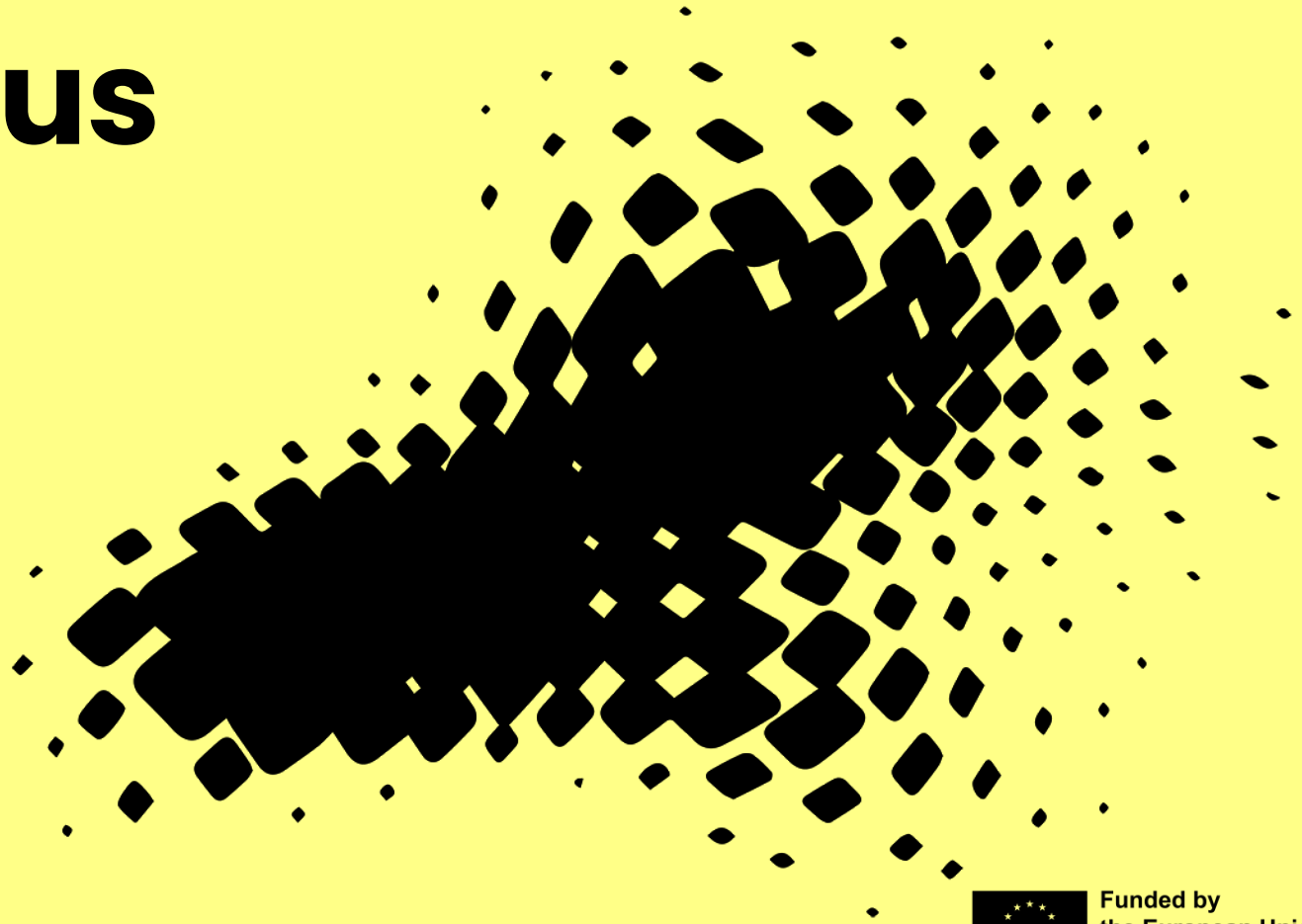
DIGIVISIO

Digivisio ja tietoturvallisuus

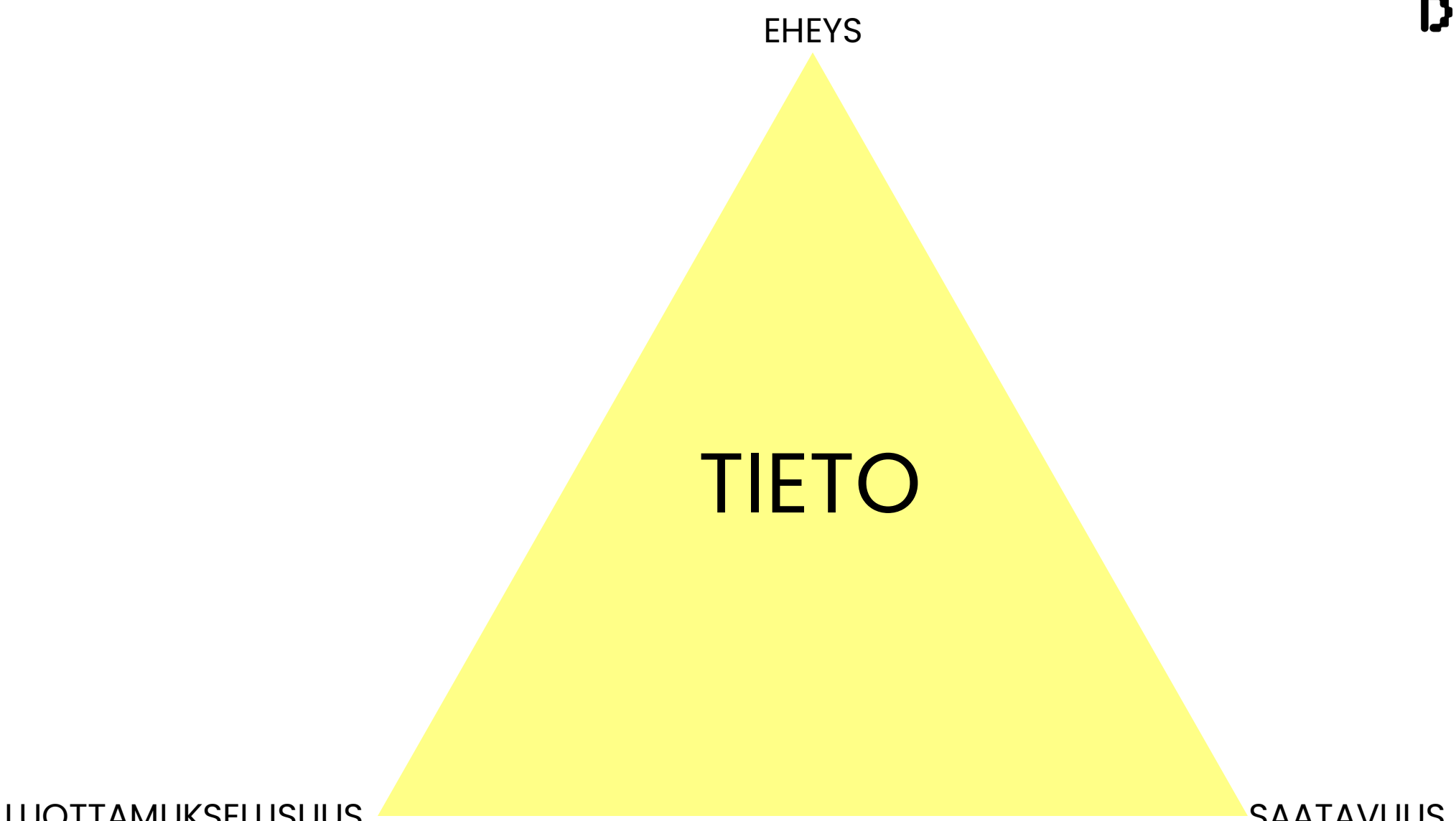
Opin.fi-palvelun tietoturvallisuuden varmistaminen



IT-webinaari 7.6.2024

Funded by the European Union
NextGenerationEU

DIGIVISIO



DIGIVISIO

Uhkien tunnistamisesta

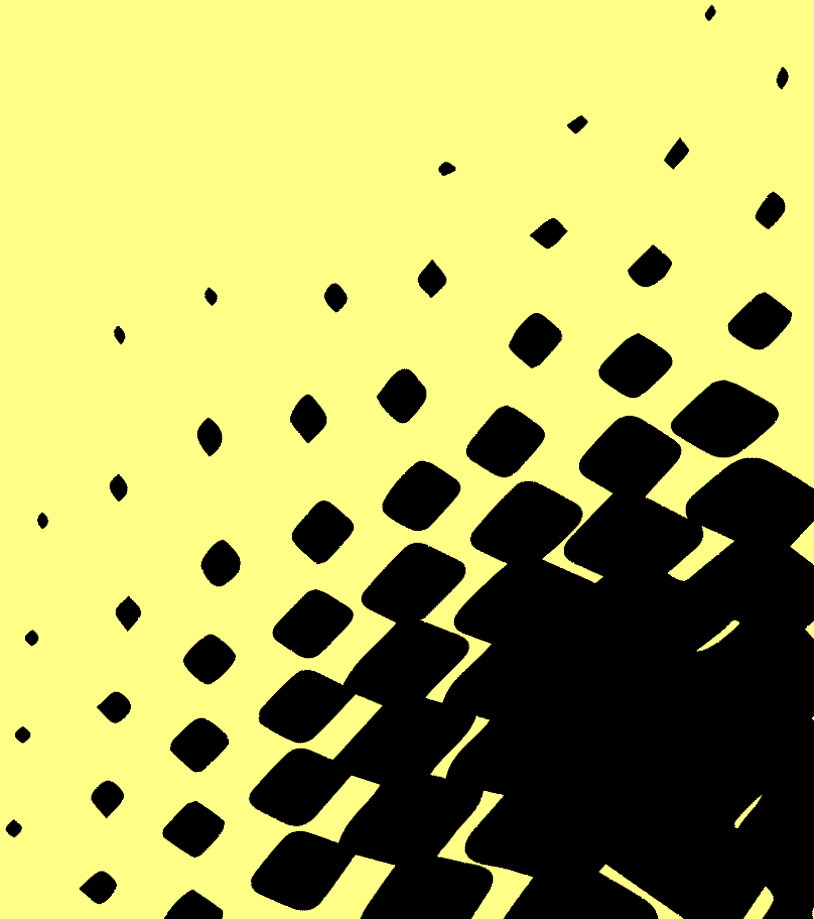
- Uhkamallinnuksen avulla tunnistetaan mahdolliset hyökkäysskenaariot sekä niiden todennäköisyydet ja vaikutukset.
- Uhkamallinnuksessa mallinnettavan ominaisuuden tai järjestelmän parissa työskentelevät henkilöt kirjaavat yhteistyössä uhkamallin, siitä mitä mallinnettavassa kohteessa voi mennä pieleen.

