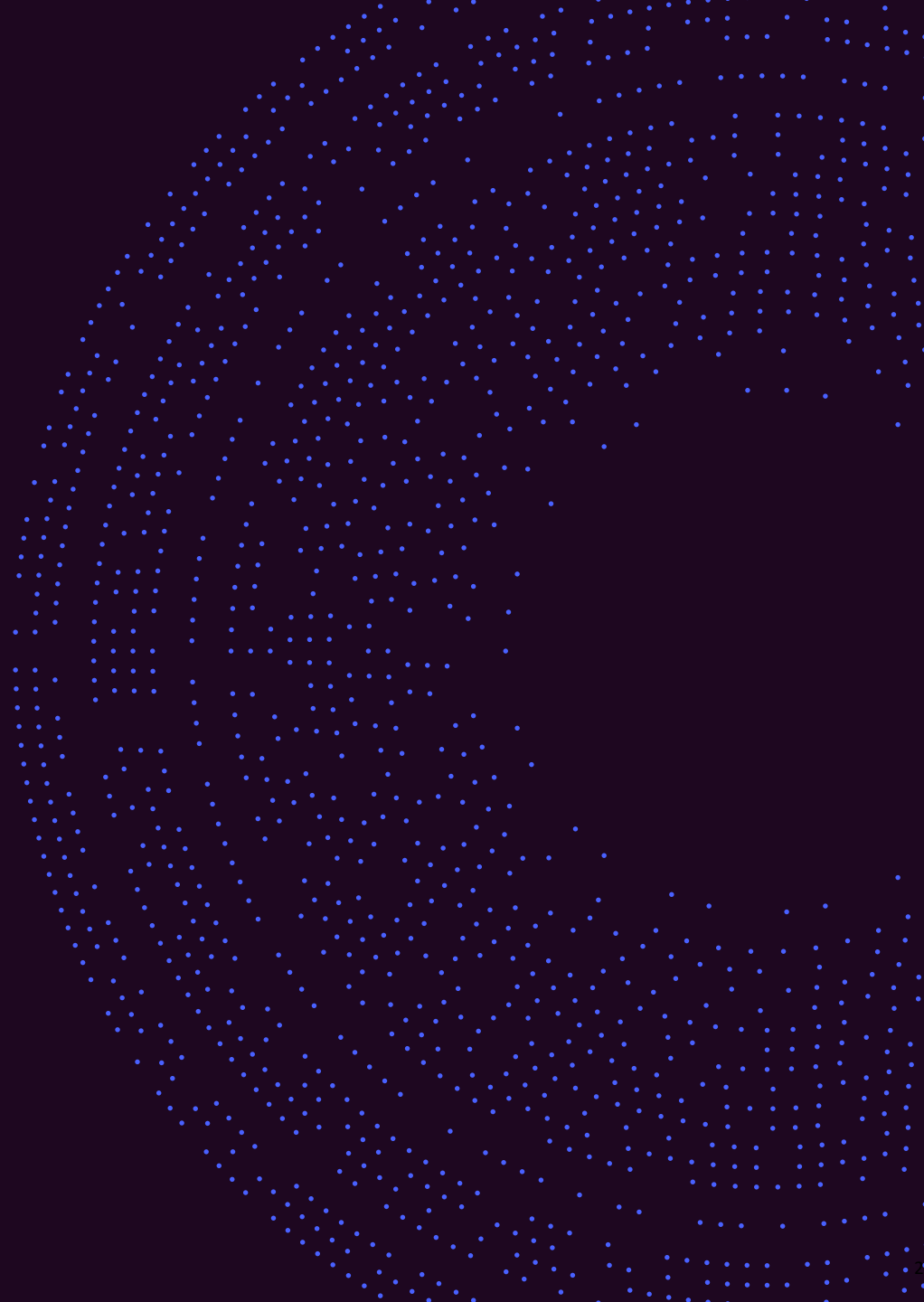
# Oda človeški inteligenci

Jan Bervar
Glavni arhitekt digitalne varnosti
Lastnik storitve NIL Managed Detection and Response

NIL
Part of Conscia

If it bleeds,
it leads.



NIL
Part of Conscia

NIL
Part of Conscia

# Digitalna (?) varnost

- Če hočeš prikriti, da se na tvojem področju nič zelo novega ne dogaja, mu spremeni ime
- Kibernetska varnost!
- No, ni čisto res, da se ne dogaja nič
  - Poslovni modeli kriminalcev, ki izkoriščajo sivo cono obnašanja
  - Hitrost napadov
  - Ogromne poslovne izgube
  - Evolucija obrambe

# Orientacija

| Key | Value |
|---|---|
| Povprečna poslovna škoda v incidentu | 4.300.000 EUR |
| Globalna poslovne škoda incidentov | 9.250.000.000.000 EUR |
| Proračun RS | 15.000.000.000 EUR (0.16%) |
| Povprečen čas do pridobitve domain admin | 90 minut |
| Povprečno bivanje napadalcev v našem okolju | 10 dni |
| Količina nezasedenih delovnih mest v digitalni varnosti | 3.400.000 |

