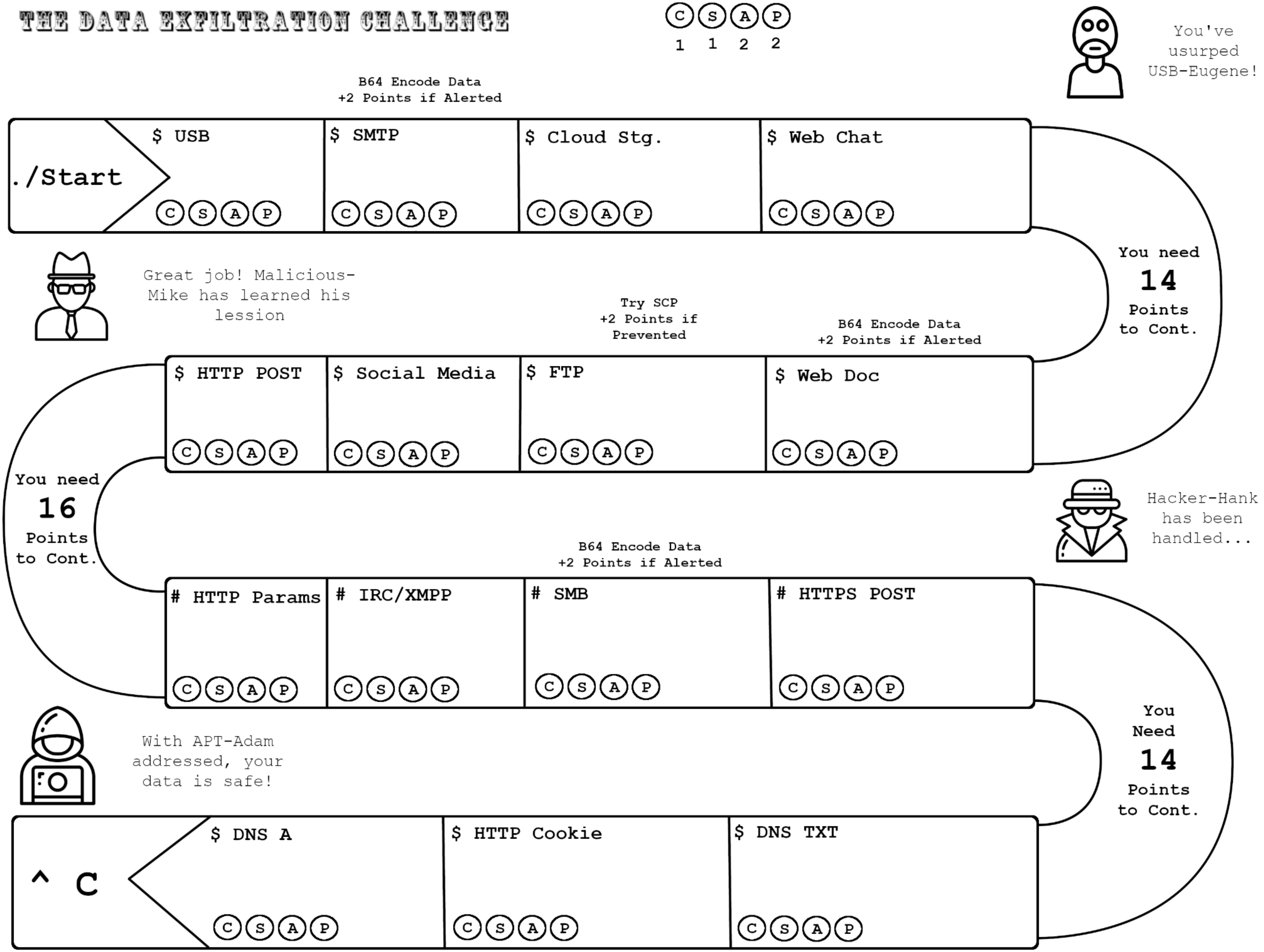
THE DATA EXFILTRATION CHALLENGE

C	S	A	P
1	1	2	2



./Start

$ USB
C S A P

B64 Encode Data
+2 Points if Alerted

$ SMTP
C S A P

$ Cloud Stg.
C S A P

$ Web Chat
C S A P

You've usurped USB-Eugene!

You need **14** Points to Cont.

B64 Encode Data
+2 Points if Alerted

$ Web Doc
C S A P

Try SCP
+2 Points if Prevented

$ FTP
C S A P

$ Social Media
C S A P

$ HTTP POST
C S A P

Great job! Malicious-Mike has learned his lession

You need **16** Points to Cont.

HTTP Params
C S A P

IRC/XMPP
C S A P

B64 Encode Data
+2 Points if Alerted

SMB
C S A P

HTTPS POST
C S A P

Hacker-Hank has been handled...

You Need **14** Points to Cont.

$ DNS TXT
C S A P

$ HTTP Cookie
C S A P

$ DNS A
C S A P

^ C

With APT-Adam addressed, your data is safe!

THE DATA EXFILTRATION CHALLENGE

Preparing for the Challenge

1. Generate a data file containing (mock!) sensitive data.
2. Prepare your infrastructure: test host, external servers, cloud service provider accounts, etc.
3. Get approval to test from the appropriate group(s) in your org
4. Select a token to move across the game board
5. Start at the "./Start" spot and end at "^C"

Playing

- Start at the first game board spot ("USB")

- Perform the appropriate test for that spot

- Mark the response that was taken (see responses to the right), or don't mark anything if there was no response

- Move to the next space

- If you encounter a "You need X Points to Continue" space, sum your points using the scale to the right and move forward if you have enough points

Keeping Score

Ⓒ	Ⓢ	Ⓐ	Ⓟ
1	1	2	2

Ⓒ Control - The activity was logged in the relavent security control - 1 point

Ⓢ SIEM - The activity was logged in the SIEM - 1 point

Ⓐ Alert - An alert was generated in the SIEM and made it to the SOC - 2 points

Ⓟ Prevented - The activity was blocked by a control - 2 points

USB: Transfer your test file to a USB drive, confirm the file can be read on another device

SMTP: Send out an email via SMTP that has your test data as an attachment or in the body

Cloud Storage: Transfer your file to a cloud storage (ex: Google Drive) account

Web Chat: Send your data over a web chat app (ex: Google Hangouts)

Web Doc: Enter your data into a web document (ex: Google Docs)

FTP: Transfer your data to an external FTP server

Social Media: Put your data on Twitter! (please ensure it's mock data...)

HTTP POST: Upload your data via an HTTP POST form

HTTP Params: Embed your data in HTTP query parameters

IRC/XMPP: Send your data via IRC or XMPP

SMB: Upload your data to an external SMB server

DNS TXT: Embed your data in a DNS TXT query and send the query to an external server

HTTP Cookie: Embed your data int an HTTP cookie and send the request to an external server

DNS A: Embed your data into a DNS A query and send the query to an external server