-based detection of generated domains/URLs with very high precision.

2 SAPPAN selected use cases

This section contains the use cases selected for demonstrating SAPPAN functionality. The use cases are based on the real-world use cases described above from partner organizations, but there are also new use cases designed to address the identified areas for improvement. The use cases were selected to allow demonstrating SAPPAN functionality and also to address the trending threats like phishing, malware, spam and ransomware that emerged from our literature review above.

The use cases have been selected based on the current state of knowledge. Thus, it is likely that some changes will be necessary, for instance, to address new threats, during the project lifetime. Therefore, it may be necessary to review the current

document in the course of the project in an iterative fashion and reflect important changes.

2.1 Addressed trending threats

Phishing is a social engineering technique designed to obtain users' trust using fraudulent messages and to convince them to perform a certain set of actions, beneficial to the adversary, who is in most cases an author of the phishing campaign. The most prevalent communication medium of phishing campaigns is e-mail, mostly due to its widespread use among enterprise employees and its decentralized nature. However, recent reports show a steady increase in the utilization of other communication channels, such as SMS, mobile instant messaging and social media Cisco, Threat Report, February 2019. Phishing is currently the most prevalent method of malware delivery Symantec, Internet Security Threat Report, February 2019. The payload is usually delivered either as an attachment or using a malicious URL, which may seem legitimate at first glance. Employees with limited technical knowledge are particularly susceptible to phishing campaigns. Therefore, user training focused on cybersecurity awareness is one of the best countermeasures against phishing. However, due to high implementation costs of training, an automated or semi-automated approach to phishing mitigation is more feasible.

Spam is the abusive use of e-mail and messaging technologies to distribute unsolicited messages. These may include messages that fall into the "phishing" category. Since e-mail operates without a central monitoring authority, the responsibility to protect users against spam is on the shoulders of e-mail service providers. Thanks to the advancements in anti-spam protection techniques, changes in underground spam ecosystem and law enforcement activities, overall spam activity is on the decline. However, the majority of spam messages originate from mail servers of compromised companies. This negatively impacts the company itself, since their domains end up on a variety of spam blocklists. Therefore legitimate e-mail communication will be dropped by an anti-spam solution of recipient's mail server. Negotiations with blocklist providers to remove the domain from the list are often tedious and compromised company is expected to provide proof that the source of spam campaign has been eradicated. Additionally, messages, that are moved into spam folders, negatively impact the credibility of the company.

Ransomware is a type of computer malware that blocks victim's access to its device and/or data stored on its drives. It then presents the victim with a message describing the situation and demanding ransom in exchange for the access to the blocked resources. If the malware is written properly, recovery from such attack is very difficult without a backup. The ransom is extorted using cryptocurrency, making tracing and prosecution of perpetrators challenging. While cybersecurity researchers have developed many tools, that are able to successfully recover encrypted data, there are many variants of ransomware where recovery without original decryption key is impossible. It is then to the choice of the victim whether or not the ransom should be paid. However, it should be noted that paying the ransom does not guarantee data recovery. While significant portion of ransomware is spread using e-mail attachments, a drive-by download from compromised websites has also been observed ENISA, Threat Landscape Report 2018, January 2019.

2.2 Use cases summary

The following table shows the selected use cases along with the threats they address and their relation to the other work packages.

- WP3: Massive Data Acquisition and Local Attack Detection
- WP4: Managing and Automating Threat Intelligence
- WP5: Sharing and Federation for Cyber Threat Detection and Response

Use Case Name	Threat/s	WP3	WP4	WP5	Visualization
Manual detection of phishing with malware	Phishing, Malware			X	
Automated phishing detection by ML tool that analyses egress URLs	Phishing, Malware	X		X	
Ransomware detection, containment and impact mitigation (manual)	Ransomware	X		X	X
Ransomware detection, containment and impact mitigation (semi-automatic)	Ransomware	X		X	
Automated processing of historical data when new intelligence arrives	Phishing, Malware		X	X	
Handling successful phishing campaigns	Phishing, Spam	X		X	
Domain Generation Algorithm (DGA) detection	Malware	X	X	X	
Detection of compromised servers	Malware	X		X	
Automatic assessment of suspicious account activity	Malware	X			

