Achievement: Unlocked

Designing a Compelling Security Awareness Program

Bob Rudis (@hrbrmstr)
Liberty Mutual

The Goal:

Create an awareness program that is:

The Goal:

Create an awareness program that is:

- Creative

The Goal:

Create an awareness program that is:

- Creative
- Compelling

The Goal:

Create an awareness program that is:

- Creative
- Compelling
- Continuous

The Goal:

Create an awareness program that is:

- Creative
- Compelling
- Continuous
- Customized

SECURITY AWARENESS

SECURITY AWARENESS HD

WHY WOULD A FLY EVER LAND ON SOMETHING THAT LOOKS LIKE THAT?

MICE SHOULD BE ASHAMED
OF GETTING CAUGHT OFF GUARD BY
SOMETHING SO OBVIOUS.

COME ON BEARS, HOW CAN YOU POSSIBLY LET YOURSELF GET STUCK IN THIS?

http://buttersafe.com/2011/01/27/traps/

1.

2.

3.

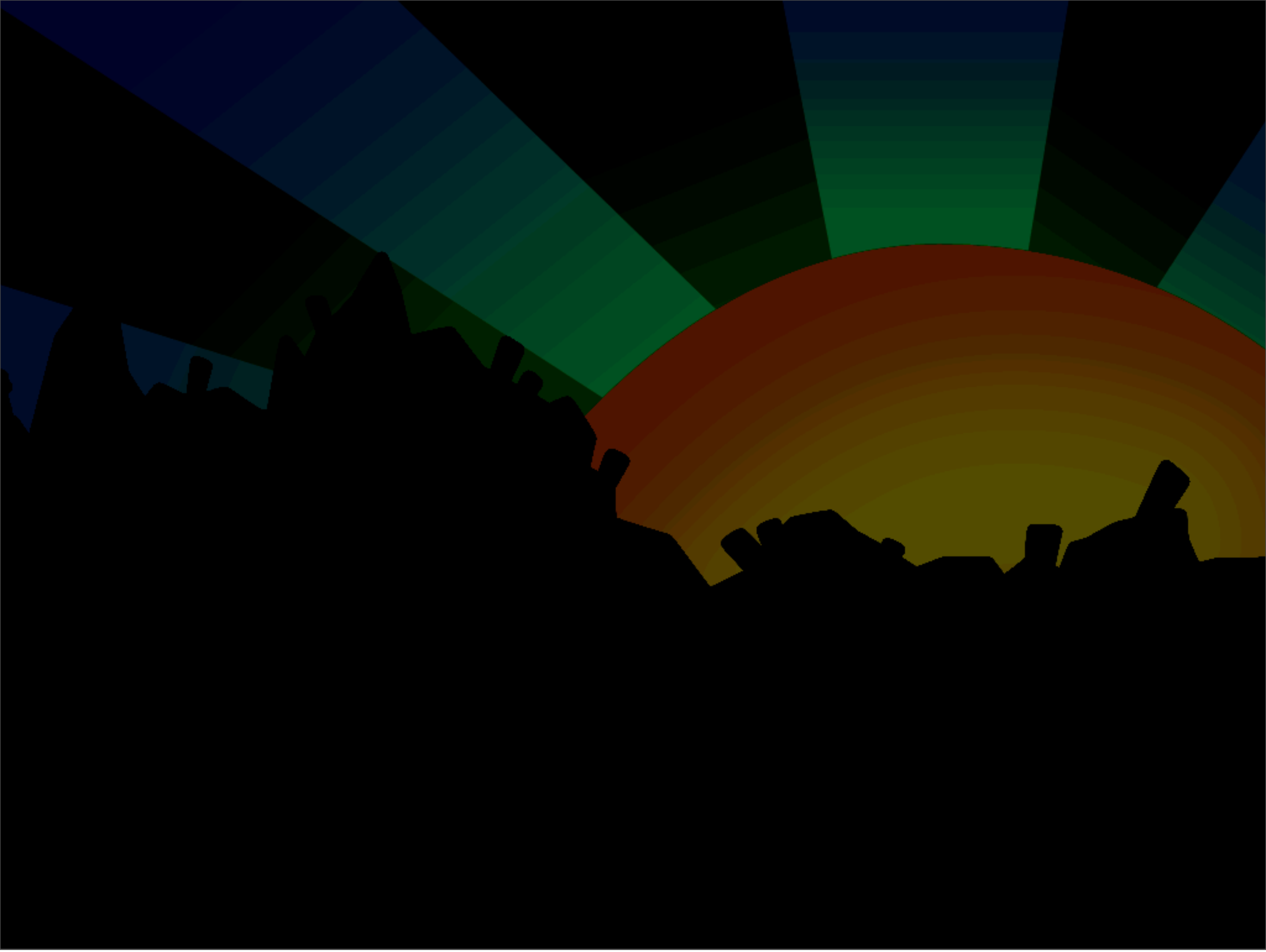
4.

1. CREATIVE

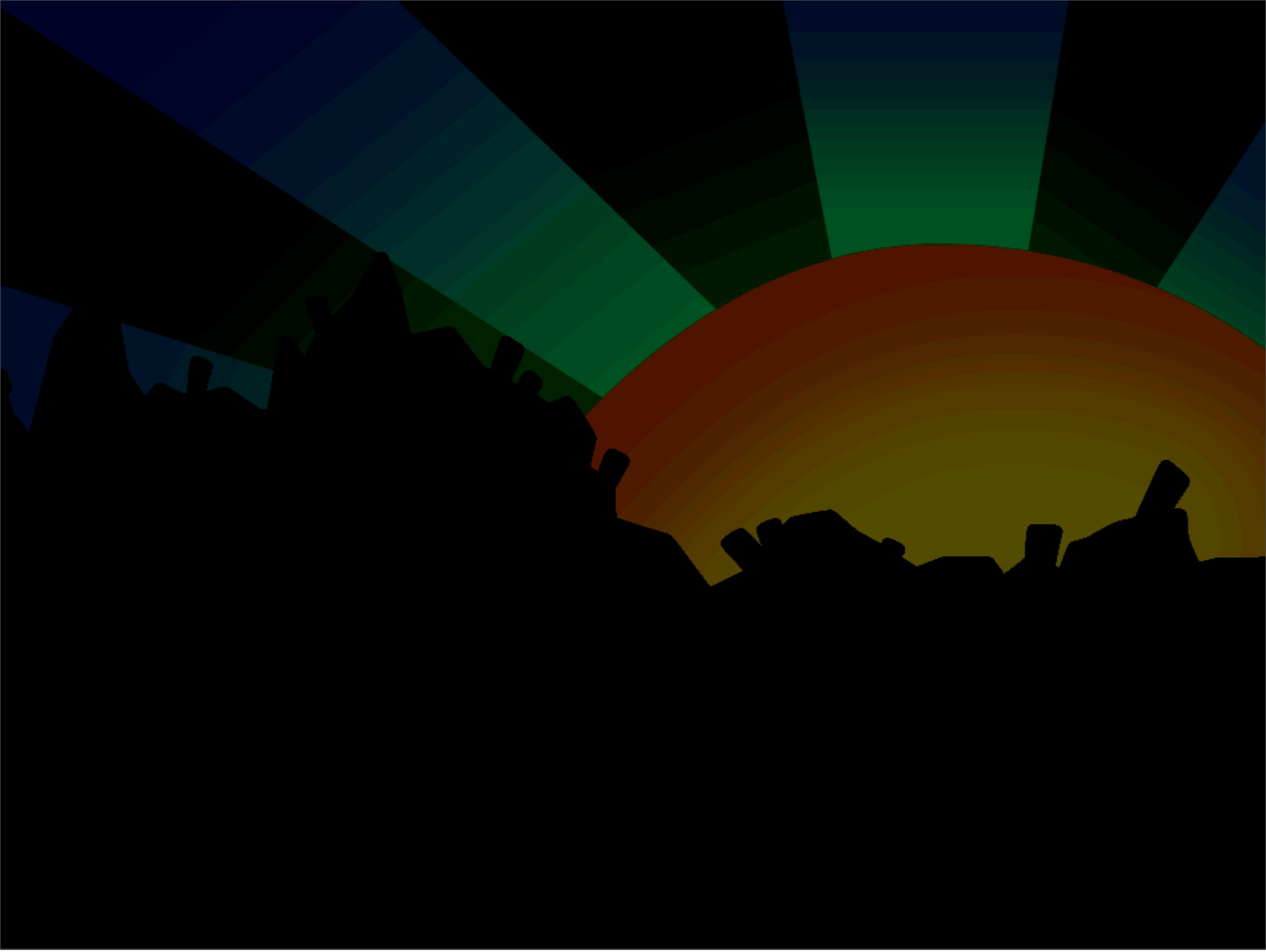
2.

3.

4.



You
Tube



Computer Based Training (CBT)

Computer Based Training (CBT)

== NECESSARY EVIL

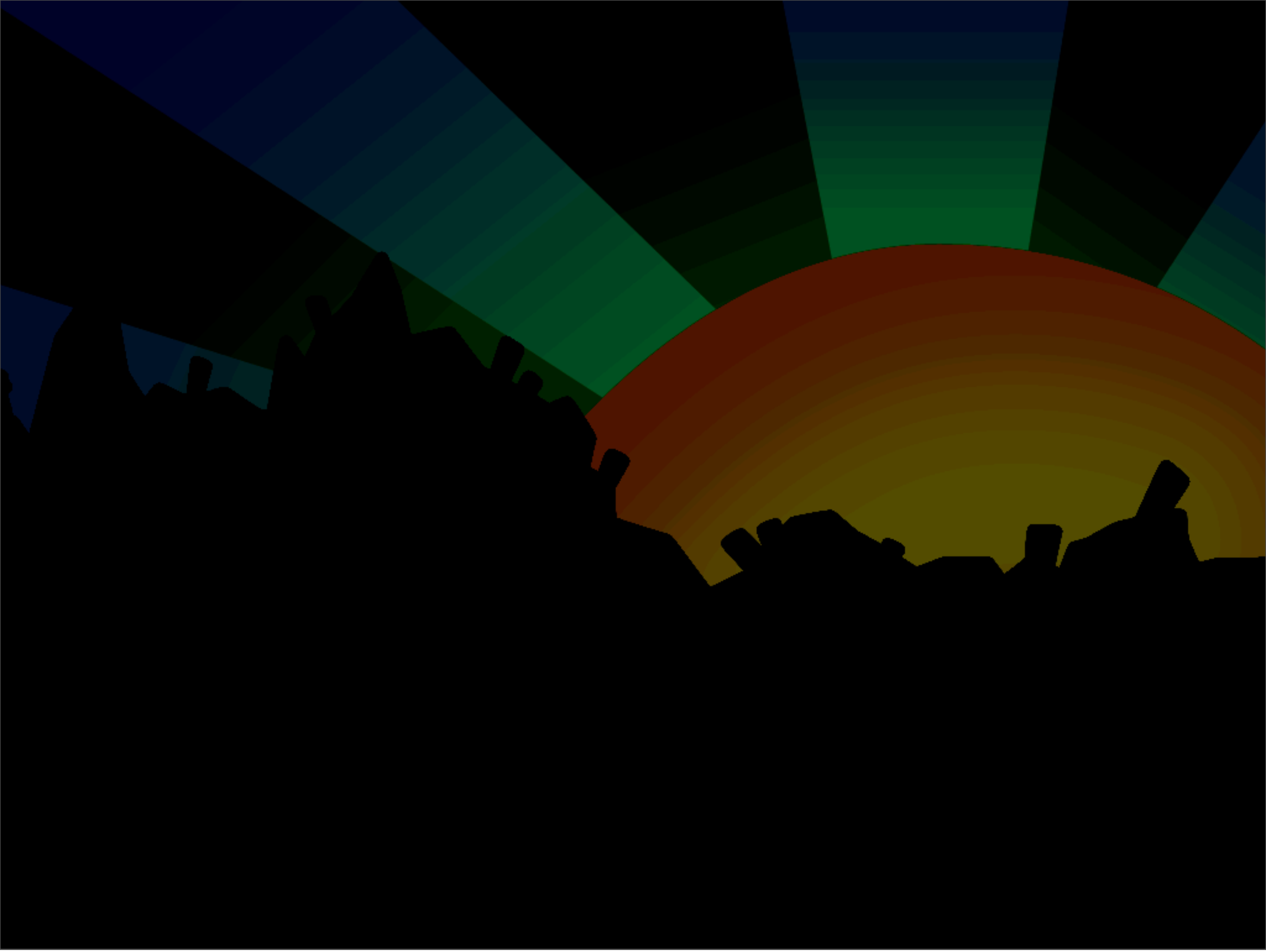
Computer Based Training (CBT)