1. Järjestelmän määrittäminen ja suojattavien ominaisuuksien tunnistaminen
2. Uhkien tunnistaminen: Mahdolliset ulkoiset ja sisäiset uhat sekä hyökkäysskenaariot
3. Uhkien arviointi ja lieventämistoimet

Lopputuotoksena saadaan turvallisempi ja luotettavampi palvelu, jonka uhat on saatu lievennyttä ennakoivasti ja kustannustehokkaasti.

DIGIVISIO

Sovelluksen elinkaari ja tietoturvallisuus



DIGIVISIO

Vaatimusmäärittely	• Sovellusta koskevat lait ja standardit luovat pohjan tietoturvavaatimuksille
Suunnittelu	• Sovellus on suunniteltu oletusarvoisesti toimimaan turvallisesti • Teknologiavalinnat
Kehitys	• Turvallisen ohjelmistokehityksen ohjeistus • Turvalliset kehitysympäristöt
Laadunvarmistus ja testaus	• Automatisoitu tietoturvatestaus osana sovelluskehitystä • Ulkoiset tietoturvatestaukset
Julkaisu	• Toistettava ja turvallinen julkaisuprosessi • Turvallinen tuotantoympäristö
Ylläpito	• Sovelluksen monitorointi • Poikkeamien ja korjauspäivitysten hallinta

DIGIVISIO

Tietoturva Opin.fi sovelluskehityksessä

- Digivision sovelluskehittäjiä tuetaan ja koulutetaan tietoturvalliseen työskentelyyn toimittajien ja hankkeen toimesta.
- Sovelluskehityksessä käytettävien kirjastojen ja viitekehysten tietoturvallisuus varmistetaan kiinnitetyillä kirjastoversioilla ja kirjastojen riippuvuuksien haavoittuvuuksia tarkastellaan automaatiotyökalujen avulla CI-putkessa.
- Opin.fi:n käyttöliittymään ja rajapintoihin suoritetaan viikoittain automaattista dynaamista tietoturvatestausta ZAP työkalulla.
- Staatista testausta käytetään koodinlaadun varmistamiseen osana kehitystyötä.
- Pohjaimaget skannataan Trivy-skannerilla haavoittuvuuksien tunnistamiseksi CI-putkessa.

Lisäksi palveluun suoritetaan ulkoisia tietoturvatestauksia pilvialustaan ja web-käyttöliittymään ja integraatioihin.

DIGIVISIO

Tietoturva Opin.fi sovelluskehityksessä

Dynaaminen testaus

- ZAP-työkalulla ajetaan viikoittain testitapauksia Opin.fi:n käyttöliittymää ja rajapintoja vasten.

- Aktiivisella skannauksella ZAP pyrkii löytämään haavoittuvuuksia tekemällä mahdollisesti haitallisia kutsuja rajapinnoille ja syöttämällä mahdollisesti haitallista ja odottamatonta syötettä tekstikenttiin.

