

DAVE ON CYBER PRESENTS

Domain 1, Booklet 3

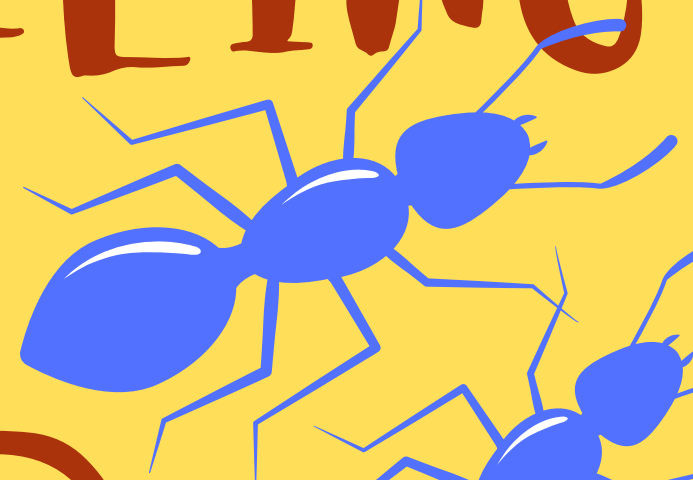
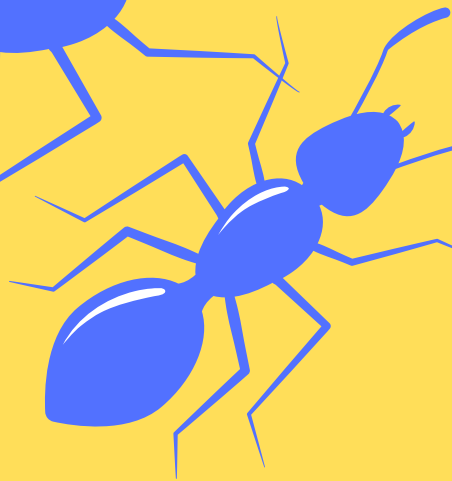
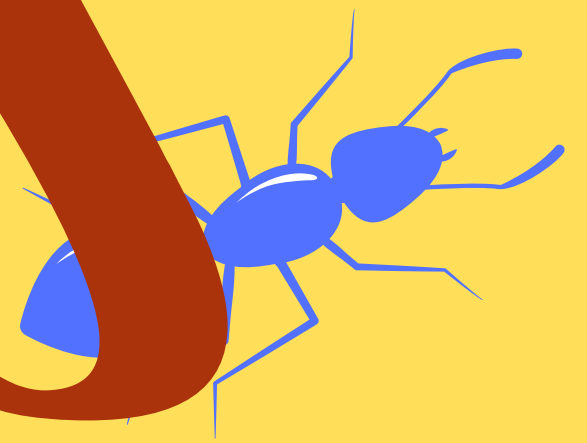
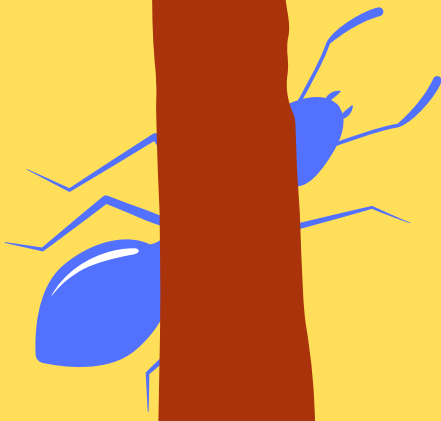
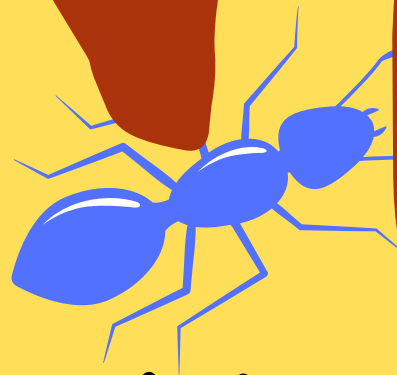
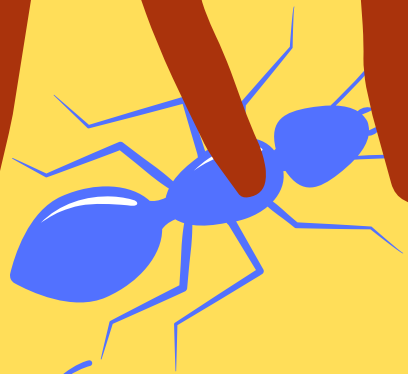
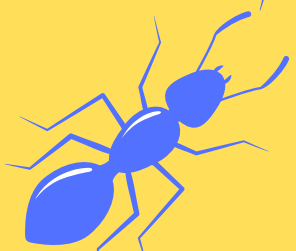
CISSP as an Art

THREAT MODELING

WITH

ANTS

created by Dave Krunal





Once upon a time, there was a place
- SUGAR CASTLE.