== NECESSARY EVIL

☑ Achievement Unlocked

Make It Quick

Ditch The Stock



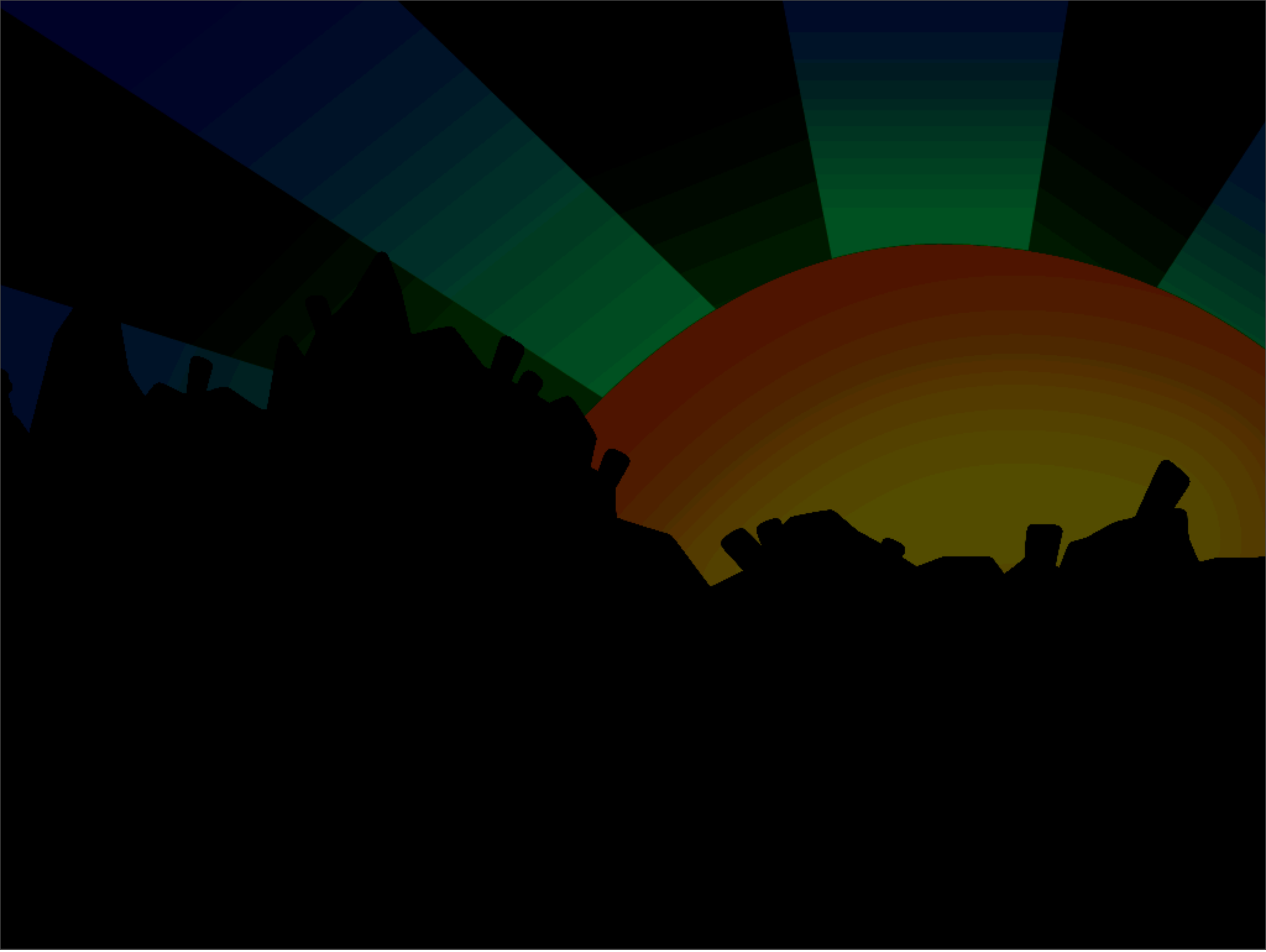
www.shutterstock.com

www.shutterstock.com · 18558820

www.shutterstock.com · 46793158

www.shutterstock.com · 18558820

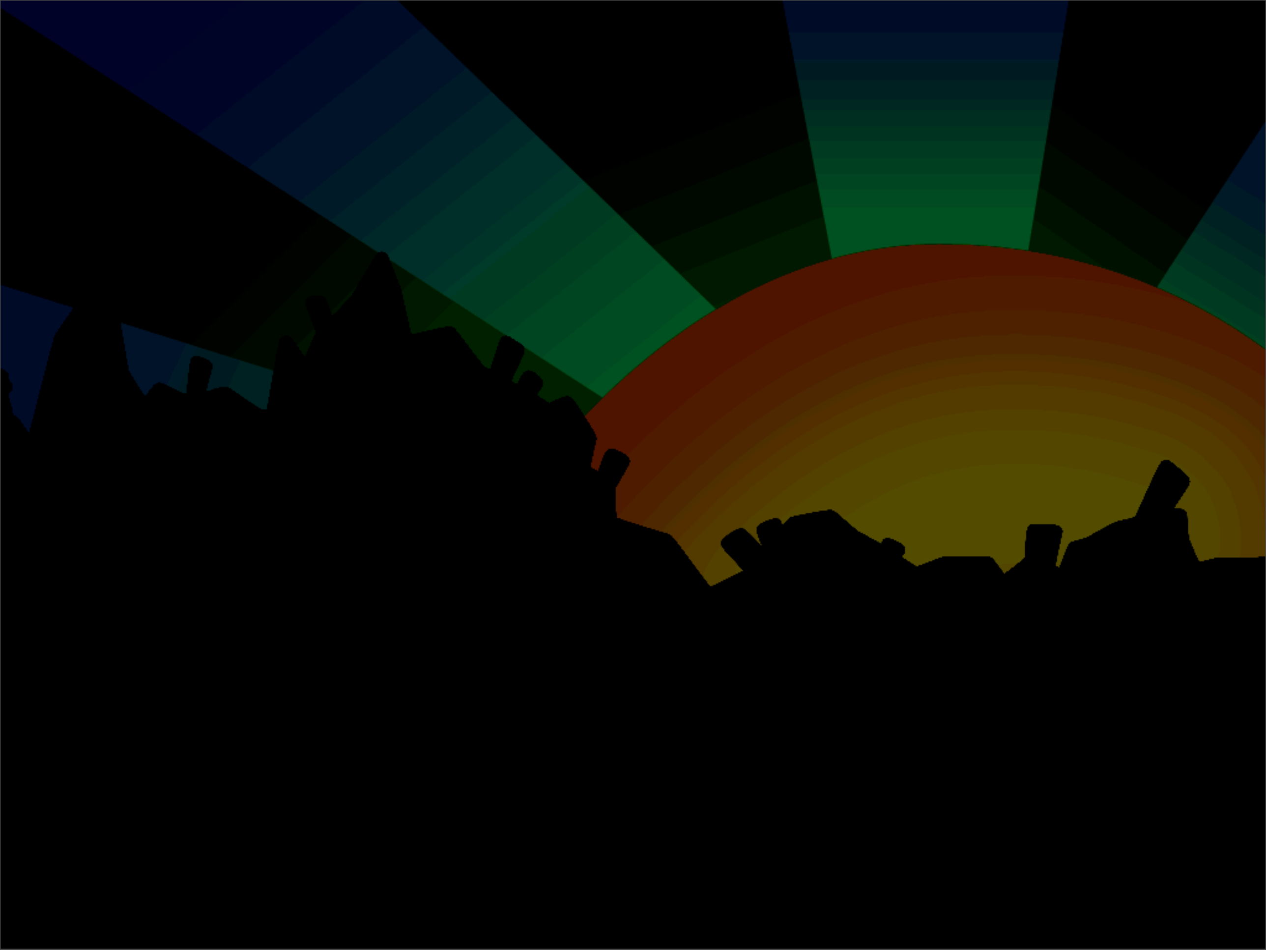
www.shutterstock.com · 46793158



@MaximumYin

Everyone used in training materials had 1-10 direct inquiries

Lose The Slides



Information Security Policy

Data Classification

Handling NPPI Data

https://wiki.internet2.edu/confluence/pages/viewpageattachments.action?pageId=17854

Introduction

- All administrative data and information are University resources. They are owned by the University and are shared as appropriate to meet the needs of the University and its various constituencies.
- This University maintains administrative computing resources, including data and information, that are essential to performing University business. These are University assets over which the University has both rights and obligations to manage, secure, protect, and control.

Reasons for this Policy

The reason for this policy is to provide procedures for accessing data, and to protect the data from unauthorized access, misuse or damage to computer assets.

The goals for these policy statements are as follows:

- To assure employees access to relevant data they need to conduct University business;
- To prevent unauthorized access to systems, data, facilities, and networks; and
- To prevent any misuse of, or damage to, computer assets or data.

Scope

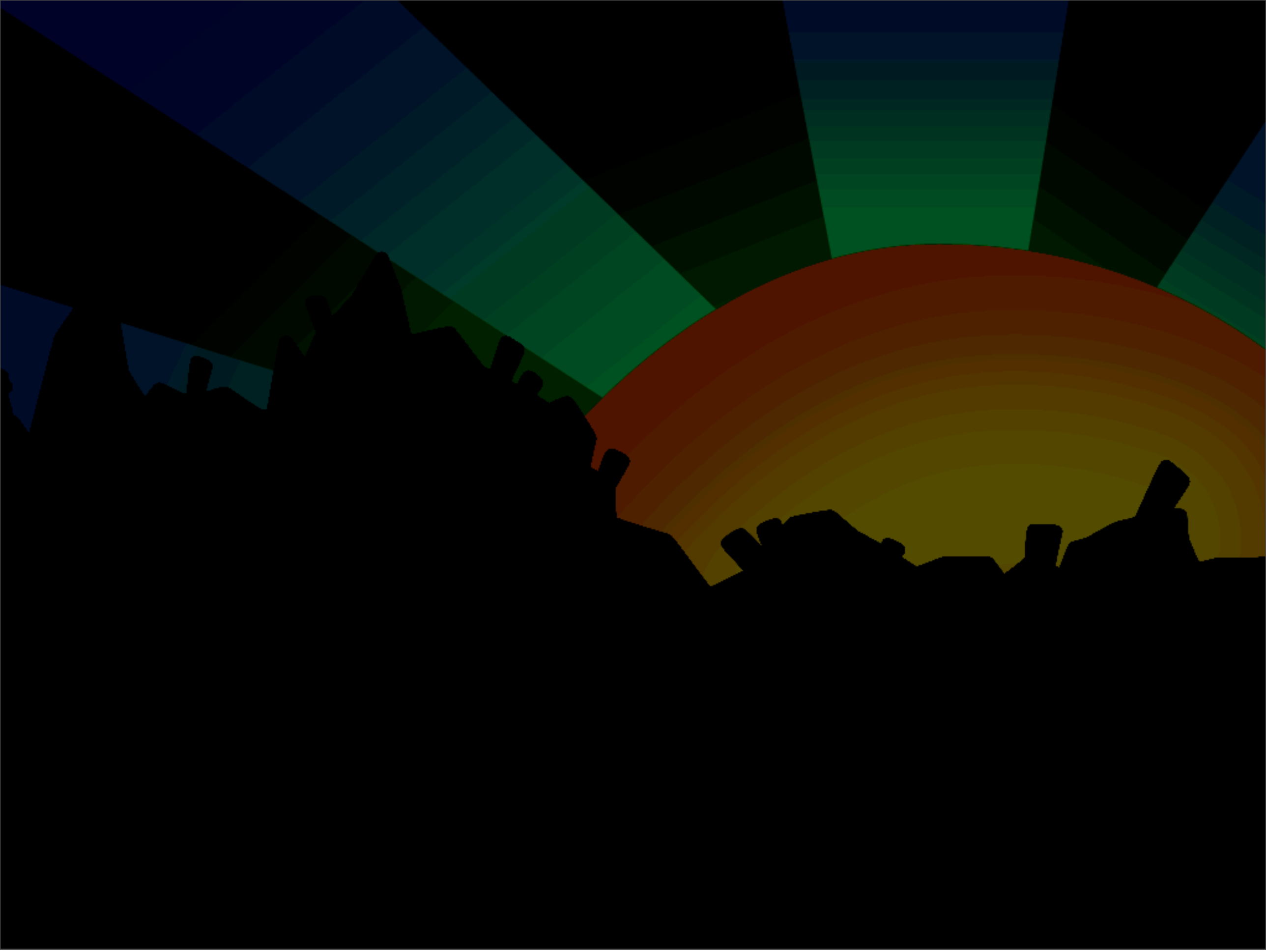
- This policy applies to administrative computing resources regardless of where they reside. It requires that members of the University

Who Should Know This Policy?

- President
- Provost
- All others with access to University IT Resources
- Business Office Staff

https://wiki.internet2.edu/confluence/pages/viewpageattachments.action?pageId=17854

https://wiki.internet2.edu/con ments.action?pageId=17854



Confidential
Internal
Public
Restricted
Classification Match Game
INFORMATION SECURITY
Annual Report
Annual Report

N.P.P.I. GAME
Driver's License Number
NEW YORK STATE
ENHANCED
DRIVER LICENSE
ID: 012 345 678
CLASS D
DOCUMENT
SAMPLE, LICENSE
2345 ANYPLACE AVE
ANYTOWN NY 12345
DOB: 06-09-85
Need more information about NPPI? Click here

Over 10,000 (25%) Played
At Least Once

Over 10,000 (25%) Played
At Least Once

One Person Played *over 15 times*

1. CREATIVE

2.

