Early stage detection of cyber attacks

Bc. Martina Pivarníková

Supervisor: JUDr. RNDr. Pavol Sokol, PhD.

Advisor: Mgr. Tomáš Bajtoš

Goal:

Identify relationships between security incidents to predict attacks = more effective defense against attacks

Intrusion Detection Evaluation Dataset (CICIDS2017)

Monday

Benign
(Normal human activities)

Tuesday

Brute Force -
FTP-Patator
SSH-Patator

Wednesday

DoS / DDoS
DoS slowloris
DoS Slowhttptest
DoS Hulk
DoS GoldenEye
Heartbleed Port 444

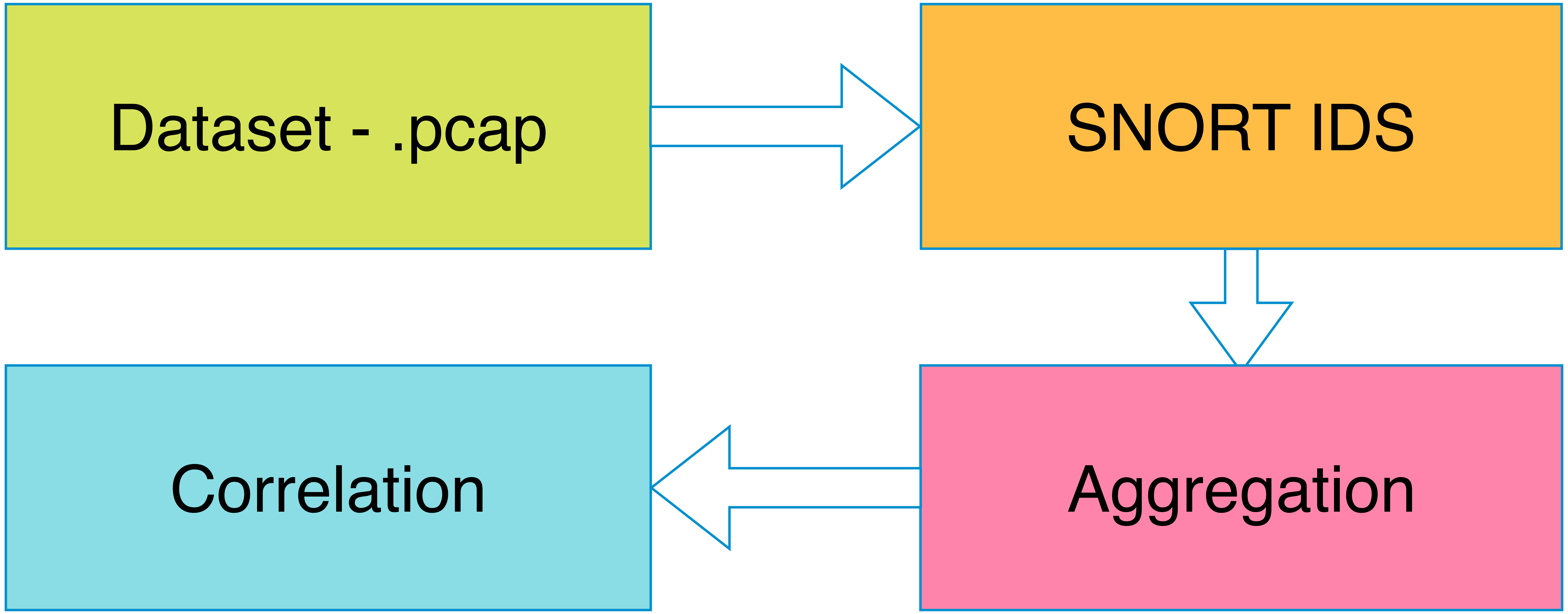
Thursday

Web Attack – Brute Force
Web Attack – XSS
Web Attack – Sql Injection
Infiltration – Dropbox download
Meta exploit Win Vista
Infiltration – Cool disk – MAC