- ZAP:lla tehtäviä löydöksiä voivat olla:
    - Injektiot
    - XSS-haavoittuvuudet
    - Sensitiivisen tiedon vuotaminen
    - Puutteet HTTP-otsakkeissa

- ZAP: https://www.zaproxy.org & ZAP alerts: https://www.zaproxy.org/docs/alerts/

DIGIVISIO

Ulkoinen tietoturvatestaus

Tietoturvatestaukset suoritetaan alan yleisiä tunnettuja viitekehyksiä ja standardeja vasten

Opin.fi käyttöliittymä ja integraatiot

- OWASP top 10 – Yleisimmät verkkosovellusten haavoittuvuudet: https://owasp.org/www-project-top-ten/
- OWASP top 10 API – Yleisimmät rajapintojen haavoittuvuudet: https://owasp.org/API-Security/editions/2023/en/0x11-t10/
- OWASP Application Security Verification Standard (ASVS) Level 2 - Avoin sovellusturvallisuuden standardi: https://owasp.org/www-project-application-security-verification-standard/

AWS

- AWS Foundational Security Best Practices: https://docs.aws.amazon.com/securityhub/latest/userguide/fsbp-standard.html
- CIS Benchmarks - Amazon Web Services Foundations: https://www.cisecurity.org/benchmark/amazon_web_services

DIGIVISIO

Ulkoinen tietoturvatestauksen hyödyt

Opin.fi käyttöliittymä ja integraatiot

- Käyttöliittymän ja integraatioiden testauksella varmistetaan, että toteutus ja sen turvamekanismit ja -kontrollit ovat asianmukaisesti toteutettuja, ja ne toimivat kuten on suunniteltu.
- Omaksumalla testaukseen hyökkääjän näkökulma ja toteuttamalla testaus white box-menetelmällä varmistetaan, että testaus tehdään reaalimaailman uhkatoimijoiden metodeja noudattaen, mutta tehokkaammin, kun testaajalla on käytössään laajemmat taustatiedot, kuten lähdekoodit. Lopputuloksena järjestelmä on paremmin suojattu reaalimaailman uhkia ja uhkatoimijoita vastaan.

AWS

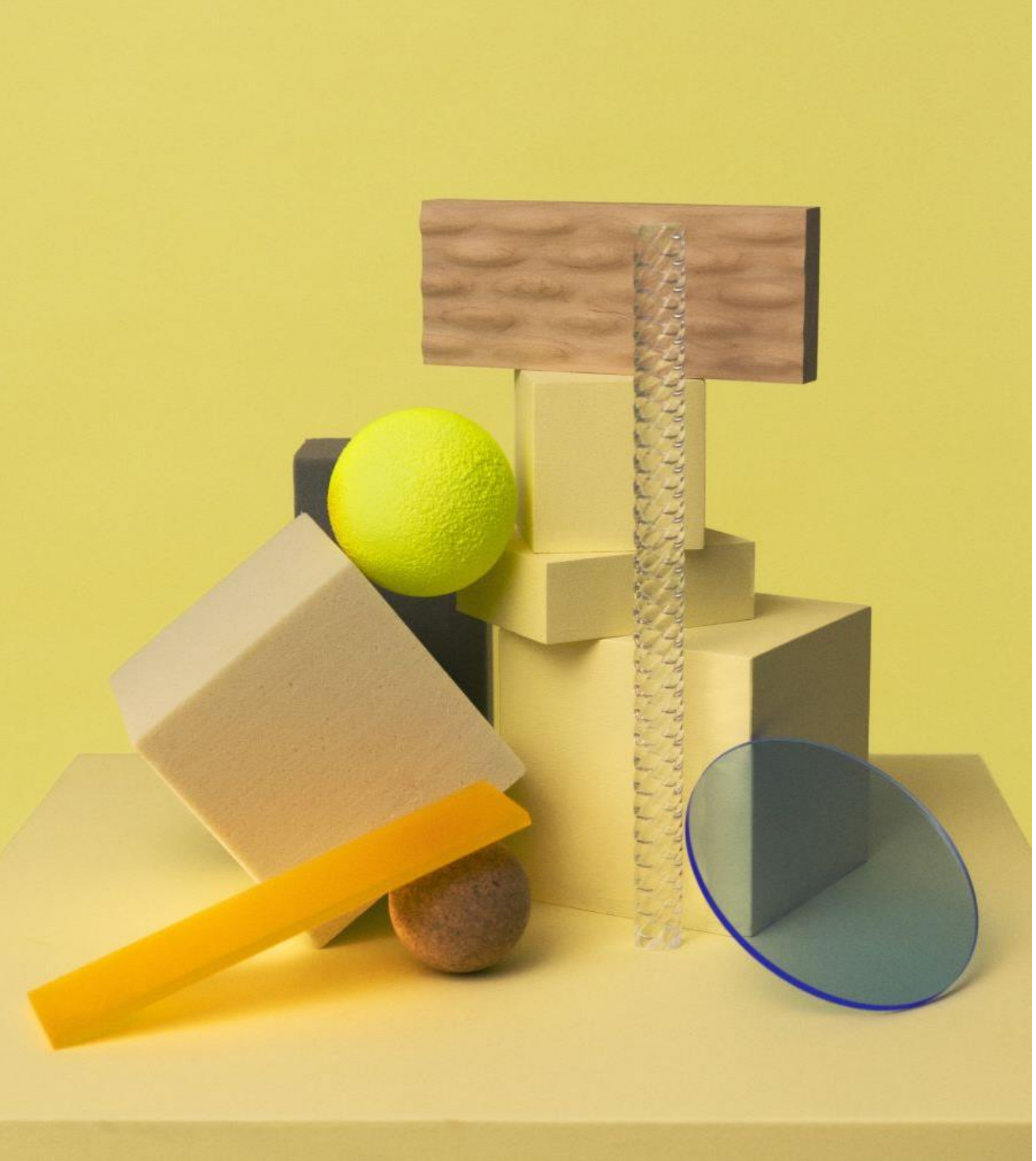
- Pilviympäristön arvioinnilla ja testauksella varmistetaan, että toteutus on tietoturvallinen, vikasietoinen, skaalautuva ja noudattaa parhaita käytäntöjä pilven hallinnan ja vaatimusten-mukaisuuden osalta.
- Testauksen tuloksena tulee todennettua, että pilviympäristön toteutus kestää mahdollisia hyökkäysyrityksiä, ja mahdollisen murron tapahtuessa, hyökkääjän mahdollisuudet liikkua ja edetä ympäristössä ovat mahdollisimman tiukasti rajattuja. Lisäksi varmistetaan, että mahdolliset yritykset edetä havainnoidaan.