3.

4.

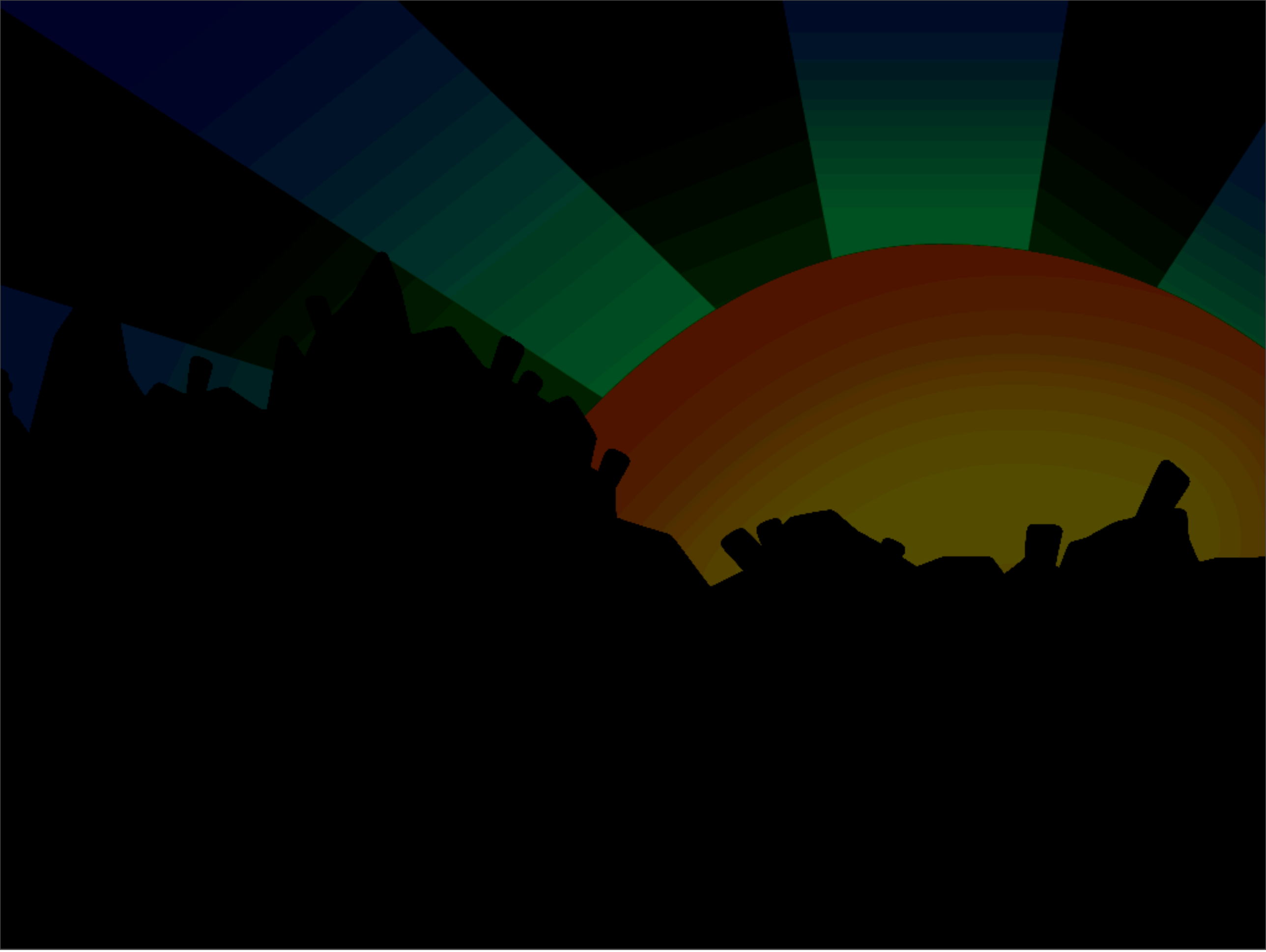
1. CREATIVE

2. COMPELLING

3.

4.

Start The Presses



INFORMATION SECURITY

Recognize Social Engineering

What is Social Engineering?

Social Engineering is an attempt to access sensitive or private information through e-mail or telephone communication. Social Engineers are "people hackers" who will prey on traits of human nature, such as fear, politeness, or helpfulness, to trick people into revealing sensitive information or do something that weakens security or is against policy.

How Can You Recognize It?

If something doesn't feel right, it could be a clue. Often, someone attempting a Social Engineering attack will:

- avoid providing his/her contact information
- seem to be in an extreme rush for information
- drop a lot of names to establish credibility or authority
- pressure you for information
- make small mistakes, such as mispronouncing na
- ask peculiar questions about things they should already know
- instruct you to visit an external Web site or enter computer commands

INFORMATION SECURITY

Resist Social Engineering Attacks!

DON'T:

- disclose personal or company information without verifying the identity of the recipient and whether they are authorized to have that information. *(Use a publicly available source to verify contact information. Keep in mind that caller ID is NOT a reliable means of verifying a caller.)*
- share your password.

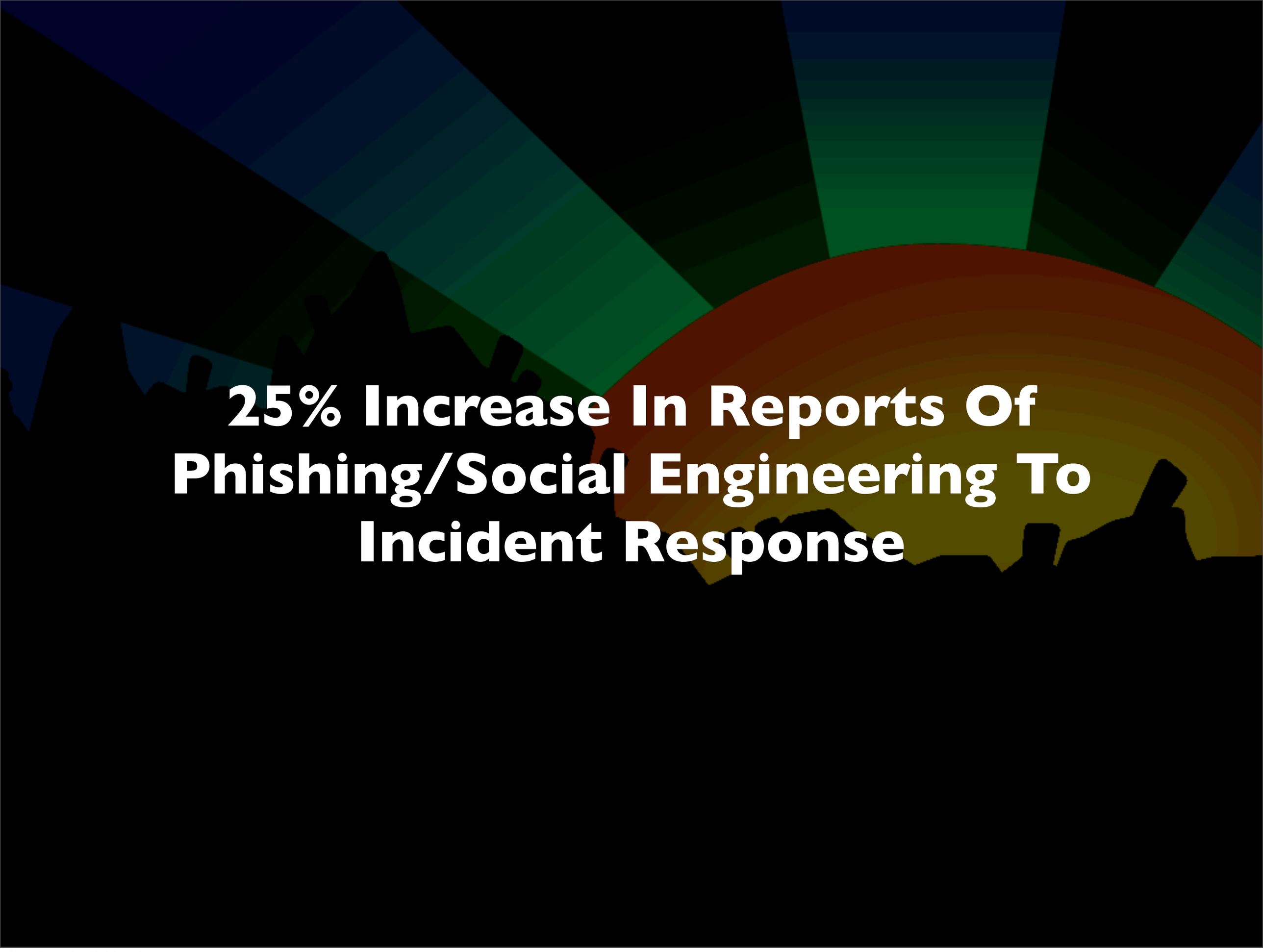
BE WARY:

- of unsolicited phone calls or email messages from individuals asking about employees or other internal information.
- of individuals who ask you to visit external Web sites, download or execute files, or change computer system settings.
- of telephone surveys. *(Even better, decline to participate.)*

DO:

- trust your instincts.
- learn and understand information security policies.
- refer a suspicious call or e-mail to your manager or supervisor.
- ask questions if a request seems suspicious.

Liberty Mutual


25% Increase In Reports Of
Phishing/Social Engineering To
Incident Response

All Cameras On

Your Message Here
LG

20% Reduction
(Observed By Officers)
In Physical Security Policy Violations

Incentivize Participation

JEOPARDY!

$100
AMERICAN EXPRESS
3759 8765
GIFT CARD RECI
GIFT CARD
GIFT CARD
GIFT CARD
GIFT CARD
$100
AMERICAN EXPRESS
Gift
7997
3759 876543 21001
PREPAID
GIFT CARD
GIFT CARD RECIPIENT

(Contact @jaforest)

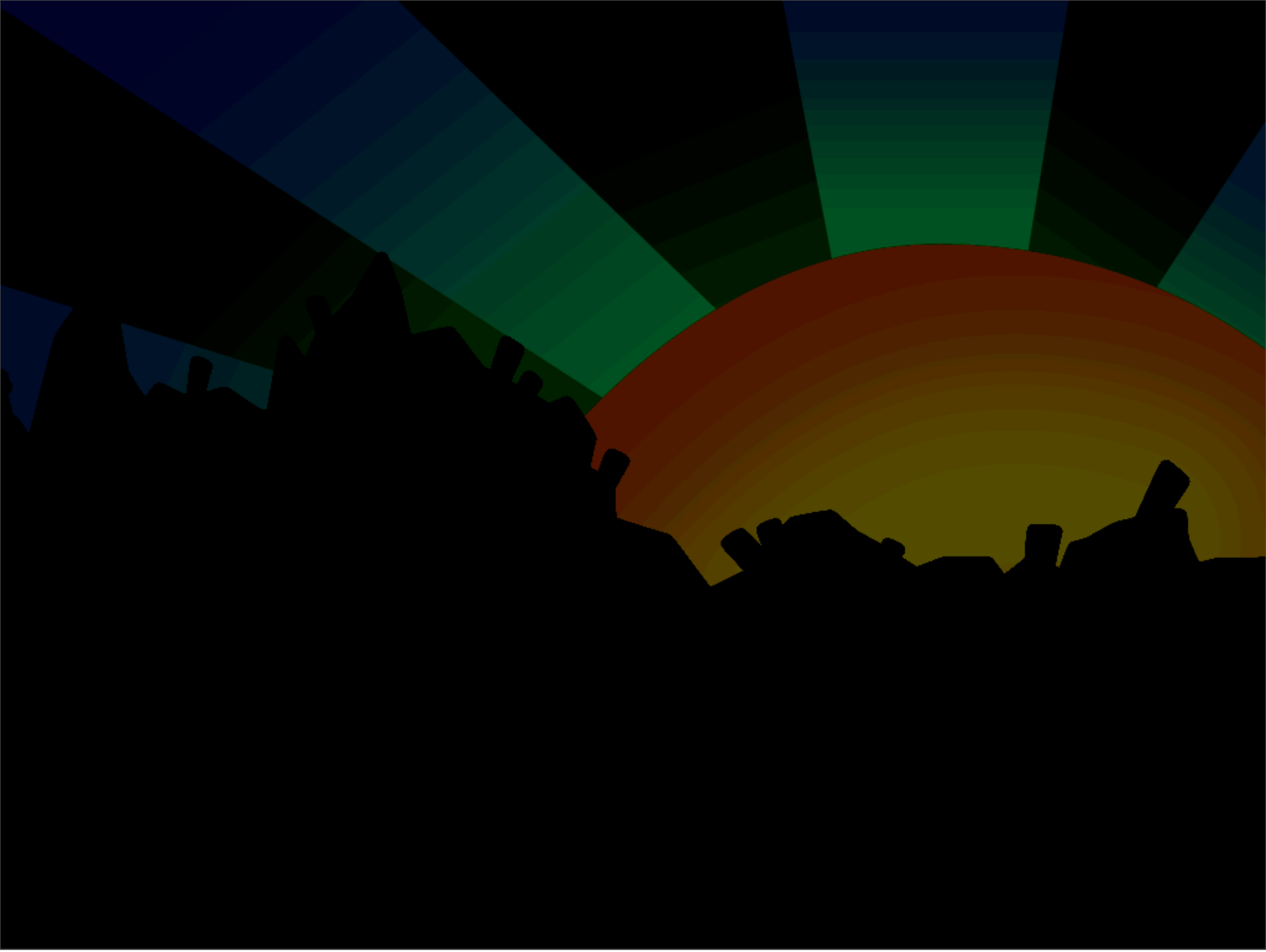
Dazzle With Demos

The New York Times
Business Day
RSA Faces Angry Users After Breach
By NELSON D. SCHWARTZ and CHRISTOPHER DREW
Published: June 7, 2011