DOBRO

NEKOLIKO NENAVADNO

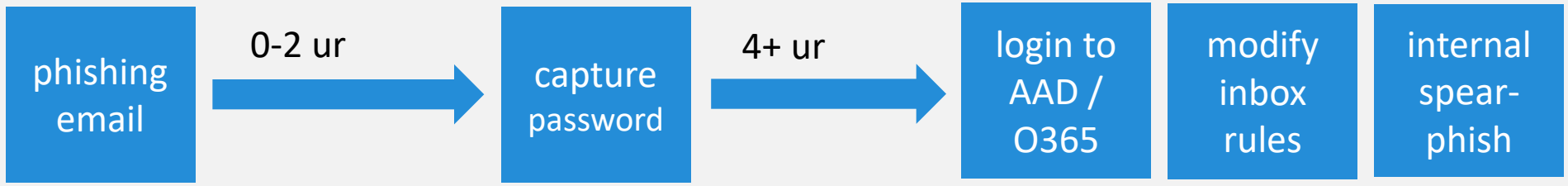
SLABO

tu deluje digitalni kriminal

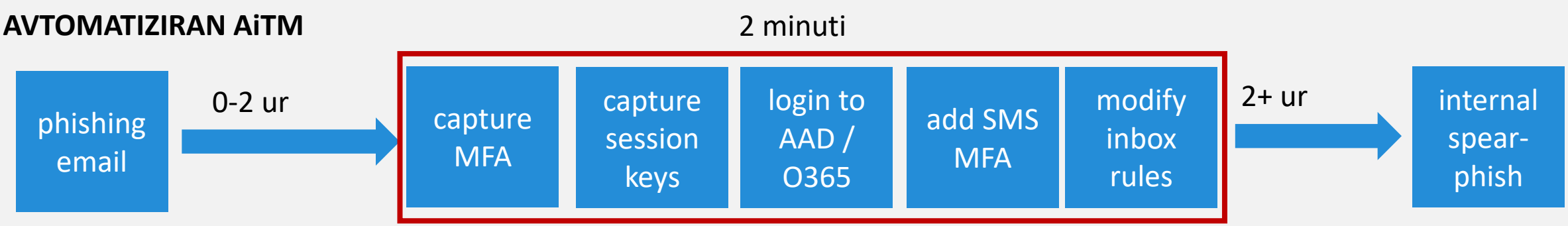
# Verige napadov

## Adversary-in-the-middle (AiTM) napad

**KLASIČEN PHISHING**




**AVTOMATIZIRAN AiTM**



# Študija primera: proizvodno podjetje

- 3 tedne po vstopu v podjetje napadalci pobrišejo vse produkcijske podatke IN backup
- En mesec dela ogromne ekipe za ponovno vzpostavitev osnovnih funkcij IT za podporo proizvodnje
- Neugodno za zunanjega partnerja
- Grožnja eksistenci podjetja

# Študija primera: velik regionalni trgovec

- Pokličejo nas, ker so našli “čudne datoteke” na strežnikih
- Ugotovimo, da je celotno okolje (7000 zaposlenih) popolnoma pod nadzorjem kriminalcev
- Motivacija je kraja in prodaja podatkov konkurenci
- Zanimiv izgon