DIGIVISIO

Tietoturva Opin.fi sovelluskehityksessä

Dynaaminen testaus

- Digivision sovelluskehittäjiä tuetaan ja koulutetaan tietoturvalliseen työskentelyyn toimittajien ja hankkeen toimesta.
- Sovelluskehityksessä käytettävien kirjastojen ja viitekehysten tietoturvallisuus varmistetaan kiinnitetyillä kirjastoversioilla ja kirjastojen riippuvuuksien haavoittuvuuksia tarkastellaan automaatiotyökalujen avulla CI-putkessa.
- Opin.fi:n käyttöliittymään ja rajapintoihin suoritetaan viikoittain automaattista dynaamista tietoturvatestausta ZAP työkalulla.
- Staatista testausta käytetään koodinlaadun varmistamiseen osana kehitystyötä.
- Pohjaimaget skannataan Trivy-skannerilla haavoittuvuuksien tunnistamiseksi CI-putkessa.



DIGIVISIO

Tietoturva osana Opin.fi:n sovelluskehitystä

- Tekstipalsta Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed fermentum a turpis vel volutpat. Nullam in luctus est.

- Phasellus congue sagittis consectetur. Class aptent taciti sociosqu.

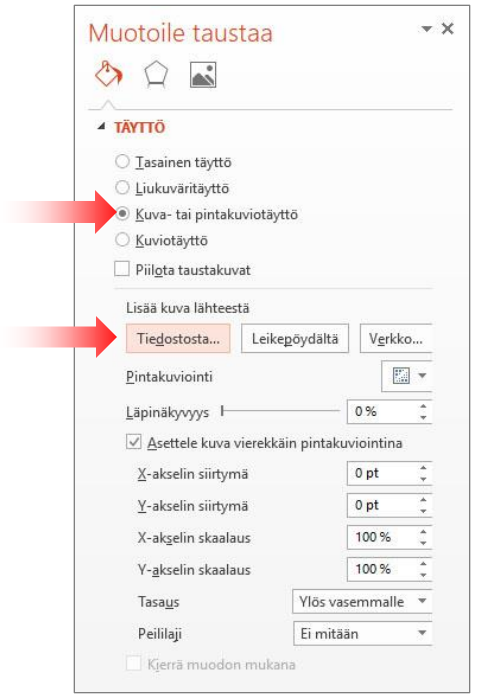
- Morbi faucibus ipsum dui, sit amet aliquam justo mollis congue.

Kuvan käyttäminen taustalla

1. Valitse Rakenne-välilehden Tausta-ryhmästä Taustatyylit ja valitse ***Muotoile taustaa***.

2. Valitse ***Täyttö*** ja valitse sitten ***Kuva tai pintakuviotäyttö***.

3. Valitse Tiedosto, etsi lisättävä kuva ja kaksoisnapsauta sitä.



DIGIVISIO

Otsikkorivi yksi, otsikkorivi kaksi

Alaotsikko, esittäjän nimi, päivämäärä tms.

Funded by the European Union
NextGenerationEU

DIGIVISIO

Otsikko

- Yksi tekstipalsta Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed fermentum a turpis vel volutpat. Nullam in luctus est.

- Phasellus congue sagittis consectetur. Class aptent taciti sociosqu.