2.3 Selected use cases

Manual detection of phishing with malware

Descriptive name/goal	Analyze possible phishing case with malware and share intelligence about it
Team member	SOC analyst
Unique use case ID	SAPPAN-selected 1
Steps	1. A user receives a suspicious e-mail with a link and sends it to the SOC. 2. The analyst checks that neither the link URL nor its domain are in intelligence. 3. The analyst opens the link in a safe environment and classifies the payload as malware. 4. The analyst collects additional information (to whom was sent the same e-mail etc.) and carries out local containment (request to sinkhole/block the domain by DNS and delete e-mails in users'

	inboxes, etc.) 5. Intelligence with the URL and additional information is shared
Data sources	Intelligence, link from the e-mail

Automated phishing detection by ML tool that analyses egress URLs

Descriptive name/goal	**Analyze possible phishing case with malware and share intelligence about it**
Team member	SOC analyst
Unique use case ID	SAPPAN-selected 2
Steps	1. The classifier raises an alert about potential phishing URL 2. The analyst opens the URL in a safe environment and classifies it (benign, credential harvester, malware, ...) 3. The analyst collects additional information (whom was sent the same e-mail etc.) and makes local containment (request to sinkhole/ block the domain by DNS and delete e-mails in users' inboxes, etc.) 4. Intelligence with the URL and additional information is shared
Data sources	DNS queries, public key certificates, TLS client hello messages (SNI), URL
Tools	• Machine learning classifier for phishing URL detection

Ransomware detection, containment and impact mitigation (manual)

Descriptive name/goal	**Ransomware detection, containment and impact mitigation**
Team Member	SOC analyst
Unique use case ID	SAPPAN-selected 3
Steps	1. The analyst monitors a visual tool that shows attack similarity and detects a quickly growing cluster of similar alerts on the screen. 2. The analyst determines the attack path by analyzing traffic from and to the computers that raised alarms using a network communication visualization tool. 3. The analyst applies quarantine/network filters for the computers that raised alarm. 4. The analyst liaises with with management to design and agree on deployment of other needed containment actions. 5. The ransomware is analyzed. 6. The remedy actions are designed, tested and deployed. 7. Intelligence is shared.
Data sources	Firewall logs, netflow and network taps data aggregated by minutes interval, hosts logs
Tools	• Visual tool that shows attack similarity • Visualization tool that shows communication between computers and additional context info (OS type, version and vulnerabilities...) • Intelligence sharing platform

Ransomware detection, containment and impact mitigation (semi-automatic)

Descriptive name/goal	**Ransomware detection, containment and impact mitigation**
Team member	SOC analyst
Unique use case ID	SAPPAN-selected 4
Steps	1. An ML-based system identifies unusual behavior of several computers that has similar features 2. It raises alarm and also shows predicted attack path and a suggestion for containment 3. The analyst verifies the attack path and suggestion for containment 4. The analyst applies the suggested containment action 5. The ransomware is analyzed 6. The remedy actions are designed, tested and deployed 7. Intelligence is shared
Data sources	Firewall logs, netflow and network taps data aggregated by minutes interval
Tools	• ML-based entity behavior analysis system • Aggregating ML-based system for clustering of alerts • Intelligence sharing platform

Automated processing of historical data when new intelligence arrives

Descriptive name/goal	**Detection of incidents that happened in past using new intelligence** There is delay between a new threat emerging and being detected and analyzed in the wild wherefore processing of historical data is important
Team member	Automated intelligence exchanging system
Unique use case ID	SAPPAN-selected 5
Steps	1. The system gets new intelligence in a machine-readable format 2. The system determines whether data for a post-hoc analysis are available in the organization and executes the analysis 3. The report is sent to a SOC analyst 4. If handling instructions are available for the intelligence, an automatic remedy can be started by the analyst
Data sources	Available network and host historical data
Tools	• Automated intelligence exchanging system • Automated handling system

Handling successful phishing campaigns

Descriptive name/goal	**Mitigation of effects of a successful phishing campaign**
Team member	SOC analyst

Unique use case ID	SAPPAN-selected 6
Steps	1. An unusual mailing activity alert is raised by a SMTP or network monitoring system 2. The analyst validates the alert and contacts the user to change his/her password 3. The analyst determines the attack chain as phishing 4. The spam e-mails are deleted and users that already clicked the malicious link are asked to change their password as well. 5. Intelligence is shared
Data sources	SMTP and network monitoring, host logs, e-mail logs, inventory LDAP, ...
Tools	• Network monitoring tools • Host monitoring tools

