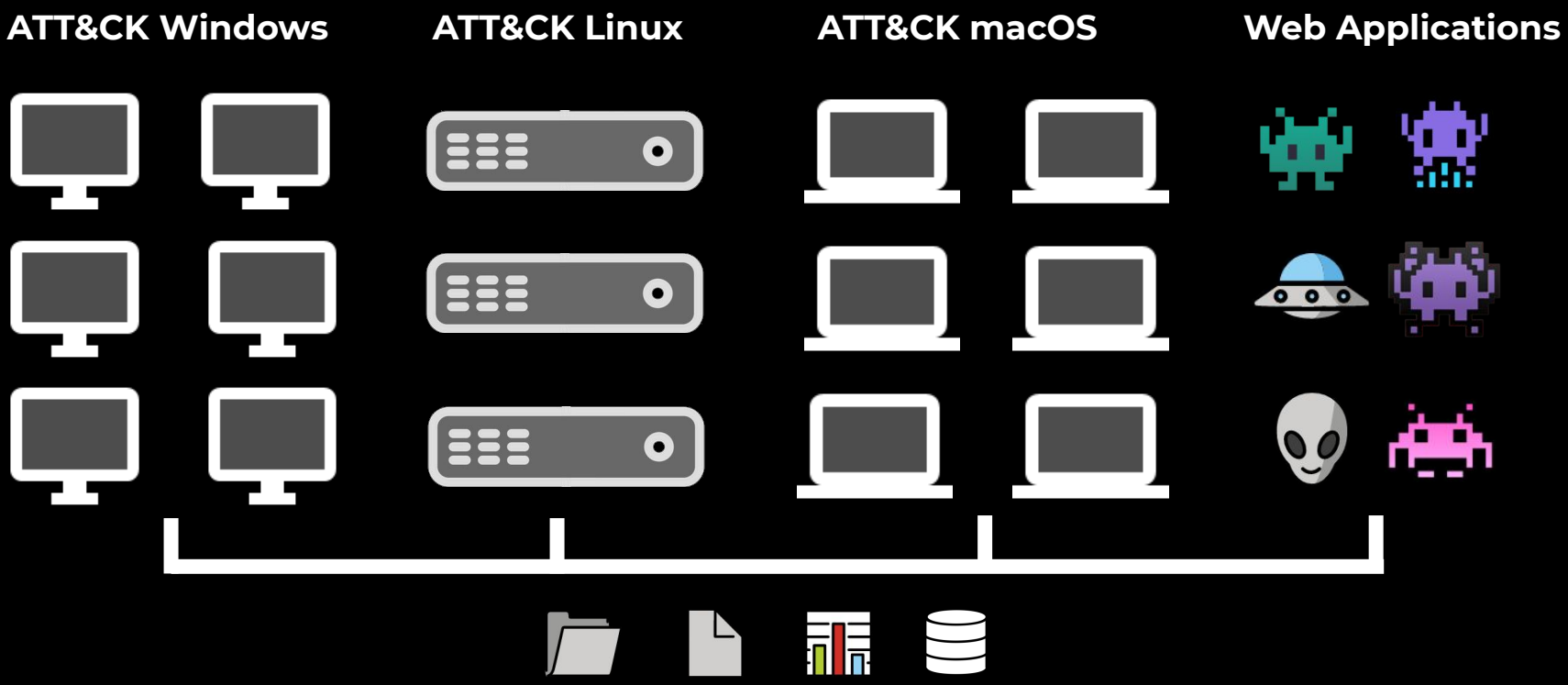
Applying ATT&CK to Web Applications

...

EU ATT&CK Community, May 19th

Securely

Current state of monitoring



ATT&CK Navigator For Web Applications

#fcf3a2	Manual URL mapping
#74c476	Default CRS detection
#c6dbef	Behavior based detection

Securely

Demo

ATT&CK Navigator for Web Applications

Why are custom web applications so hard?

They are SO CUSTOM!?!	Normalize URLs to ATT&CK
Users behave differently	Use statistics to learn normal
They change DAILY!?!	Involve Dev for DevSecOps
Developer triage required	Find similar requests in SIEM
Outsourced applications	Forward logs for correlation

Let’s be in touch

Ruben van Vreeland
Open Source Hacker at Securely

OWASP Slack (OWASP Core Rule Set)
owasp-slack.herokuapp.com

Mail ruben@securely.ai
PGP 3700 C0A7 31F4 54BC 420F
8E30 10D3 EA7B DFFE F5A0

Securely