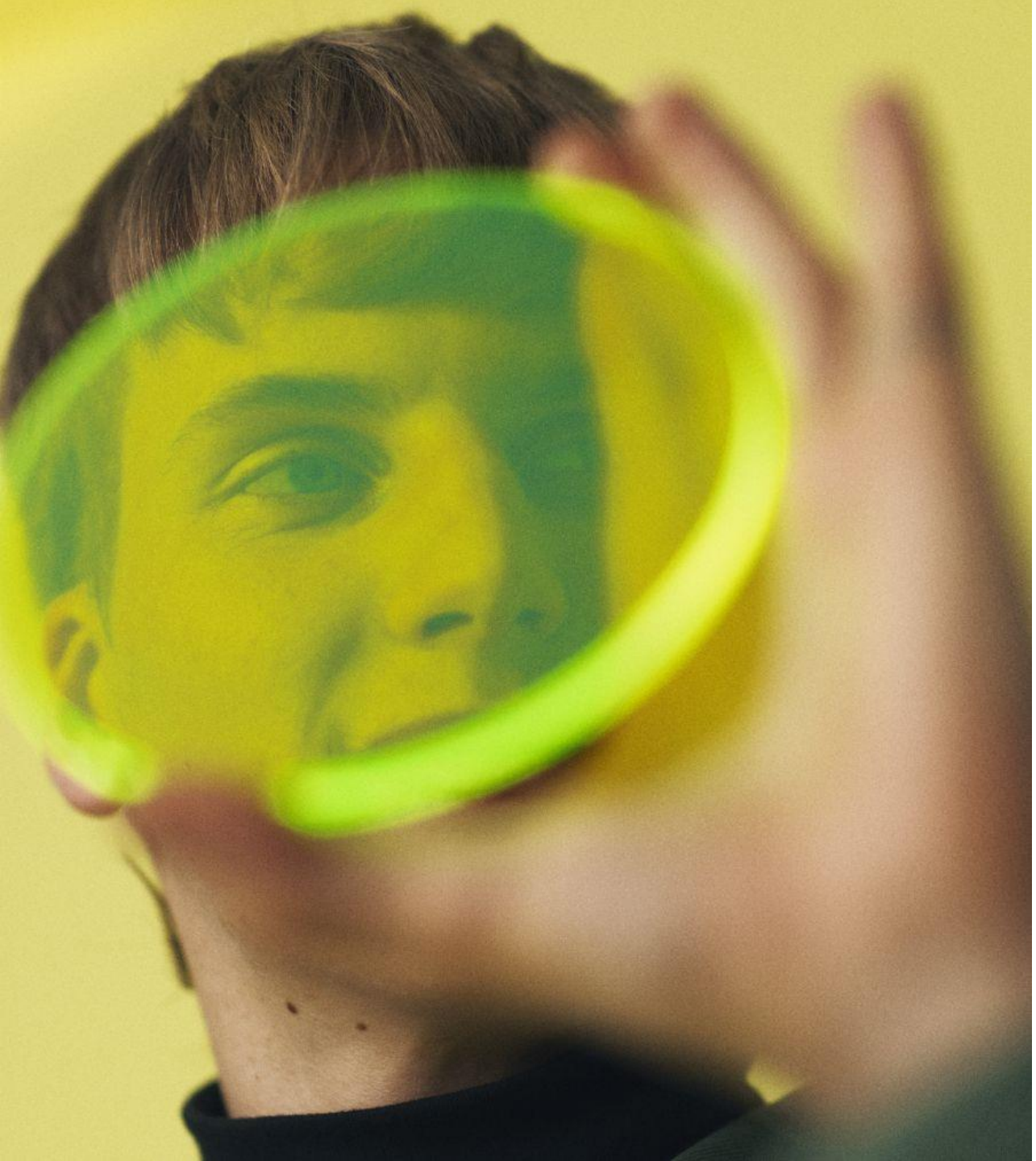
- Morbi faucibus ipsum dui, sit amet aliquam justo mollis congue. Aenean pulvinar tellus metus, et efficitur purus facilisis eu.

- Praesent est nunc, consectetur id ornare ut, pellenYksi tekstipalsta Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Otsikko

- Yksi tekstipalsta Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed fermentum a turpis vel volutpat. Nullam in luctus est.
- Phasellus congue sagittis consectetur. Class aptent taciti sociosqu.
- Morbi faucibus ipsum dui, sit amet ali-quam justo mollis congue. Aenean pul vinar tellus metus, et efficitur purus facilisis eu. Nullam in luctus est.
- Praesent est nunc, consectetur id ornare ut, pellenYksi tekstipalsta Lorem ipsum dolor sit amet, consectetur adip-iscing elit.
- Sed fermentum a turpis vel volutpat. Nullam in luctus est.

DIGIVISIO



DIGIVISIO

Otsikko

- Tekstipalsta Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed fermentum a turpis vel volutpat. Nullam in luctus est.