- FireSheep Live Demo

- FireSheep Live Demo
- Phishing & Zero Day Demo For Sr Execs

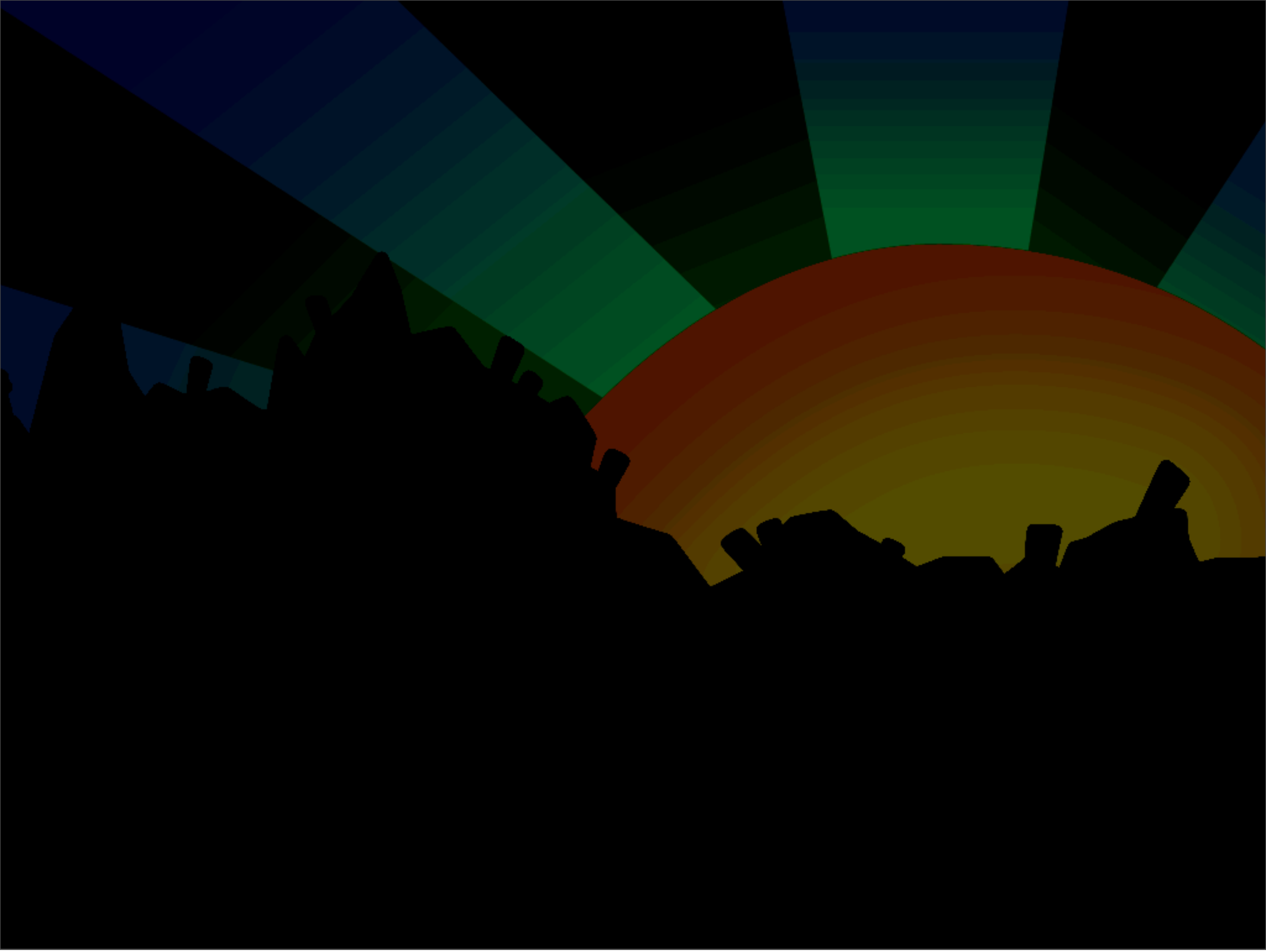
- FireSheep Live Demo
- Phishing & Zero Day Demo For Sr Execs
- SQL Injection Live Demo For Developers



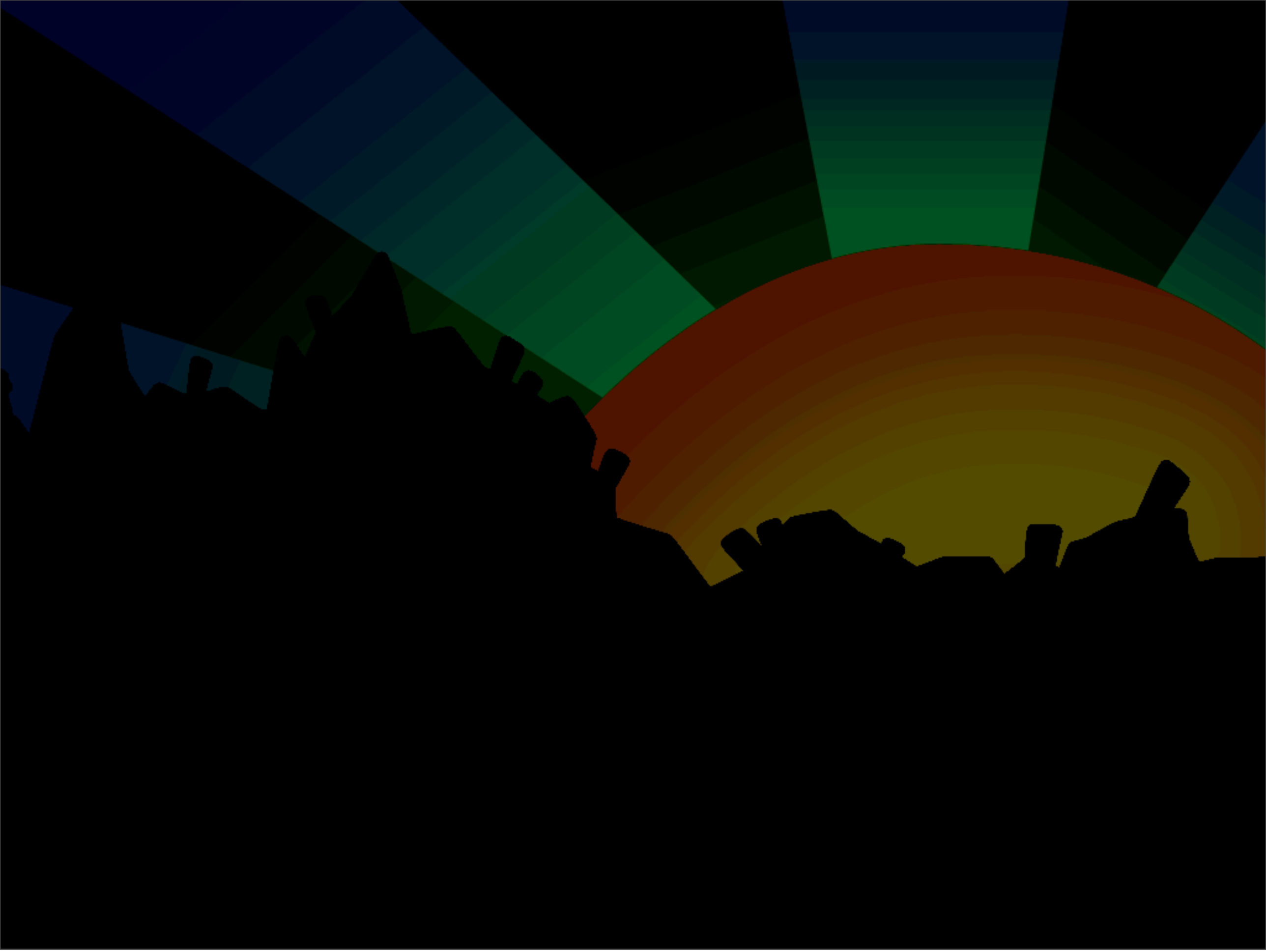
45% Increase In Reports Of Phishing By Sr Management To Incident Response

45% Increase In Reports Of Phishing By Sr Management To Incident Response

(Including External Campaigns)

