
ONLINE CHILD SEXUAL EXPLOITATION
Threats, Risks, and Responses

INTRODUCTION

Personal Introduction

Background and experience

- NCMEC Child Victim Identification Program
- INTERPOL Crimes Against Children
- European Union Agency for Law Enforcement Training (CEPOL)
- Blindspot Collaborative, Consultant (Kindred Tech, Childlight, Arina AG)

ROADMAP AND HOUSEKEEPING

Roadmap

- Overview of OCSE
- Threat landscape of OCSE
- Call to action

Vocabulary and terminology

Child sexual abuse material = CSAM

Luxembourg Guidelines

OVERVIEW OF ONLINE CHILD SEXUAL EXPLOITATION

What is online child sexual exploitation?
What is child sexual abuse material?

OVERVIEW OF ONLINE CHILD SEXUAL EXPLOITATION

What is victim identification?

The process, strategies, and best practices by which children depicted in CSAM are identified, located, and safeguarded.

- Process: proactive, iterative, and de-conflicted.

- Strategies: leveraging technology, knowing the target, going local.

- Best Practices: collaborative, sharing, and child/victim-centric

OVERVIEW OF ONLINE CHILD SEXUAL EXPLOITATION

General/inherent challenges in OCSE

- Volume of CSAM
- Access to data
- Silos (confidentiality) and need-to-know feedback loops
- Anonymity/secrecy
- Reactive vs. proactive/preventative stance
- Lack of awareness (public/private sector)

THREAT LANDSCAPE OF ONLINE CHILD SEXUAL EXPLOITATION

Generative AI/deep fake CSAM

Description

Harms/Risks

- Re-victimization of depicted victims
- Further exposure to “apparent” CSAM
- (Offender) escalation pathways

THREAT LANDSCAPE OF ONLINE CHILD SEXUAL EXPLOITATION

CSAM as Cybersecurity Risk

Description

- The use of corporate devices to access CSAM
- Human insider risk: the threat posed by individuals within an organization—such as employees, contractors, or partners— whose behavior creates serious security vulnerabilities

““Insiders—employees, contractors, vendors, or third-party personnel—offer access, deniability, and efficiency. And critically, they are often targeted not because of ideology, but because of leverage.”

THREAT LANDSCAPE OF ONLINE CHILD SEXUAL EXPLOITATION

CSAM as Cybersecurity Risk

Harms/Risks

- Targets for extortion and/or blackmail
- Data breaches/introduction of malware or spyware
- Reputational harm

THREAT LANDSCAPE OF ONLINE CHILD SEXUAL EXPLOITATION

Sadistic Online Extortion

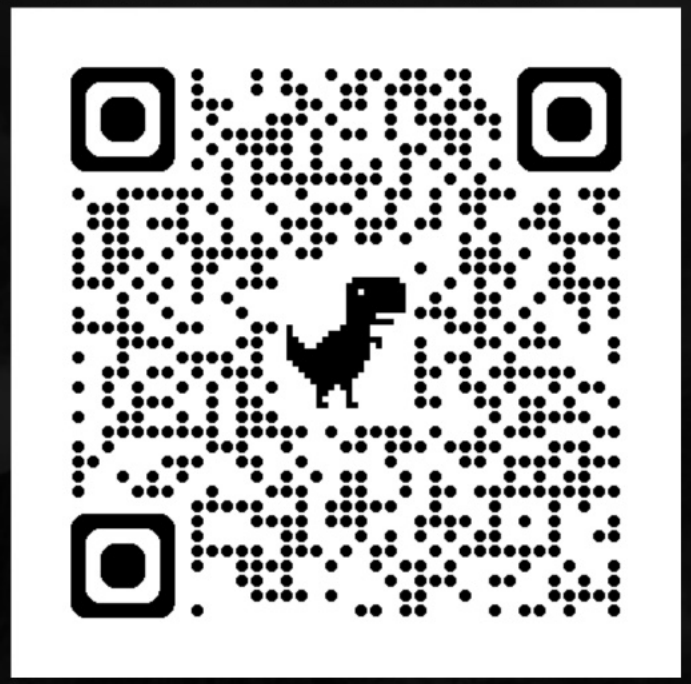
Description

- Coercion, manipulation, & blackmail
- Self-harm (suicide), animal cruelty, sexual acts, physical violence
- Noteriety, sadistic gratification, reputation, sense of power

THREAT LANDSCAPE OF ONLINE CHILD SEXUAL EXPLOITATION

Sadistic Online Extortion

Description



Harms/Risks

- Real world violence
- Property damage
- Extremism ties
- Escalation

CALL TO ACTION

Why does this matter? Why should I care?

1. A response to OCSE offers an opportunity to explore and push technical boundaries

- OCSE itself pushes technical boundaries
- (Mis)use of products and platforms
- INTERPOL DevOps - KindredTech

CALL TO ACTION

Why does this matter? Why should I care?

2. A response to OCSE offers a corporate de-risking & safer-by-design opportunity

- Passive - NetClean
- Active - Grok/xAI

CALL TO ACTION

Why does this matter? Why should I care?

3. A response to OCSE is an opportunity to contribute to human safety and well-being


QUESTIONS
THANK YOU FOR YOUR ATTENTION