It had threat from -
the ANTS Kingdom.

The attack from different kind of ants were increasing day by day.

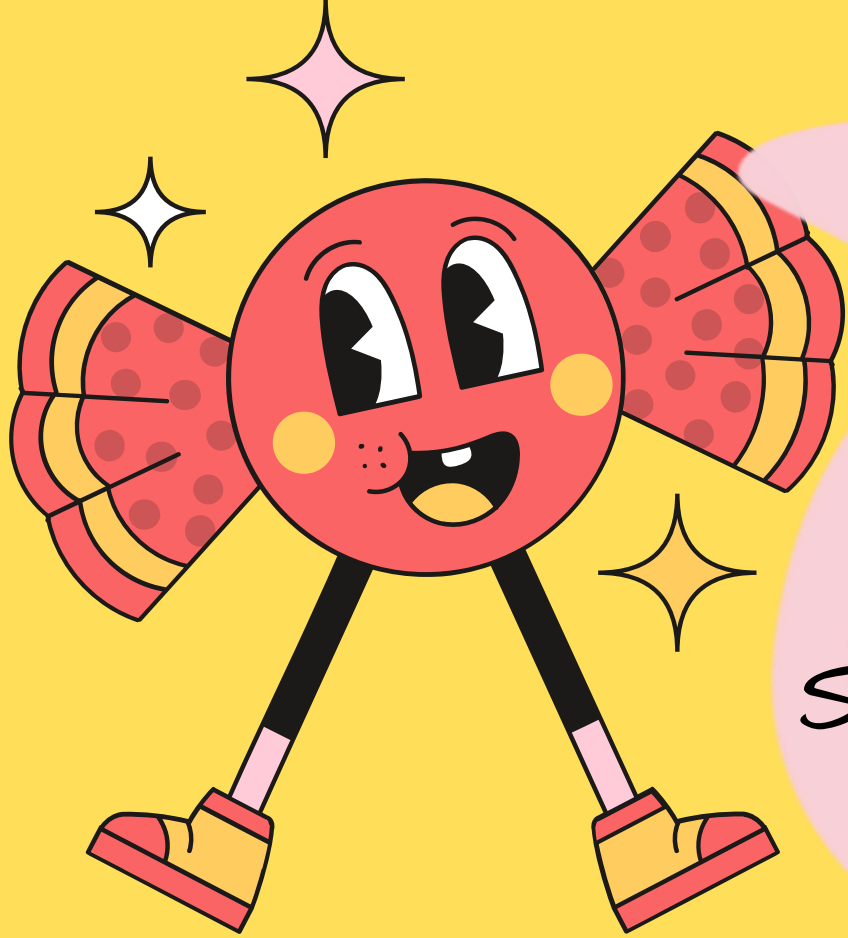


ATTACK

ATTACK

ATTACK

The Sugar Queen called for the urgent meeting.



All the candy leaders,
ASSEMBLE!!

Sugar is oil for our kingdom.
Enough is enough.

**CANDY SQUAD
WAS FORMED**



The process began to categorize
threats using S.T.R.I.D.E model.

S.T.R.I.D.E

Microsoft's STRIDE is a threat model.
It's goal is to prioritize threats
against organization's valuable assets.