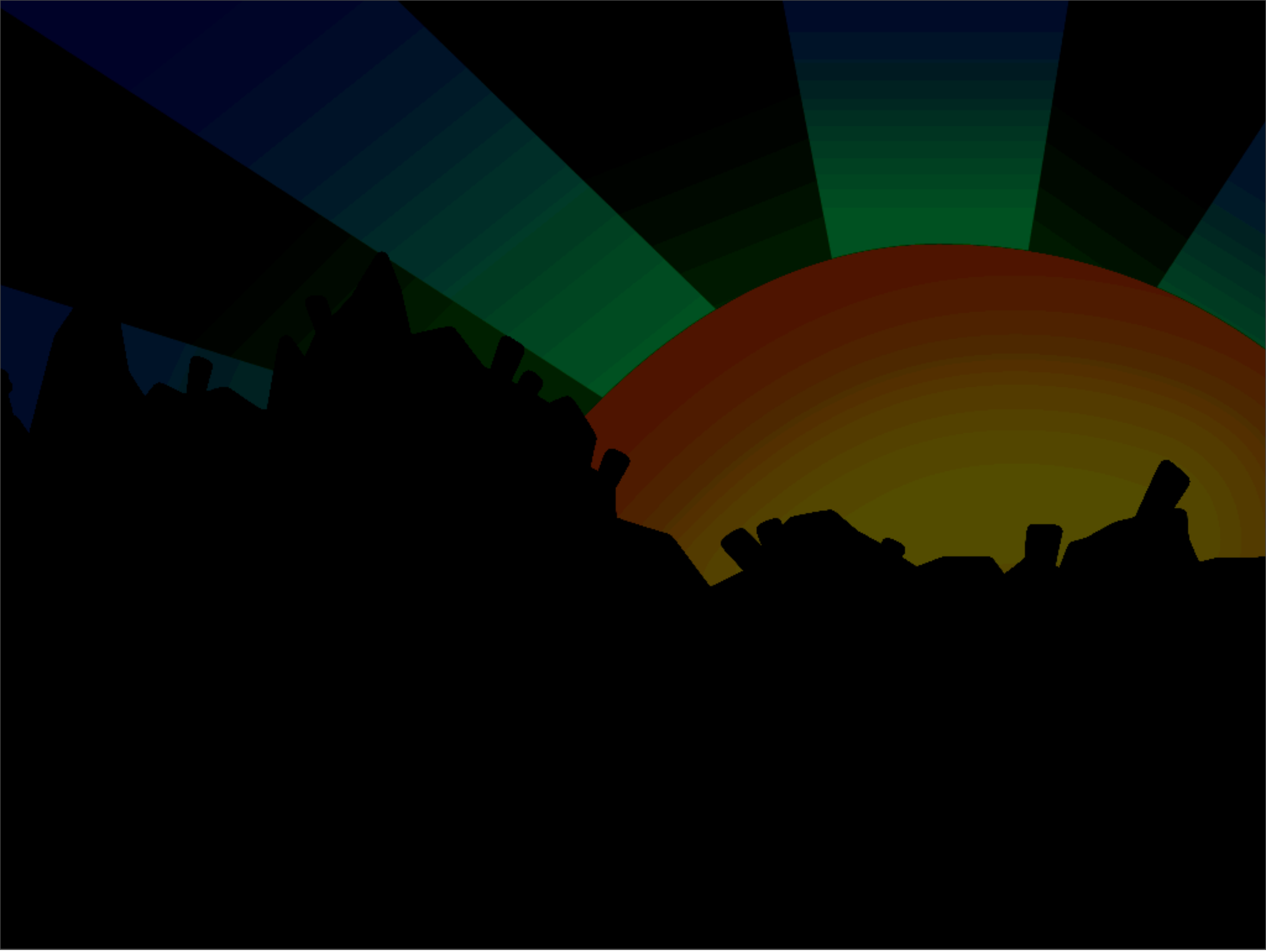


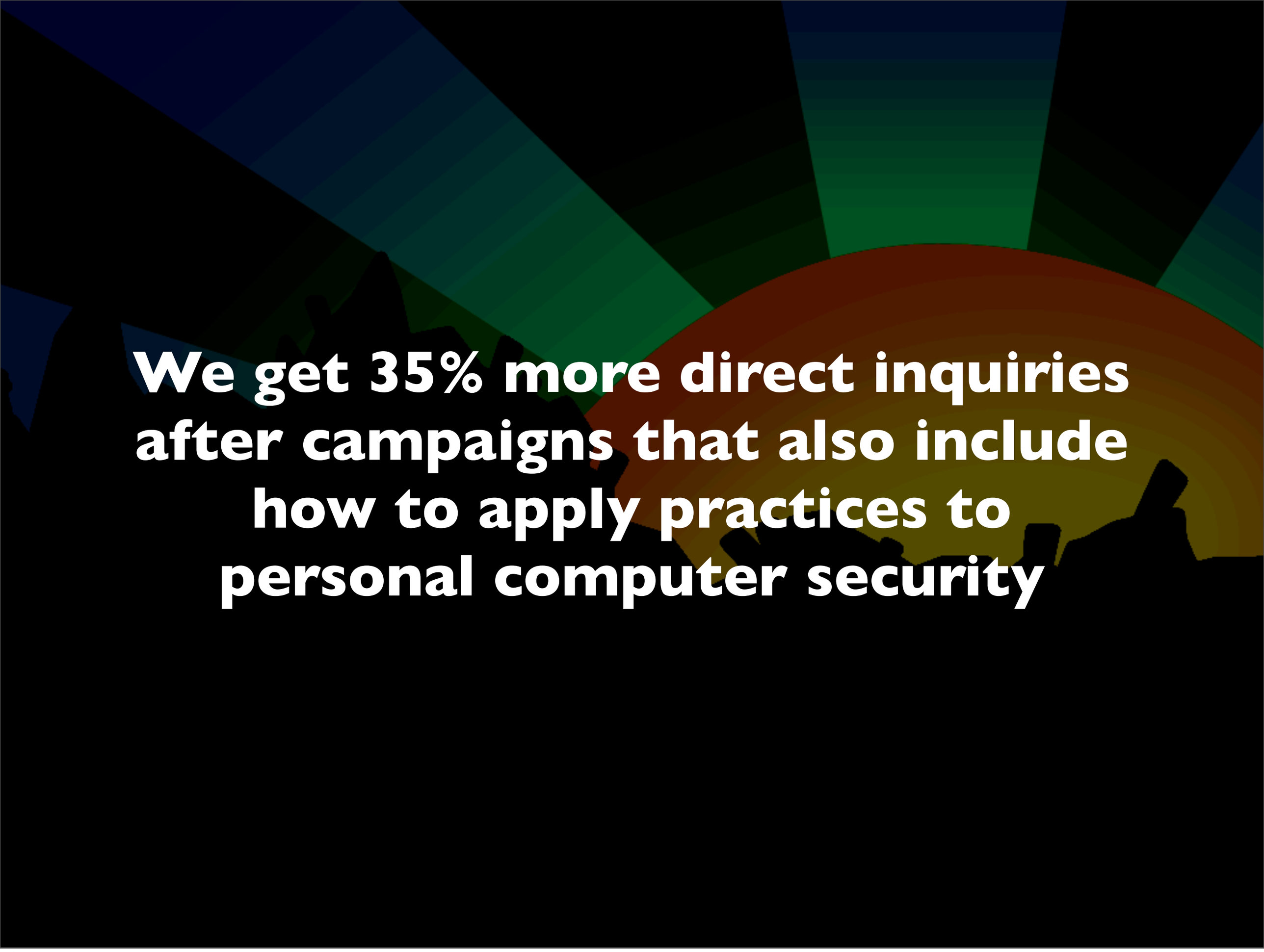
12 Requests To Perform Demos For Enterprise-wide Departments



All Demos Are Recorded And Made Available Via Internal “YouTube” Service

Make It Personal




We get 35% more direct inquiries after campaigns that also include how to apply practices to personal computer security

1. CREATIVE

2. COMPELLING

3.

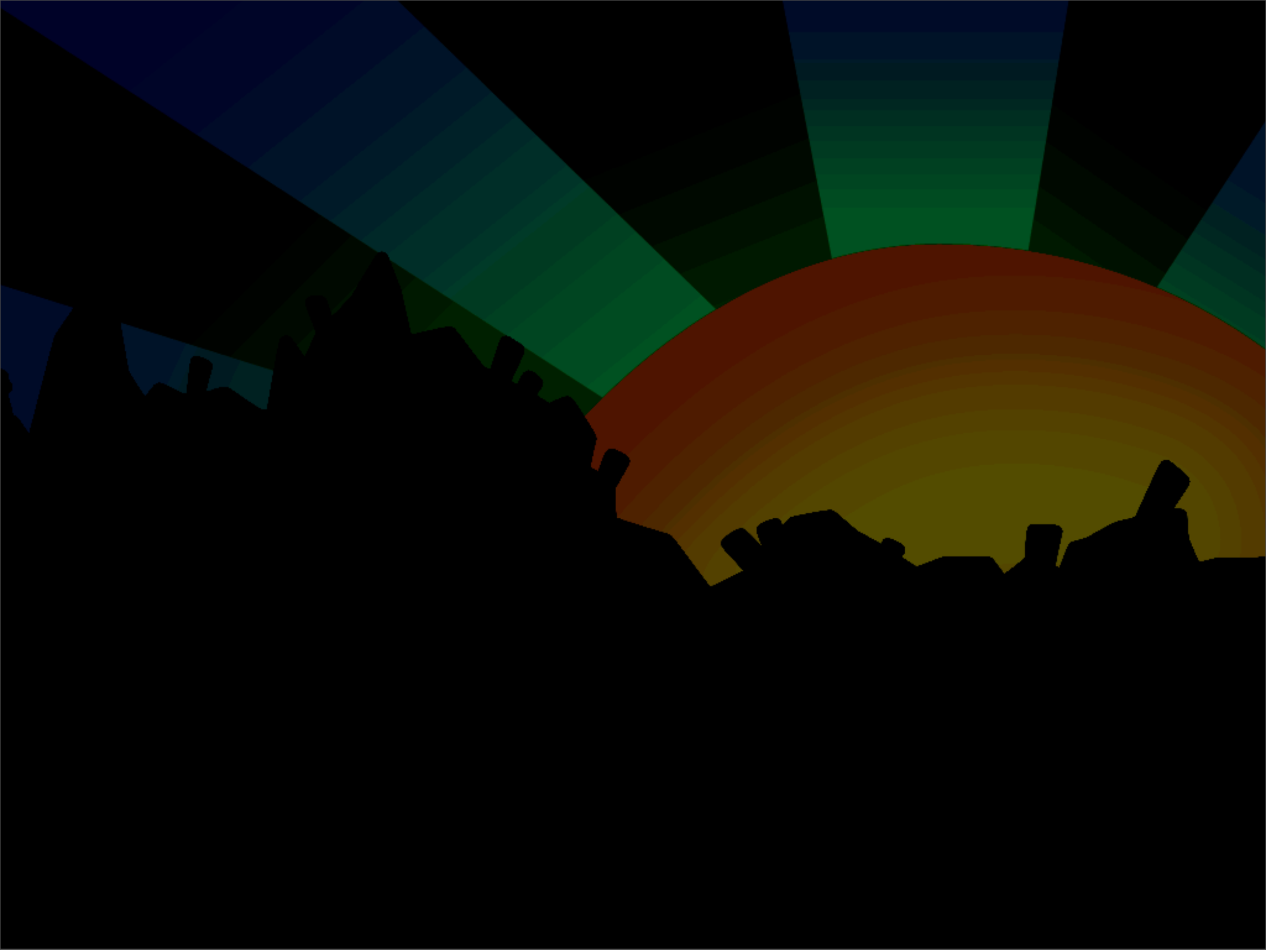
4.

1. CREATIVE

2. COMPELLING

3. CONTINUOUS

4.



One yearly CBT is not enough

Pick straightforward main themes

(Example)

How to Handle Information

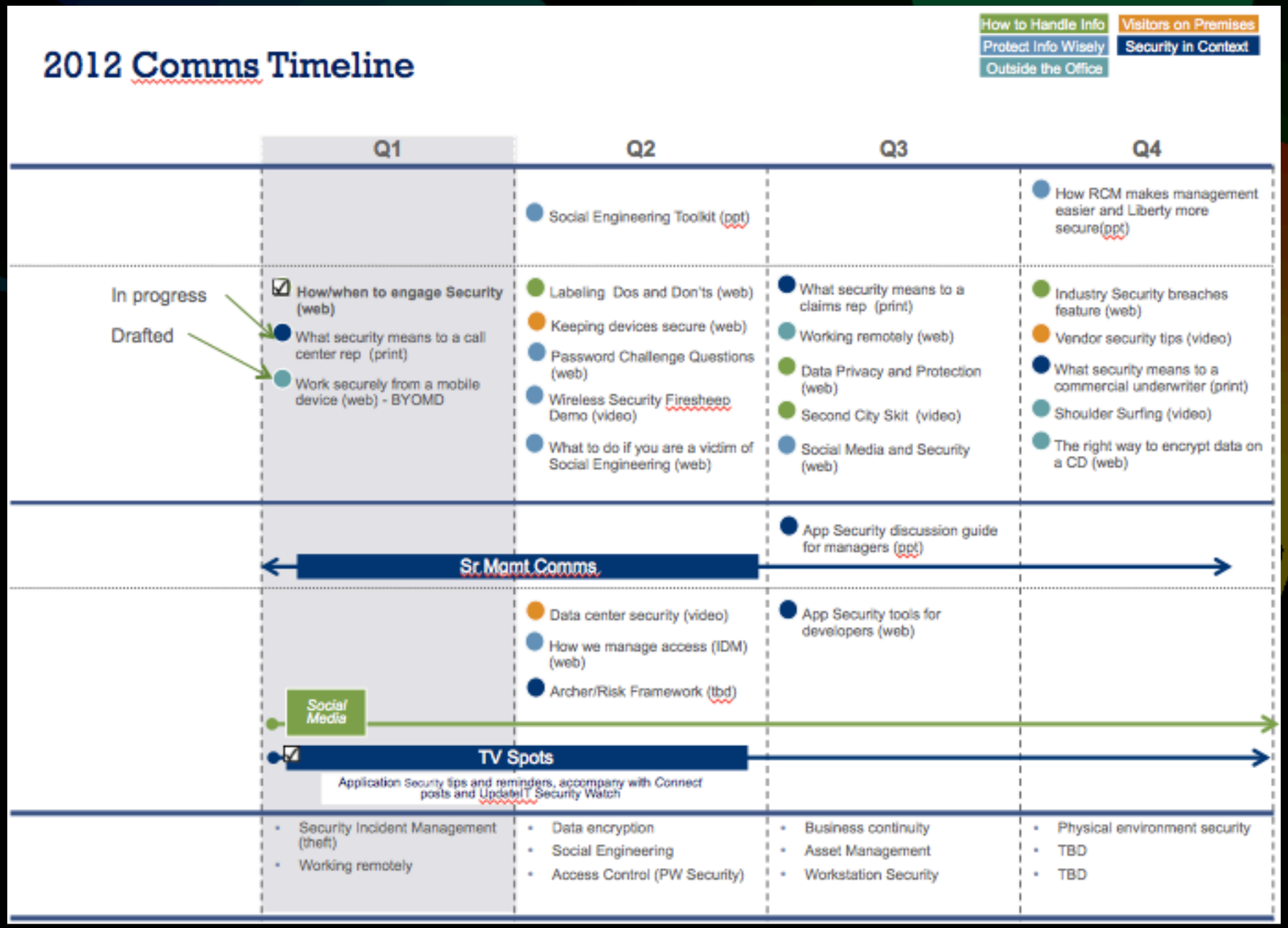
Protect Information Wisely

"Outside the Office"