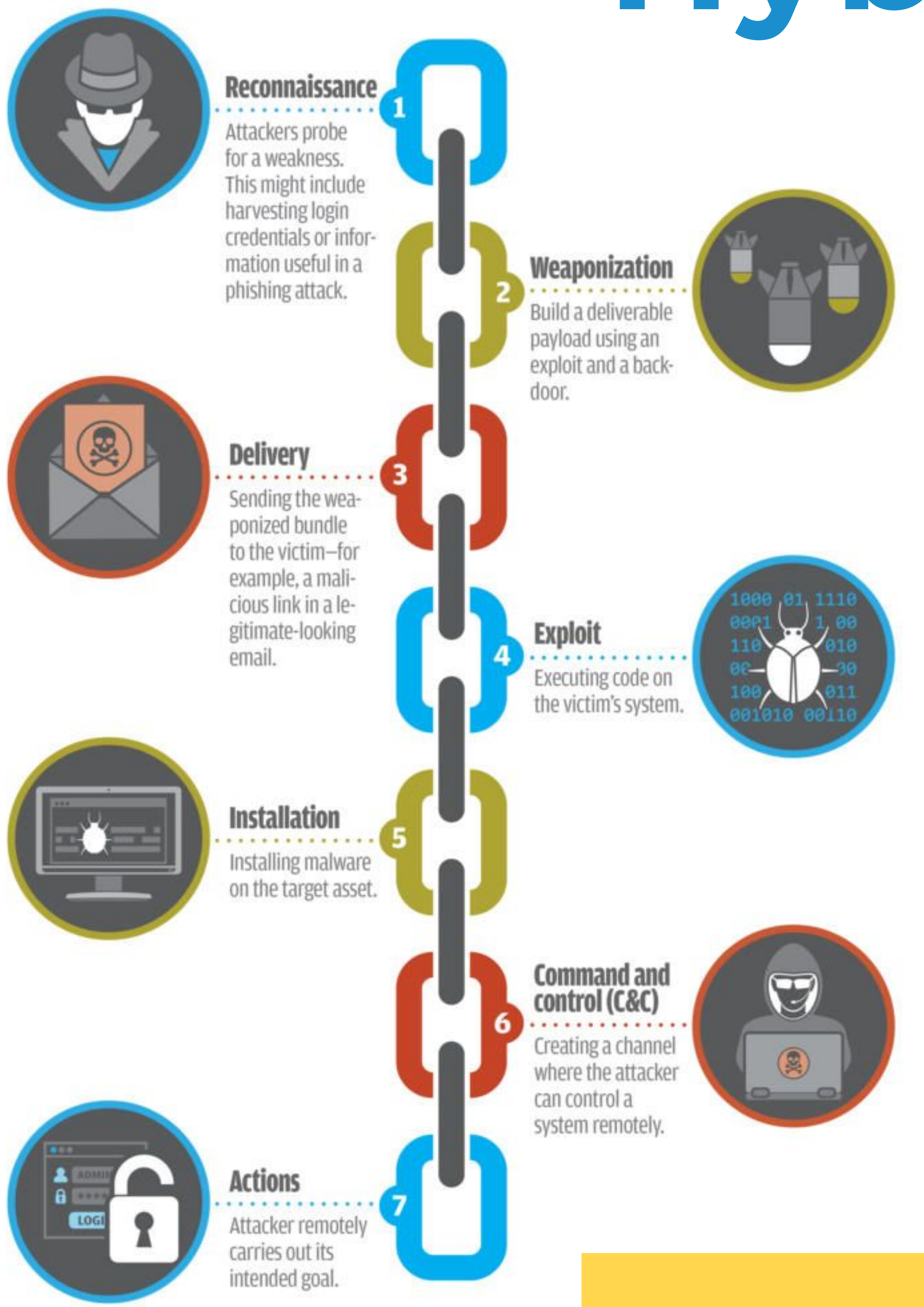
Friday

Botnet ARES
Port Scan
DDoS LOIT

Data processing



Hybrid model



Reconnaissance 1
Attackers probe for a weakness. This might include harvesting login credentials or information useful in a phishing attack.