asset



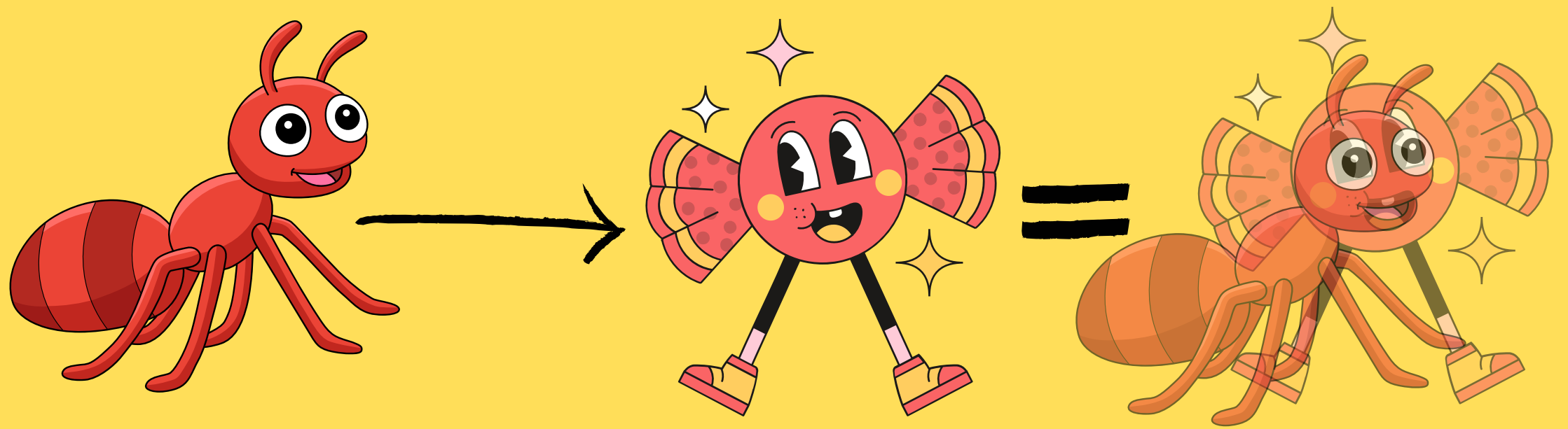
threat



S - SPOOFING

Attacker targets system with false identity.

Attacker can spoof the identity using IP, MAC, email address or any form of logical identity to bypass the security gateway.



Candy leaders identified that big ants used SUGAR QUEEN'S mask and costume to bypass Sugar Castle's perimeter security and enter the kingdom, illegally.

T - TAMPERING

When action results into unauthorised changes in transit or storage.



Tampering violates integrity and availability of the data.



Candy leaders identified that some ants were mixing sugar with white sands inside the sugar truck and warehouse to compromise sugar quality.

R - REPUDIATION

When attacker denies of
any performed action.



Repudiation attacks are
tricky because they often
blame innocent third-parties
for security violations.



They attacked!
Not us.


We are big.
The small ones did.



what? we didn't do...

1 - INFORMATION DISCLOSURE

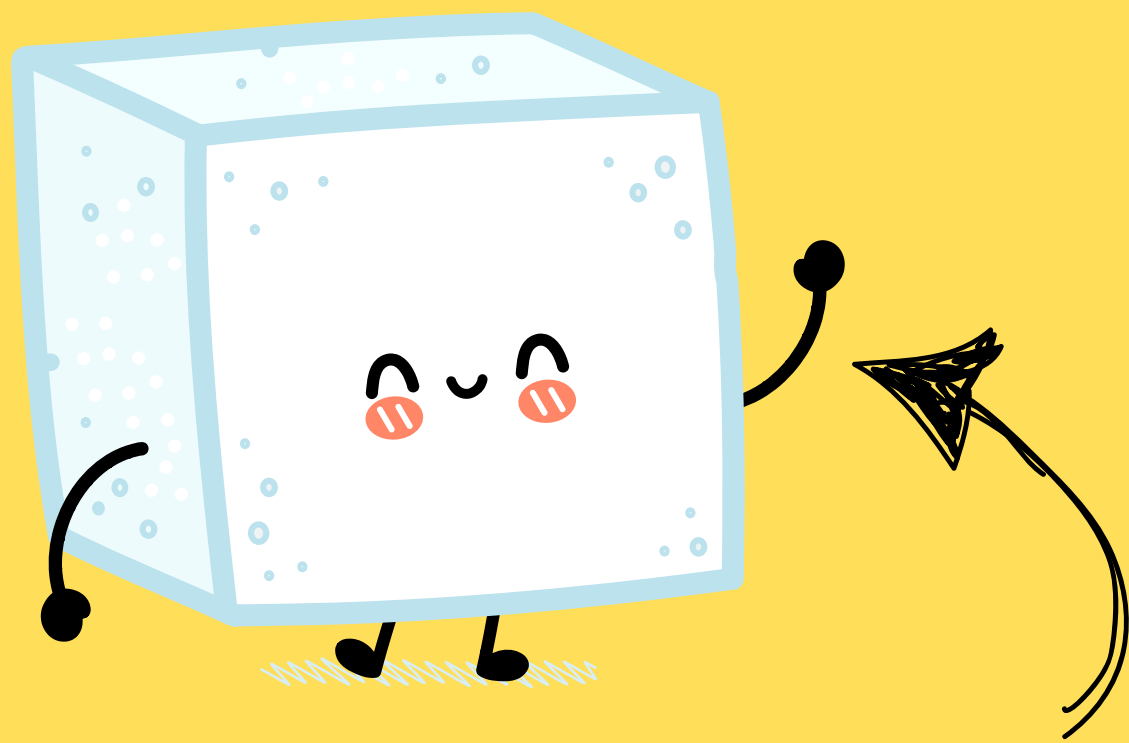
When confidential information is leaked to external unauthorised entities.