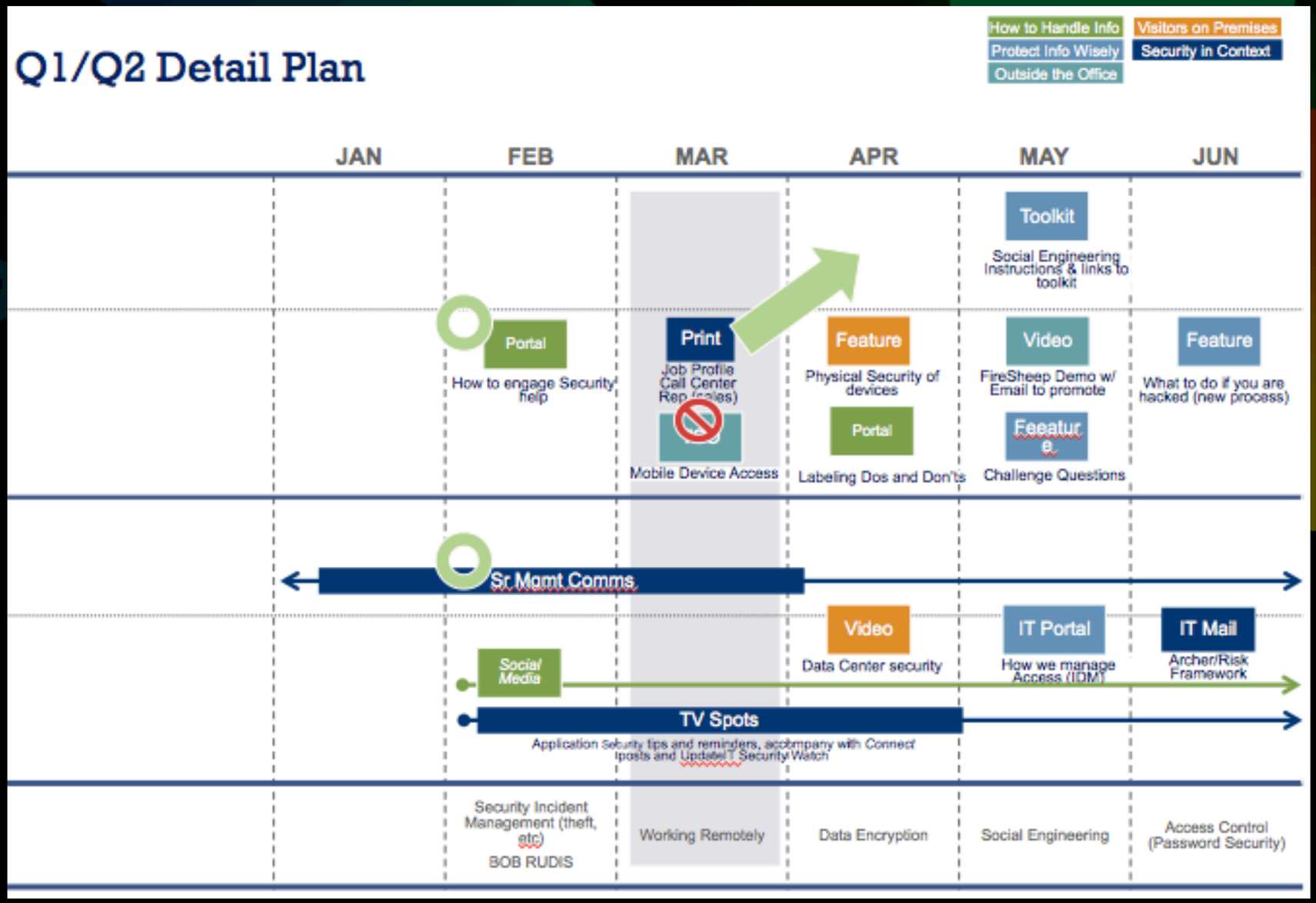
"Visitors on Premises"

Security in Context

Plan At A High Level Quarterly



Drill Down In Monthly Plans



Utilize Every Medium

E-mail (mass / targeted)
Internal Social Media
Internal Web Portal (IT/Enterprise-wide) Long-form
Internal Web Portal Snippets (“3 Things”)
Company Newsletter
Distributed TV Screens
Video-on-Demand
Department Meetings

Align With Popular Efforts

Cyber-Security Awareness Month (October)

http://www.dhs.gov/files/programs/gc_1158611596104.shtm

OUCH (Monthly)

https://www.securingthehuman.org/resources/newsletters/ouch

NPR/PRI
(Morning Edition/ATC/Marketplace)

1. CREATIVE

2. COMPELLING

3. CONTINUOUS

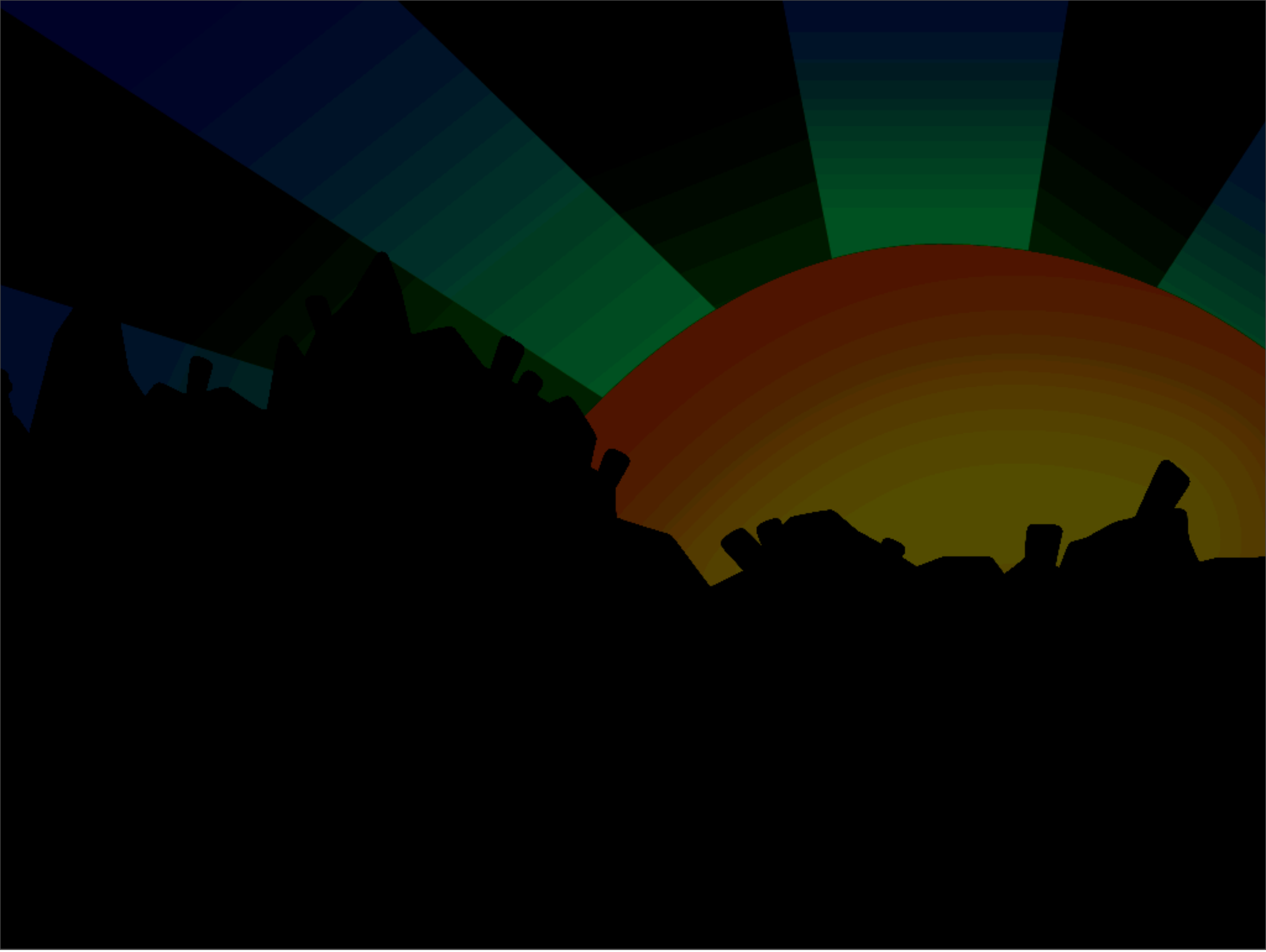
4.