Weaponization 2
Build a deliverable payload using an exploit and a backdoor.

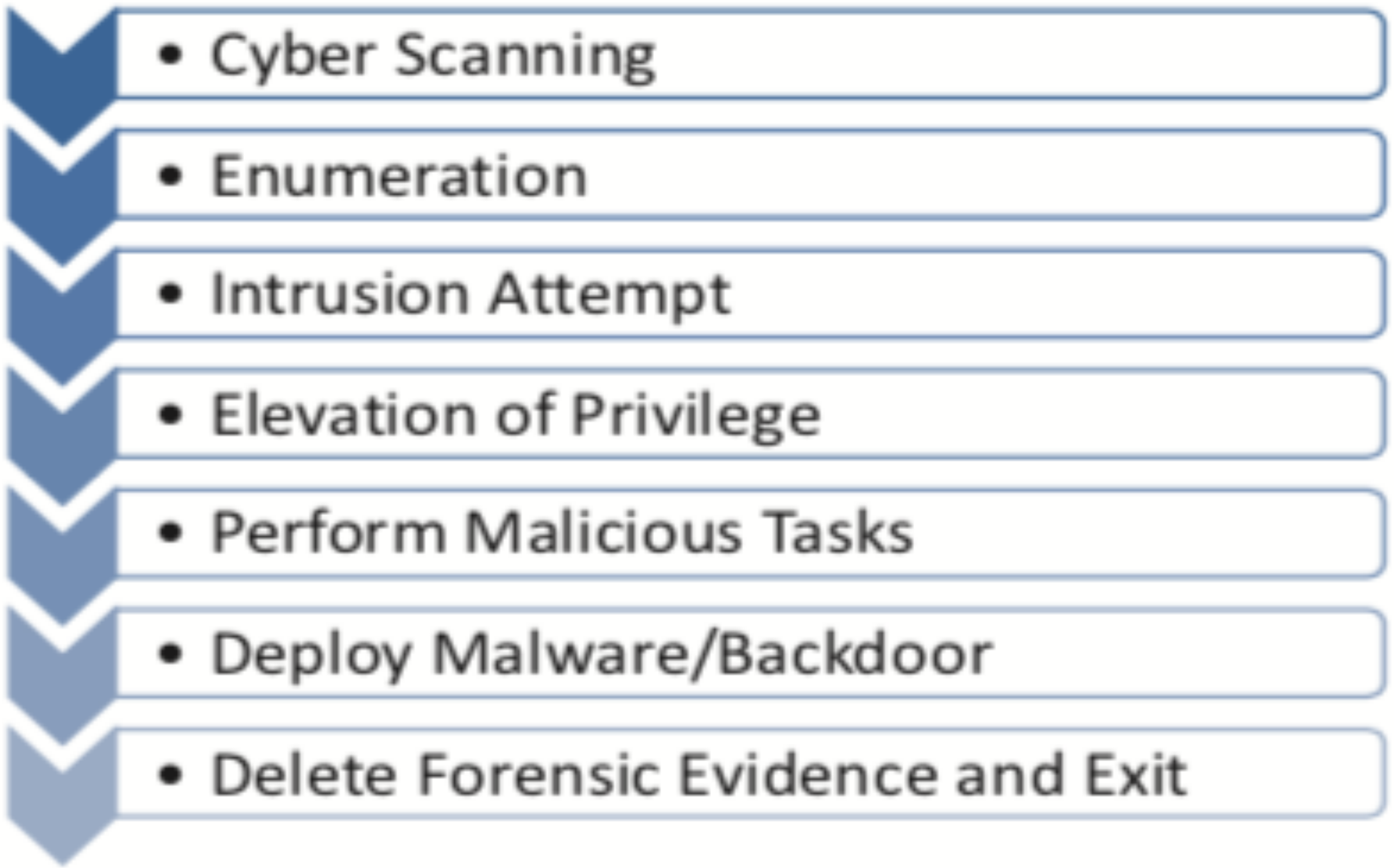
Delivery 3
Sending the weaponized bundle to the victim—for example, a malicious link in a legitimate-looking email.