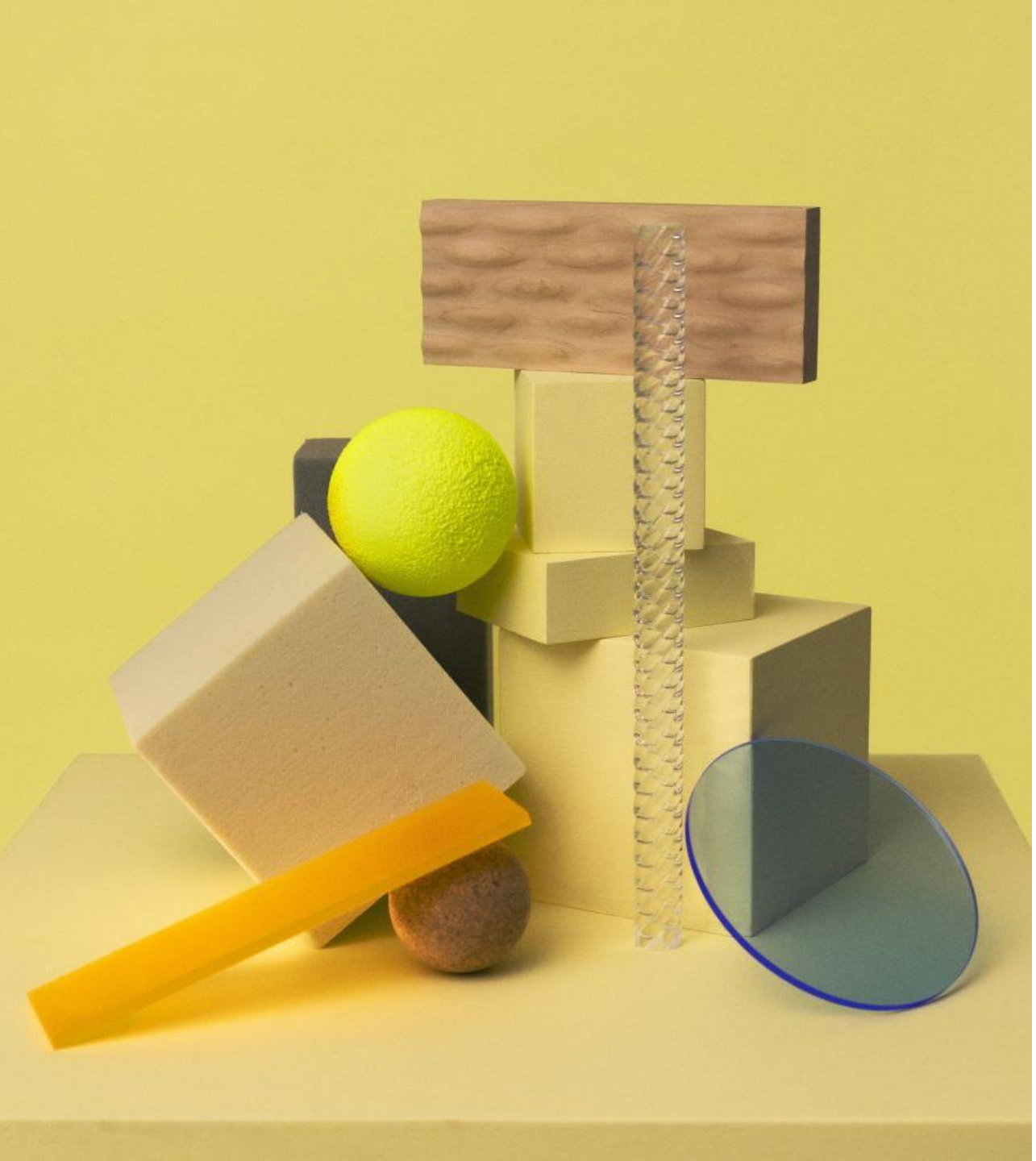
- Phasellus congue sagittis consectetur. Class aptent taciti sociosqu.

- Morbi faucibus ipsum dui, sit amet aliquam justo mollis congue.

DIGIVISIO

Otsikko

- Tekstipalsta Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed fermentum a turpis vel volutpat. Nullam in luctus est.
- Phasellus congue sagittis consectetur. Class aptent taciti sociosqu.
- Morbi faucibus ipsum dui, sit amet aliquam justo mollis congue.



DIGIVISIO

Otsikko

- Tekstipalsta Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed fermentum a turpis vel volutpat. Nullam in luctus est.
- Phasellus congue sagittis consectetur. Class aptent taciti sociosqu.
- Morbi faucibus ipsum dui, sit amet aliquam justo mollis congue.