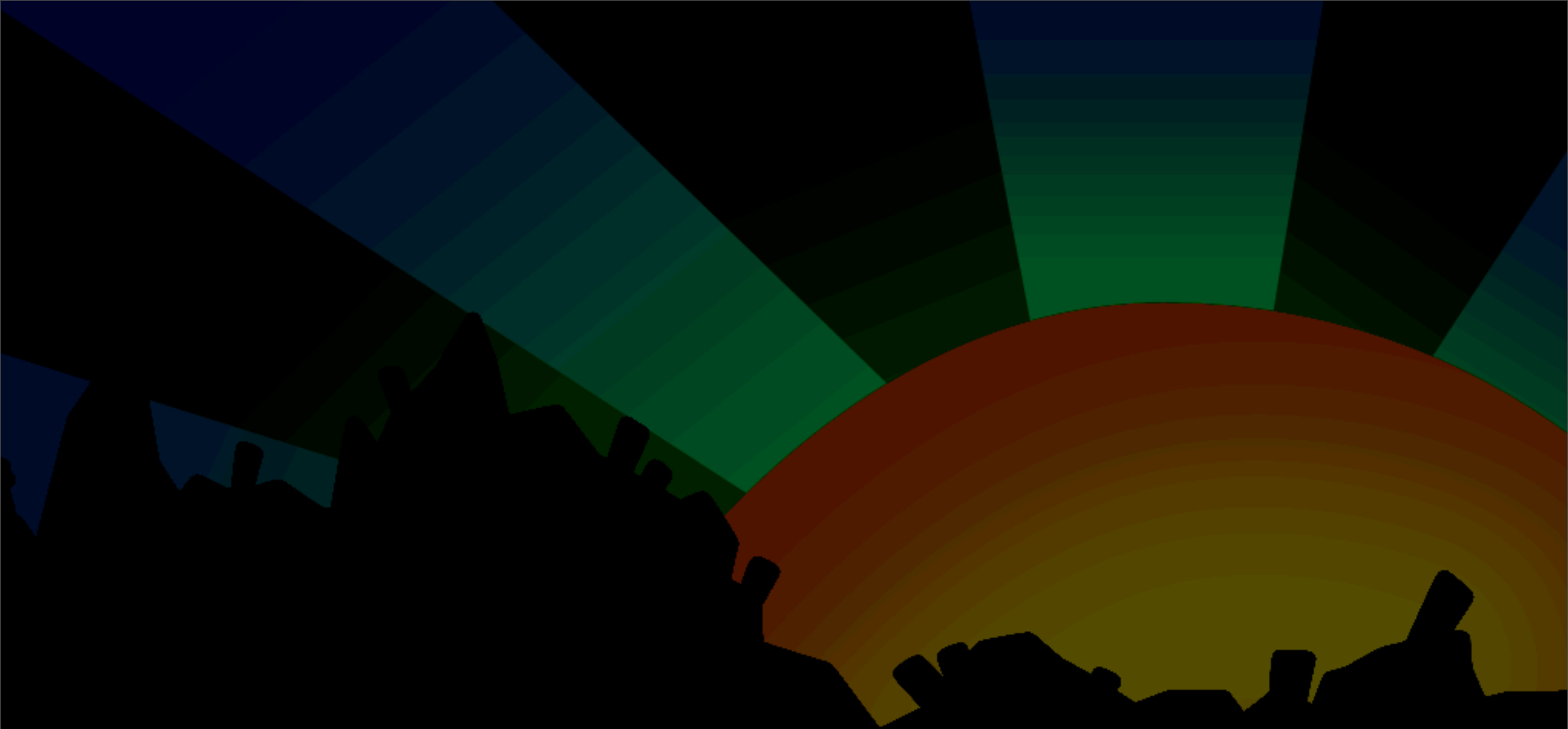
4. CUSTOMIZED

3. CONTINUOUS

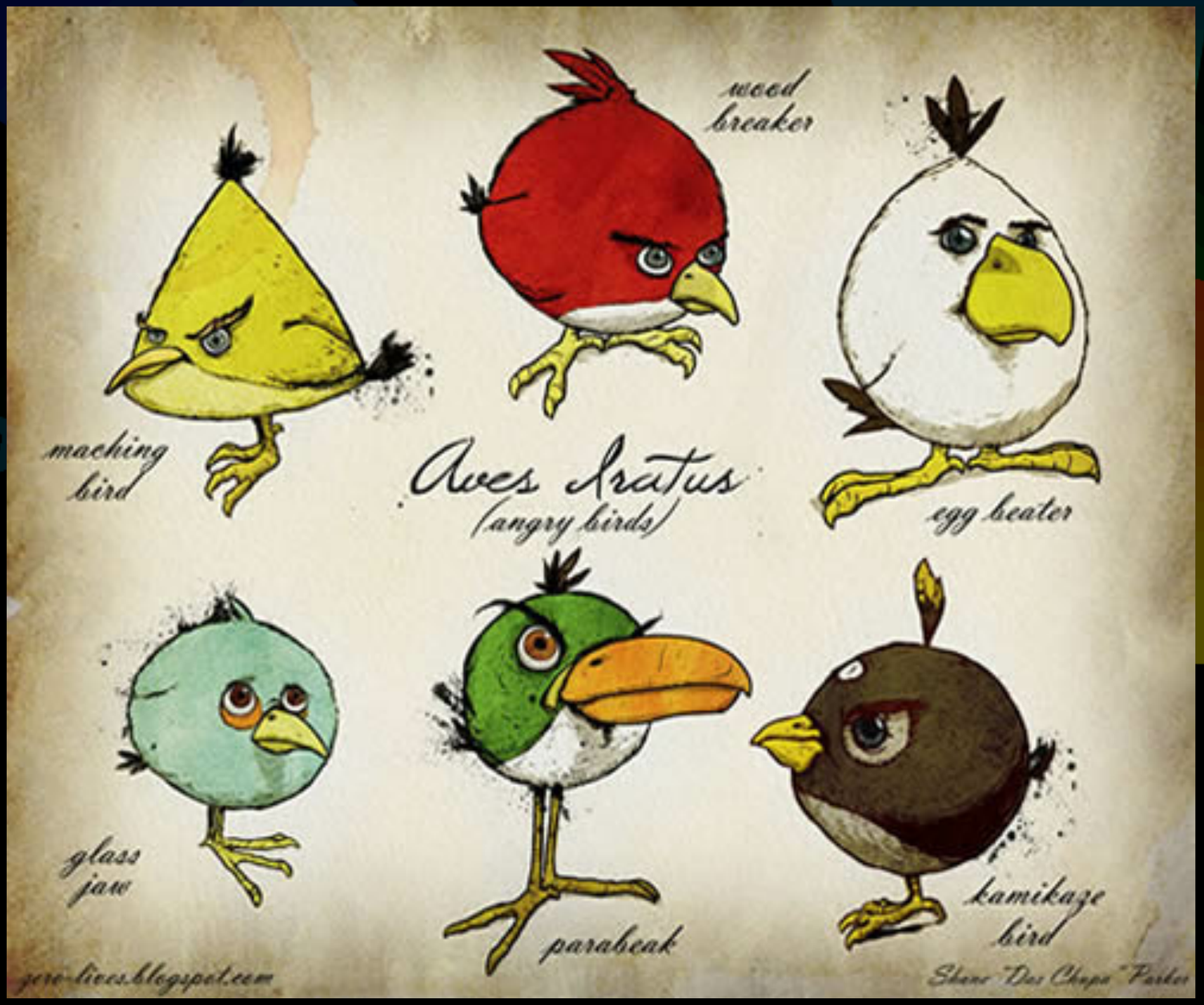
2. COMPELLING

1. CREATIVE





http://angrybirdsonline.cc/angry-birds-types-guide/



http://angrybirdsonline.cc/angry-birds-types-guide/

ext

ext

ext

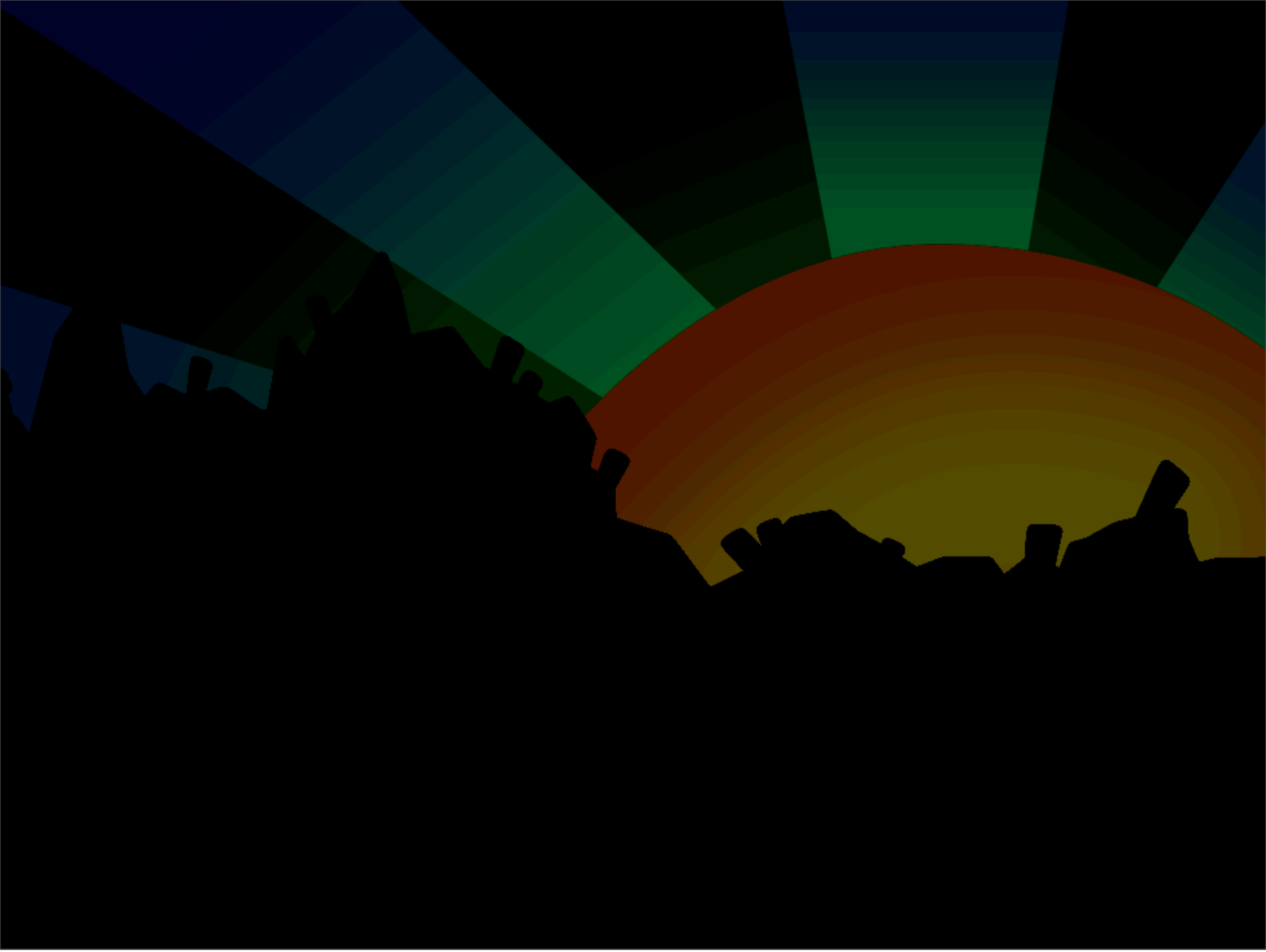
ext

ext

ext

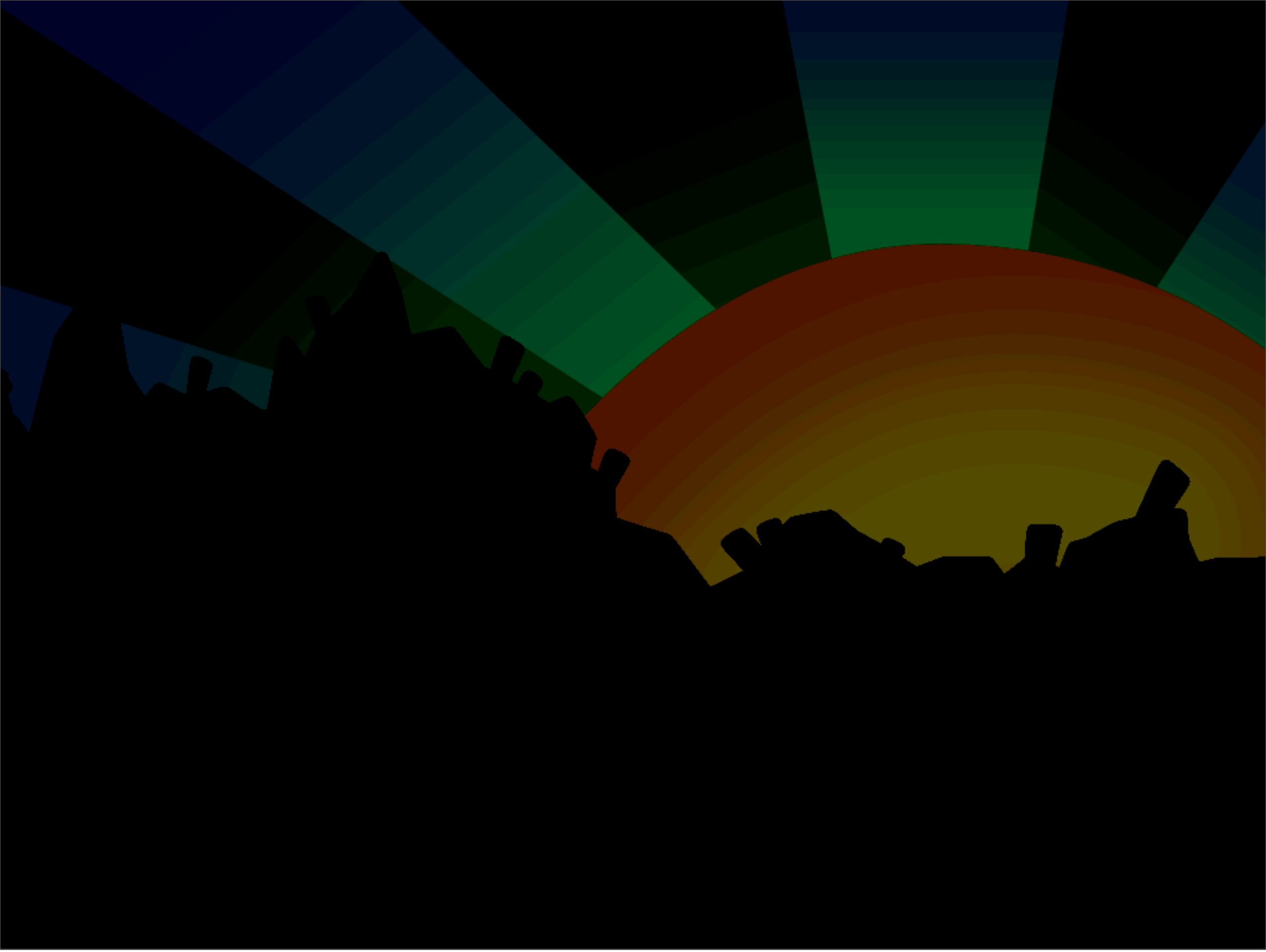
ext

ext

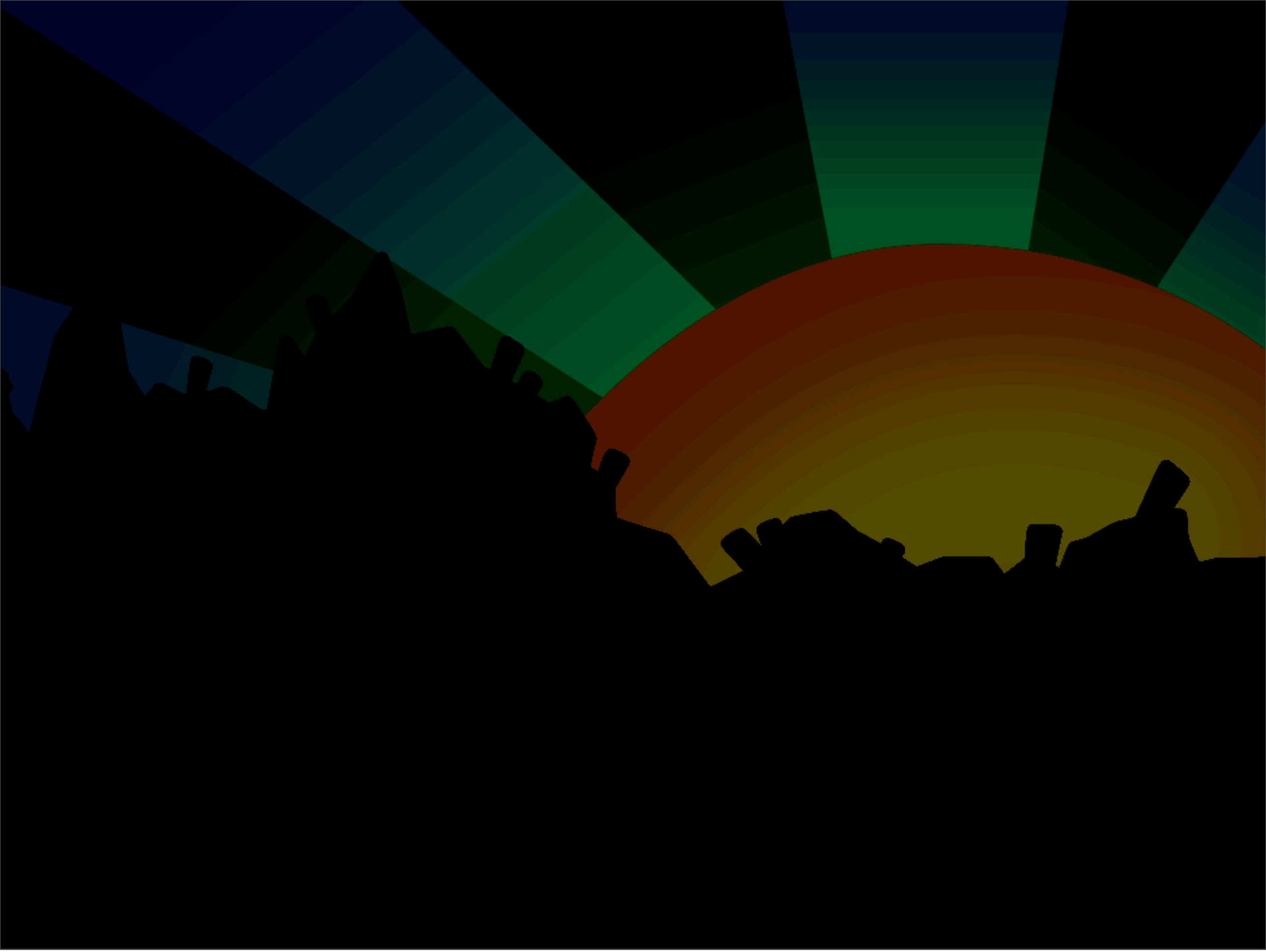