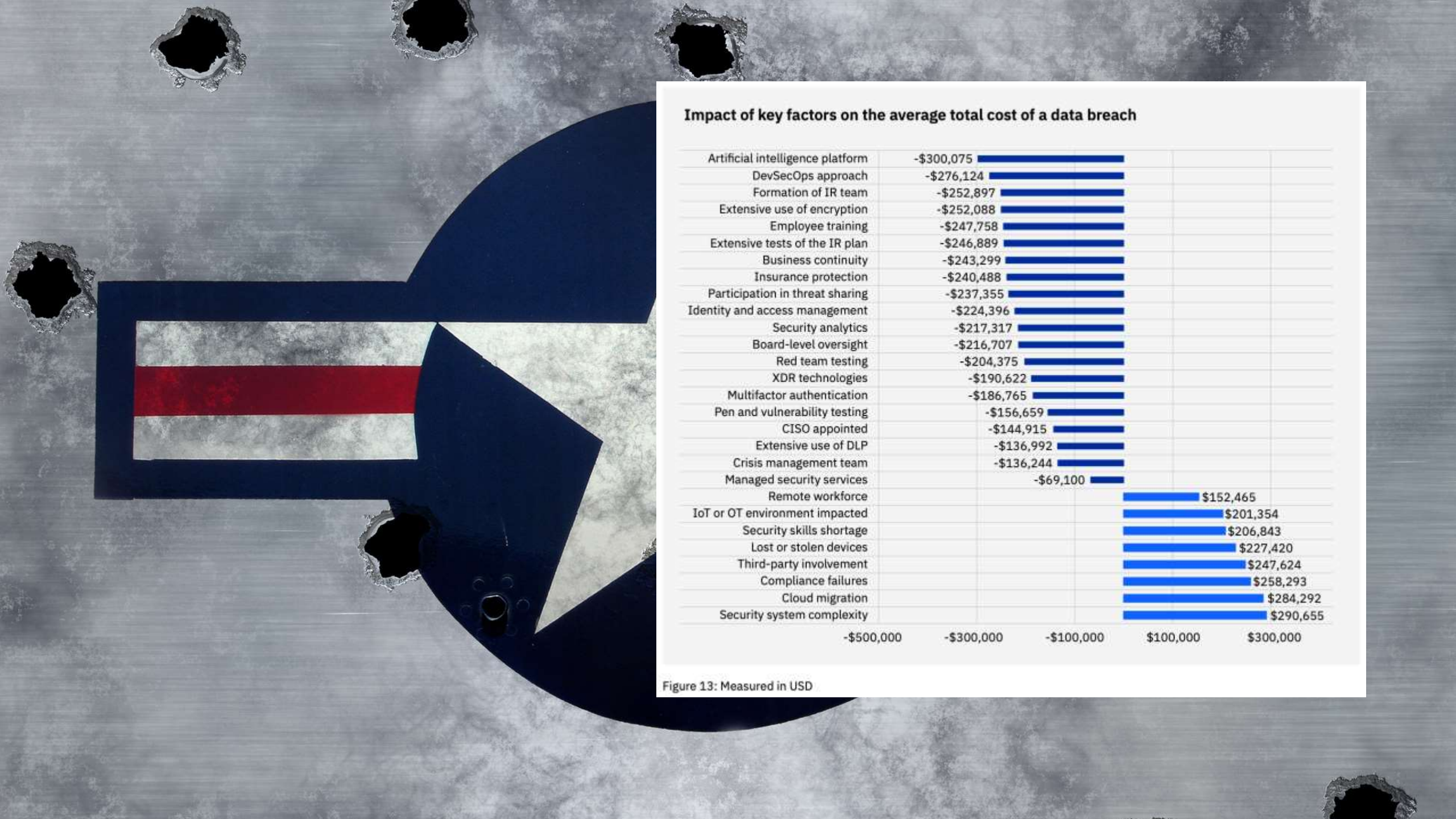



Figure 13: Measured in USD


IGRA VERJETNOSTI VSTOPA JE IZGUBLJENA

# Assume breach.

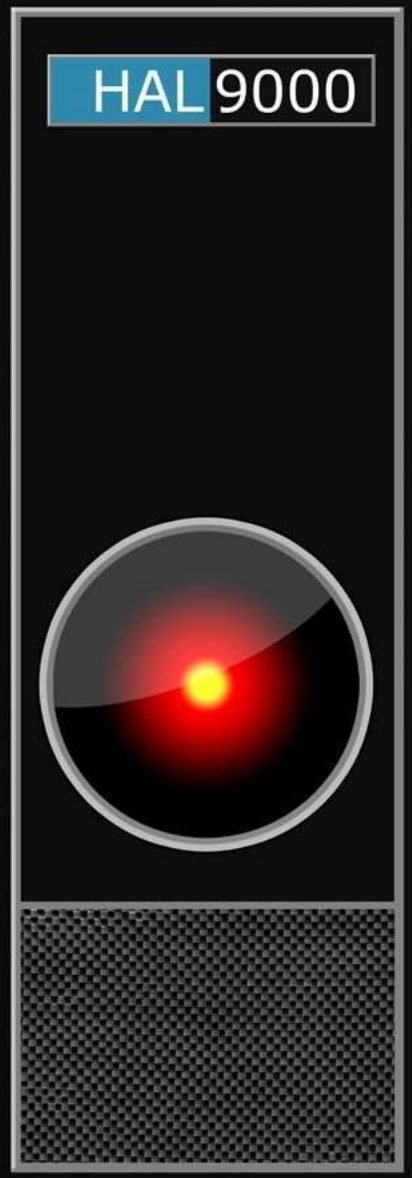
IGRA VERJETNOSTI ZAZNAVE IN ODZIVA JE DOBLJENA

ZDI SE PREPROSTO

PA NI…

IŠČEMO SUPERJUNAKE!

# GenAI NI REŠITEV



# Kaj delamo?

## NIL Managed Detection and Response


250.000 uporabnikov

10 minut TTD / malo FP

visoka inovativnost

5k preiskav / 800 napadov / 150 incidentov

Intelektualno nagrajujoče

phishing / napreden malware

0 velikih incidentov pri strankah v 6 letih

Join us,
and together we can
rule the galaxy!

Part of Conscia

Part of Conscia