Exploit 4
Executing code on the victim's system.

Installation 5
Installing malware on the target asset.

Command and control (C&C) 6
Creating a channel where the attacker can control a system remotely.

Actions 7
Attacker remotely carries out its intended goal.

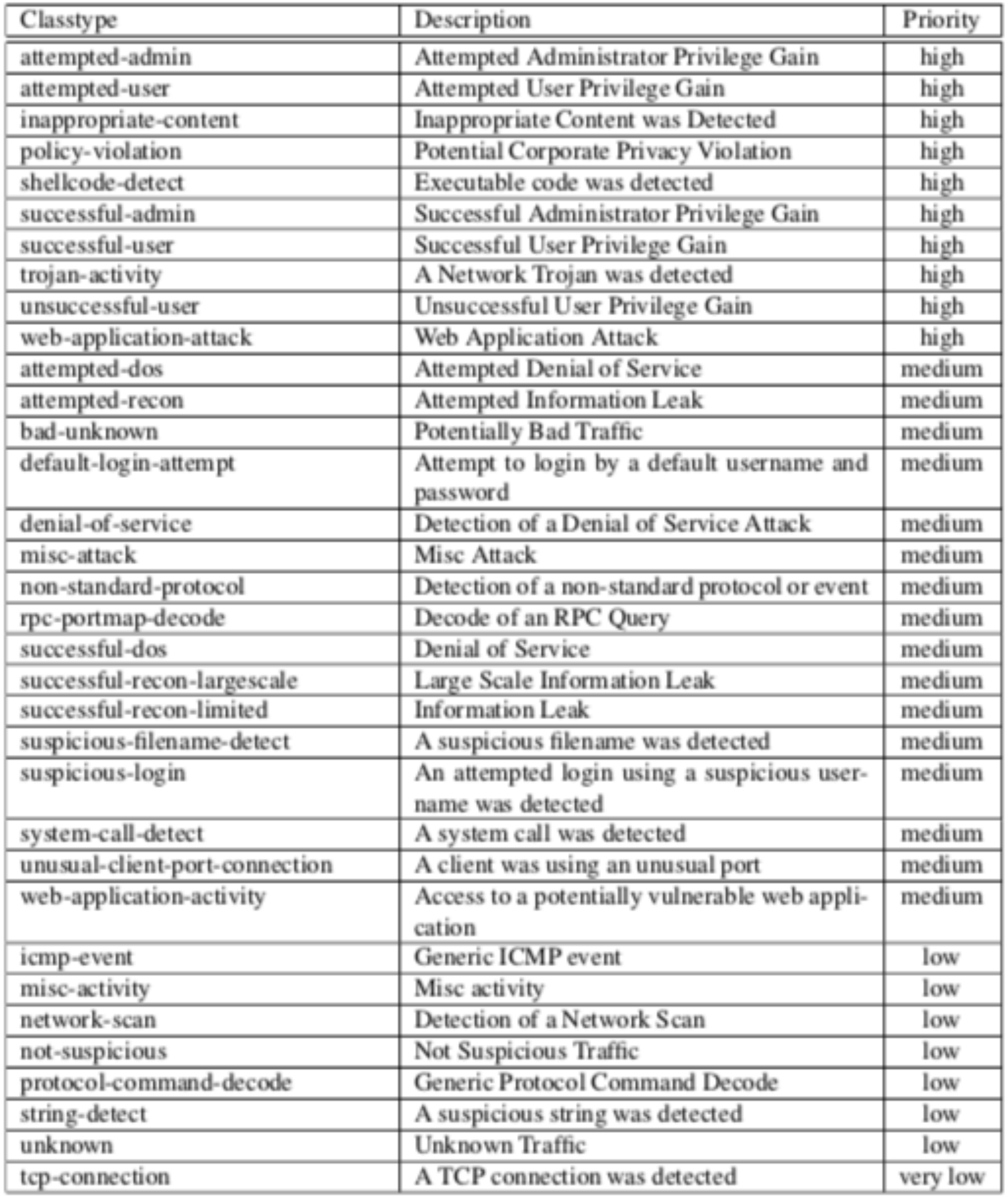


- Cyber Scanning
- Enumeration
- Intrusion Attempt
- Elevation of Privilege
- Perform Malicious Tasks
- Deploy Malware/Backdoor
- Delete Forensic Evidence and Exit