The data could be personal identifiable information (PII), payment card details or company's trade secret.

There is no security
between 4-4:30 pm.
It's a secret.

Cool.
Thanks for the tip.



Candy leaders found an internal
informant - the traitor!

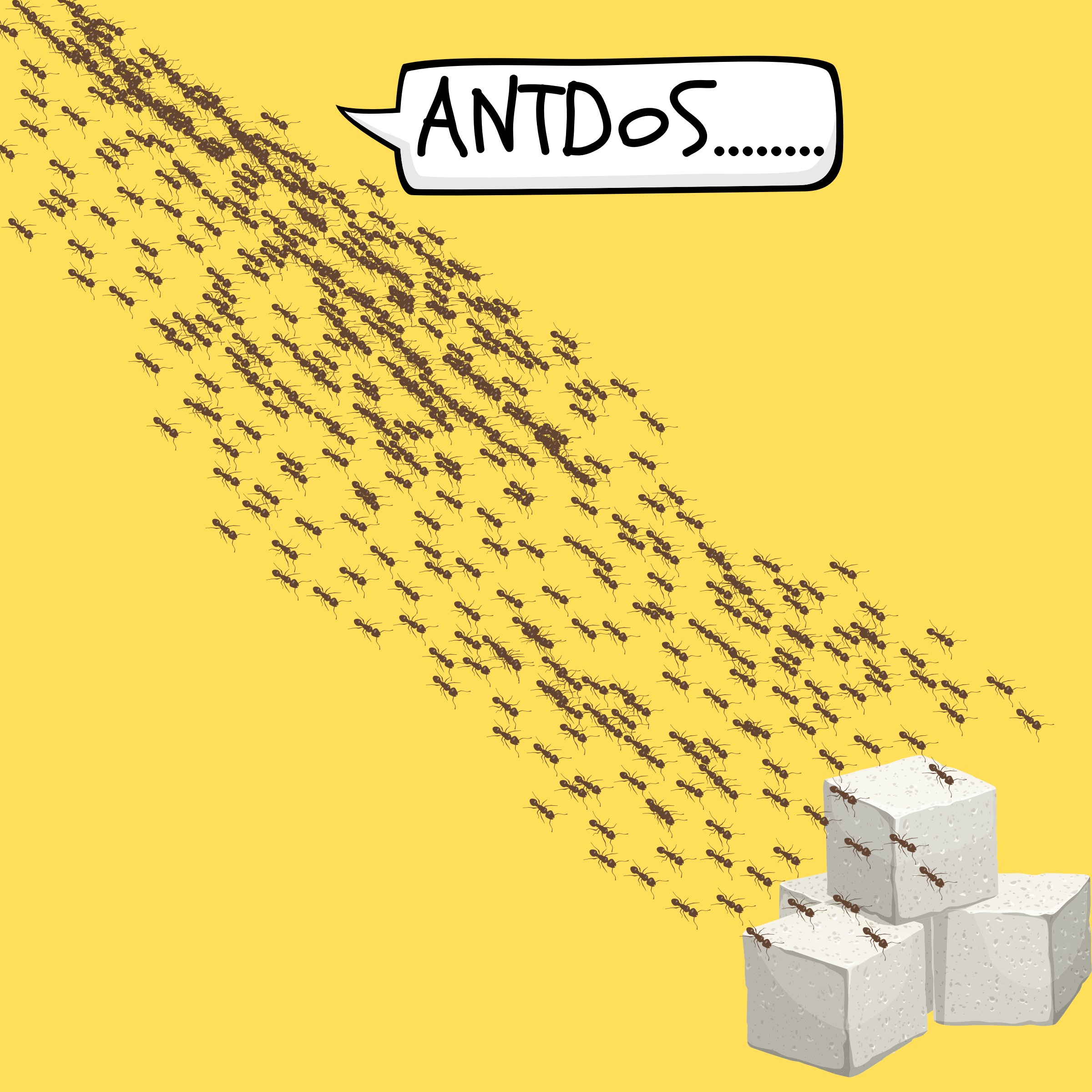
D - DENIAL OF SERVICE (DOS)

When system is hammered with too many requests.