Domain Generation Algorithm (DGA) detection

Descriptive name/goal	**Detection, assessment and handling of infected hosts or IoT devices by malware that uses Domain Generation Algorithms (DGAs)**
Team member	SOC analyst
Unique use case ID	SAPPAN-selected 7
Steps	1. The classifiers detect an algorithmically generated domain name 2. The analyst confirms or disproves the incident. The triage can be omitted in case of high-confidence classification. 3. Network traffic for the infected host is blocked until malware is removed. 4. Malicious DNS queries are attributed to a malware by another classifier. 5. Based on the detected malware, handling steps are recommended. 6. The analyst confirms or modifies the handling steps. 7. Intelligence of known malicious domain names and DGAs (e.g. DGArchive) is updated and shared
Data sources	DNS NX-traffic for detection, DNS queries and IP addresses for response action
Tools	• Machine learning classifiers on NX traffic for detection of algorithmically generated domain names • Multi-class classification model to attribute malicious queries to malware which generated it

Detection of compromised servers

Descriptive name/goal	**Detection of compromised servers and assessment**
Team member	SOC analyst
Unique use case ID	SAPPAN-selected 8

Steps	1. The classifier analyzing network flow data raises an alert with reasoning 2. The analyst validates the alert 3. The analyst determines the cause of the anomalous traffic (malware, compromised account, etc.) 4. The analyst decides on a corrective action and executes it 5. Intelligence is updated and shared
Data sources	Incoming and outgoing network traffic (unencrypted and encrypted) of servers, host logs
Tools	• Machine learning classifiers

Automatic assessment of suspicious account activity

Descriptive name/goal	**Automatic assessment of account activity** Decide if failed login attempts for an account and other activity are benign or malicious
Team Member	SOC analyst
Unique usecase ID	SAPPAN-selected 9

Steps	1. The analyst gets an alert about suspicious account activity with
	    1. confidence
	    2. reasoning (unusual location, time etc.)
	    3. contextual data (previous logins, server activity, etc.) with highlighted outlines
	2. The analyst decides if the alert is true or false positive and takes corrective actions as needed

Data sources	LDAP, AD, host logs, UEBA data
Tools	• ML classifier with reasoning • UEBA

Glossary

AD - Active Directory
ARP - Adress Resolution Protocol
BE - Back end
BYOD - Bring your own device
CA - Certification Authority
CDC - Cyber Defense Center
CEP - Complex Event Processing
CERT - Computer Emergrency Response Team
CISO - Chief Information Security Officer
CSIRT - Computer Security Incident Respone Team
CVE - Common Vulnerabilities and Exposures
C&C - Command and Control
DB - Database
DGA - Domain Generation Algorithm
DHCP - Dynamic Host Configuration Protocol
DNS - Domain Name System
ENISA - European Network and Information Security Agency
HTTP - Hypertext Transfer Protocol
HTTPS - Hypertext Transfer Protocol over SSL
ICS - Integrated Control System
IDS - Intrusion Detection System
IP - Internet Protocol
IPS - Intrusion Prevention System
IS - Information Security
KPI - Key Performance Indicator
LDAP - Lightweight Directory Access Protocol
MISP - Malware Information Sharing Platform
MITM - Man-in-the-middle
ML - Machine Learning
NOC - Network Operations Center
NX - Non-existing domain (response returned by DNS server)
OSINT - Open Source Intelligence
OS - Operating System
RAT - Remote Access Toolkit
RDP - Remote Desktop Protocol
SIEM - Security Information and Event Management
SMS - Short Message Service
SMTP - Simple Mail Transfer Protocol
SNI - Server Name Indication
SOC - Security Operations Center
SOHO - Small Office/Home Office
SQL - Structured Query Language
SSL - Secure Sockets Layer
SVM - Support Vector Machine
TCP - Transfer Control Protocol
TLS - Transport Layer Security
TOR - The Onion Router
UDP - User Datagram Protocol
UEBA - User Entity Behavior Analitics
URL - Universal Resource Link
VPN - Virtual Private Network
WPA2 - Wi-Fi Protected Access Version 2
WP - Work Package

Reference

ENISA, Threat Landscape Report 2018, January 2019

Symantec, Internet Security Threat Report, February 2019

McAfee Labs, Threats Report, December 2018

Cisco, Threat Report, February 2019

MITRE ATT&CK