DIGIVISIO

Otsikko

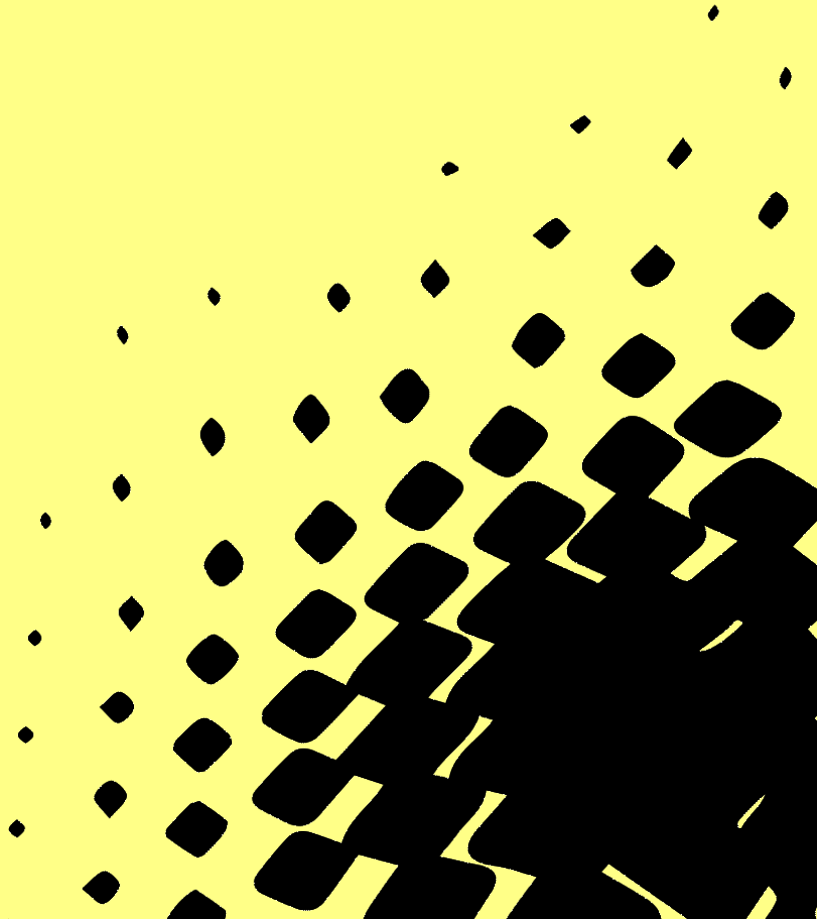
- Tekstipalsta Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed fermentum a turpis vel volutpat. Nullam in luctus est.

- Phasellus congue sagittis consectetur. Class aptent taciti sociosqu.

- Morbi faucibus ipsum dui, sit amet aliquam justo mollis congue.

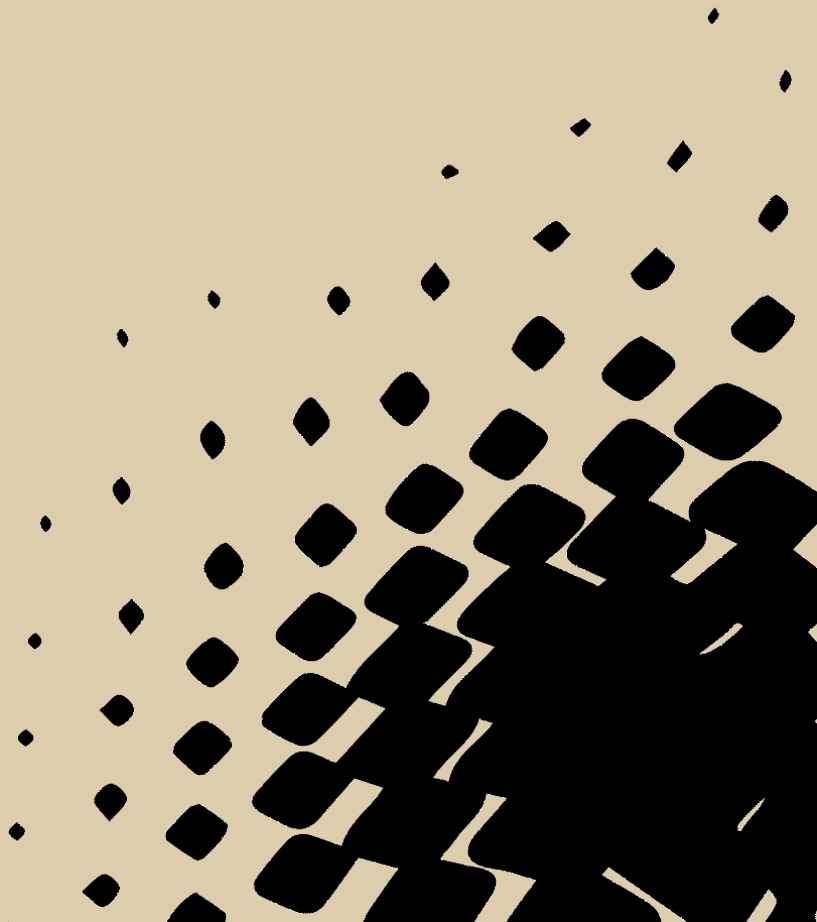
DIGIVISIO

Otsikko



DIGIVISIO

Väliotsikko rivi yksi, väliotsikko rivi kaksi, väliotsikko rivi kolme



DIGIVISIO

DIGIVISIO

DIGIVISIO

Kiitos!

Yhteystiedot
tähän

Funded by
the European Union
NextGenerationEU