DOS attack prevents authorised use of a resource.

It can introduce the latency and affect the performance and efficiency.

ANTDOS.....



E - ELEVATION OF PRIVILEGE

When attacker gains higher privilege access.



Attacker can get more access by exploiting vulnerability on the system, social engineering attack or credential theft.

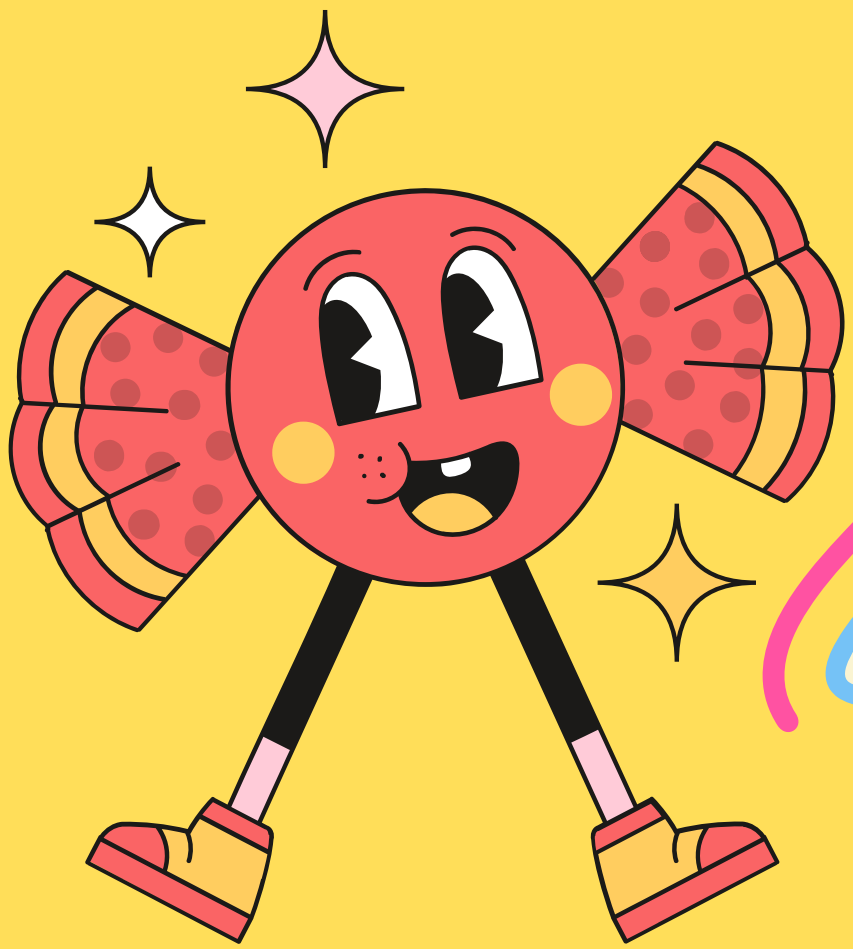


aim high & exploit

CISSP CORE CONCEPT

S - SPOOFING	AUTHENTICATION
T - TAMPERING	INTEGRITY
R - REPUDIATION	NON-REPUDIATION
I - INFORMATION DISCLOSURE	CONFIDENTIALITY
D - DENIAL OF SERVICE (DOS)	AVAILABILITY
E - ELEVATION OF PRIVILEGE	AUTHORIZATION

REMEMBER!



Using S.T.R.I.D.E threat model,
Sugar Castle revised their
security approach with
threat categorization.

IT'S A NEW BEGINNING OF SWEET JOURNEY...

DAVE ON CYBER PRESENTS

CISSP as an Art Series

created by Dave Krunal

I hope you enjoyed this
creative CISSP booklet.

I'd love to connect and hear
you feedback on my work.

SUBSCRIBE - [DAVEONCYBER.COM/SUB/](https://daveoncyber.com/sub/)

CONNECT - [LINKEDIN.COM/IN/DAVEKRUNAL/](https://www.linkedin.com/in/davekrunal/)

EMAIL - [DAVEONCYBER@GMAIL.COM](mailto:daveoncyber@gmail.com)

WEBSITE - [DAVEONCYBER.COM](https://daveoncyber.com)