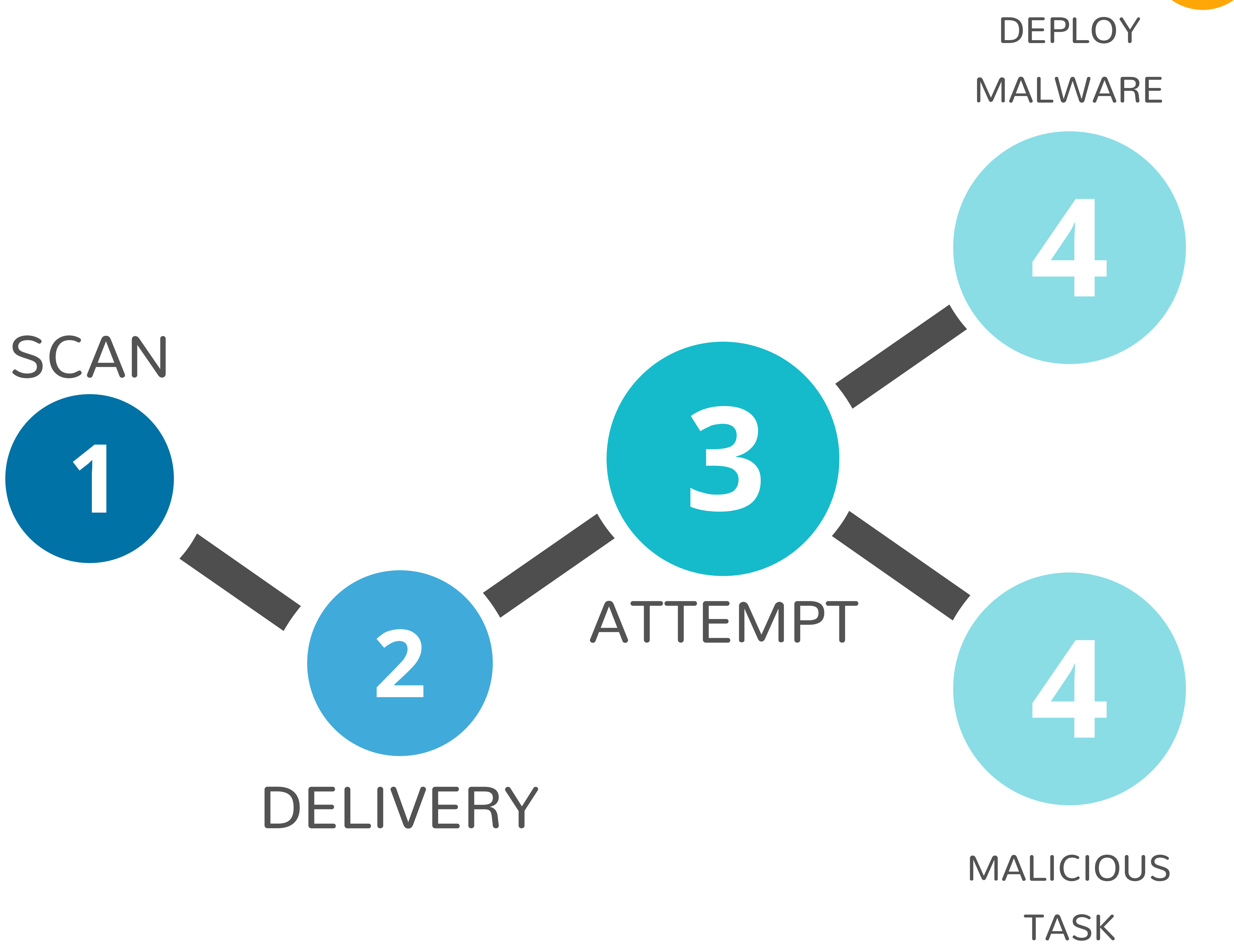
Kill Chain

Cyber Scanning:
A Comprehensive Survey
Elias Bou-Harb, Mourad Debbabi, and Chadi Assi

Table 3.2: Snort Default Classifications



Classtype	Description	Priority
attempted-admin	Attempted Administrator Privilege Gain	high
attempted-user	Attempted User Privilege Gain	high
inappropriate-content	Inappropriate Content was Detected	high
policy-violation	Potential Corporate Privacy Violation	high
shellcode-detect	Executable code was detected	high
successful-admin	Successful Administrator Privilege Gain	high
successful-user	Successful User Privilege Gain	high
trojan-activity	A Network Trojan was detected	high
unsuccessful-user	Unsuccessful User Privilege Gain	high
web-application-attack	Web Application Attack	high
attempted-dos	Attempted Denial of Service	medium
attempted-recon	Attempted Information Leak	medium
bad-unknown	Potentially Bad Traffic	medium
default-login-attempt	Attempt to login by a default username and password	medium
denial-of-service	Detection of a Denial of Service Attack	medium
misc-attack	Misc Attack	medium
non-standard-protocol	Detection of a non-standard protocol or event	medium
rpc-portmap-decode	Decode of an RPC Query	medium
successful-dos	Denial of Service	medium
successful-recon-largescale	Large Scale Information Leak	medium
successful-recon-limited	Information Leak	medium
suspicious-filename-detect	A suspicious filename was detected	medium
suspicious-login	An attempted login using a suspicious username was detected	medium
system-call-detect	A system call was detected	medium
unusual-client-port-connection	A client was using an unusual port	medium
web-application-activity	Access to a potentially vulnerable web application	medium
icmp-event	Generic ICMP event	low
misc-activity	Misc activity	low
network-scan	Detection of a Network Scan	low
not-suspicious	Not Suspicious Traffic	low
protocol-command-decode	Generic Protocol Command Decode	low
string-detect	A suspicious string was detected	low
unknown	Unknown Traffic	low
tcp-connection	A TCP connection was detected	very low



Cyber attack prediction

Machine learning algorithms

Hidden Markov Model

Bayesian network

Objectives

1 Analysis, comparison, and processing of the current approaches to cyber attacks modeling

2 Creating a model data set from security events

3 Design, implementation, and evaluation of the model for early-stage detection of cyber attacks

Literature

- SHOSTACK, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014.
- UCEDAVELEZ, Tony; MORANA, Marco M. *Risk Centric* Threat Modeling: Process for Attack Simulation and Threat Analysis. John Wiley & Sons, 2015.
- CALTAGIRONE, Sergio; PENDERGAST, Andrew; BETZ, Christopher. The diamond model of intrusion analysis. CENTER FOR CYBER INTELLIGENCE ANALYSIS AND THREAT RESEARCH HANOVER MD, 2013.
- HUTCHINS, Eric M.; CLOPPERT, Michael J.; AMIN, Rohan M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 2011, 1.1: 80.
- ERTAUL, Levent; MOUSA, Mina. Applying the Kill Chain and Diamond Models to Microsoft Advanced Threat Analytics. 2018

Thank you for your attention!

Questions?