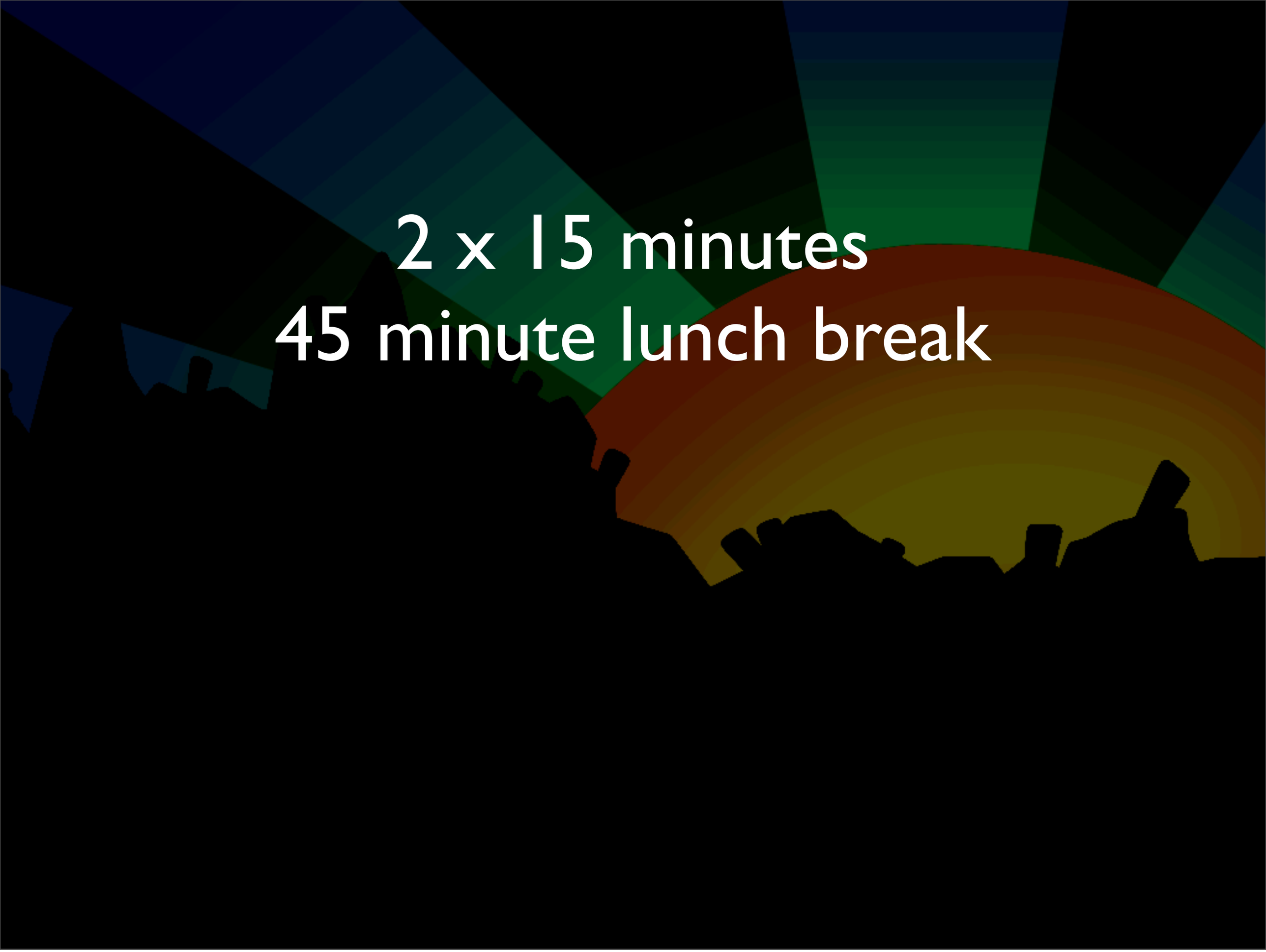
The New York Times

Do Bats Kill? Debating Wood Vs. Aluminum
THE WALL STREET JOURNAL.
Swarman Video In YouTube Debate Chills Some Politicos
Aggressive Swiss G
Rides Resources



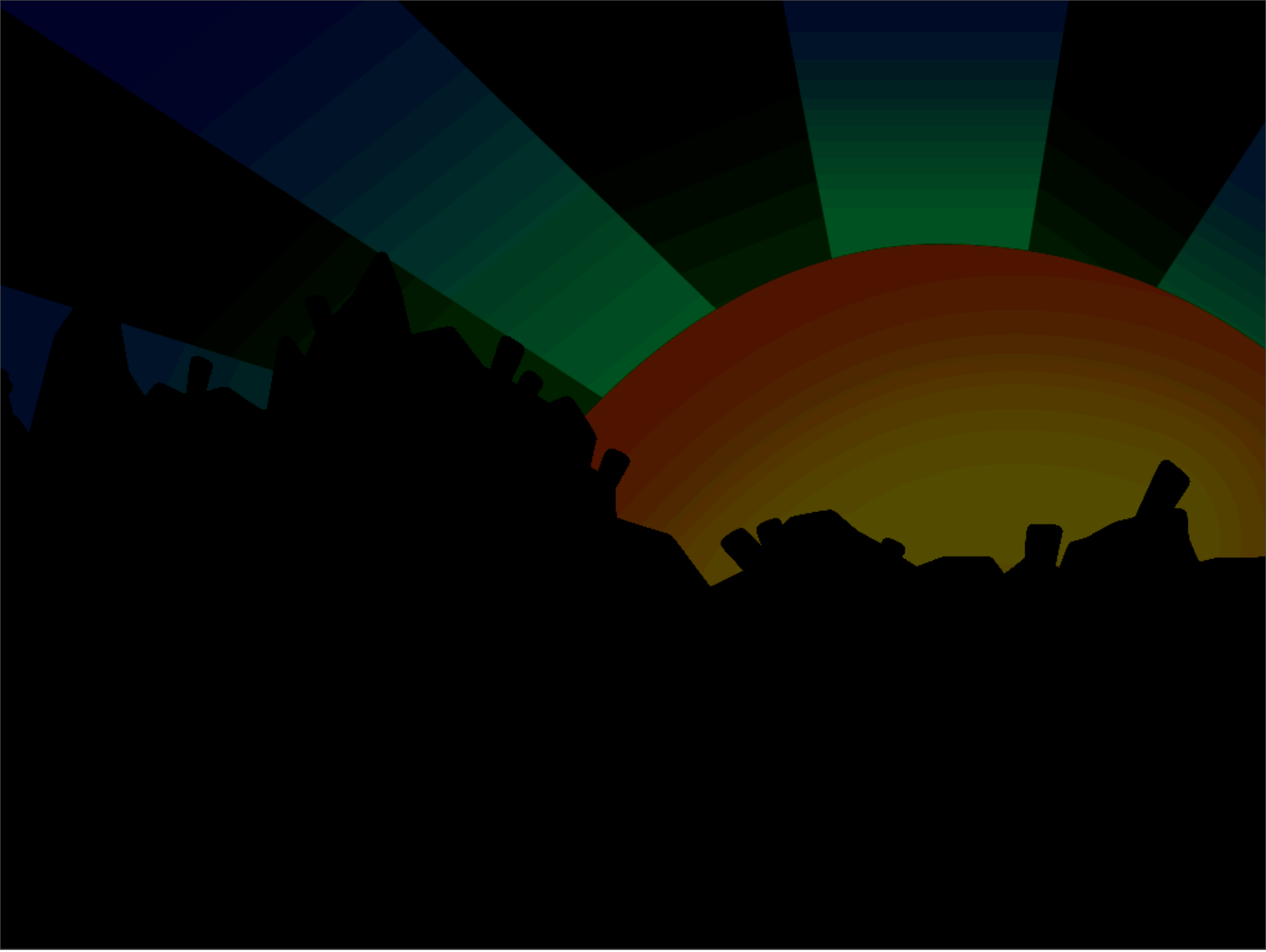
BUG



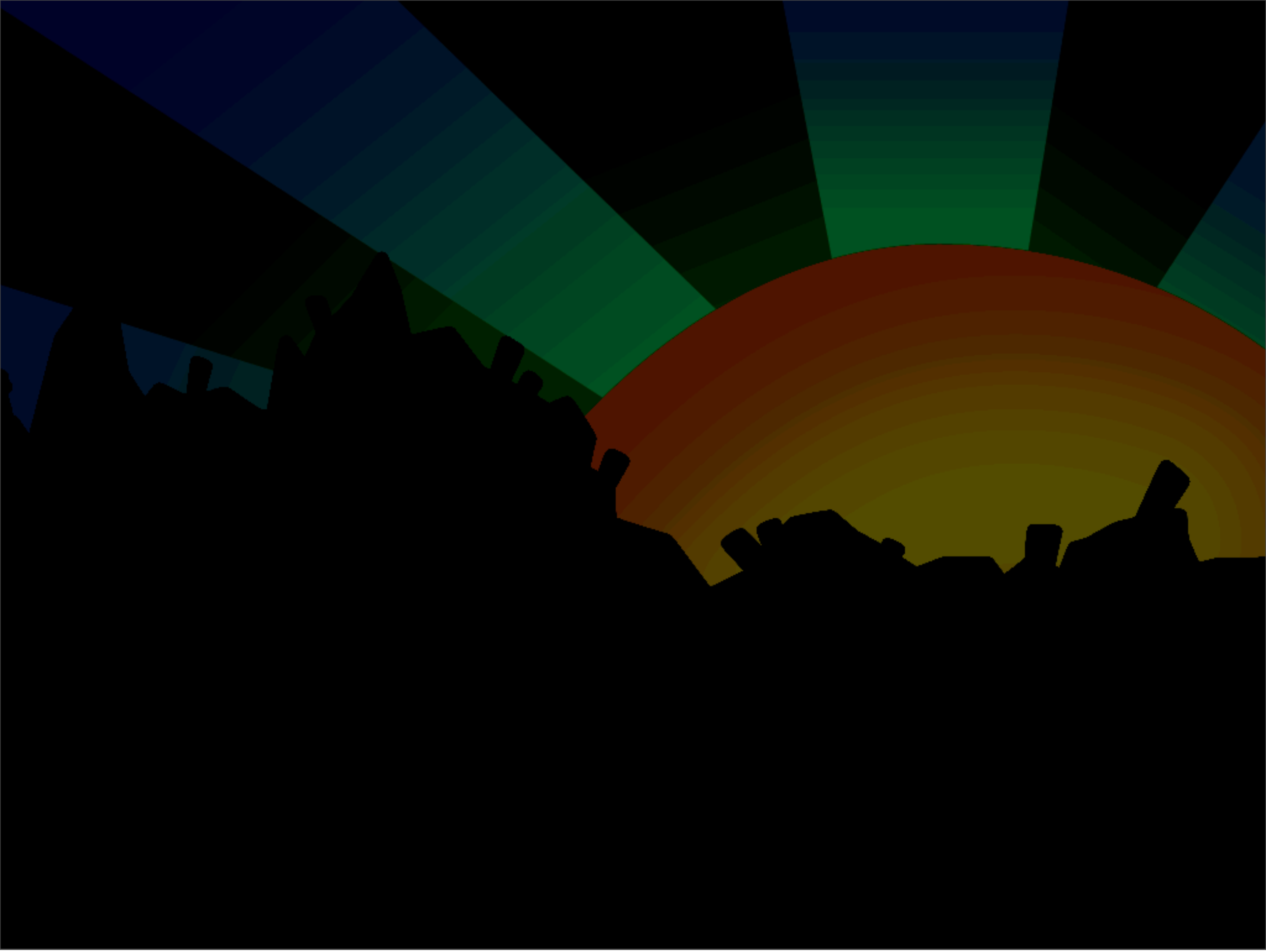

2 x 15 minutes
45 minute lunch break

2 x 15 minutes
45 minute lunch break

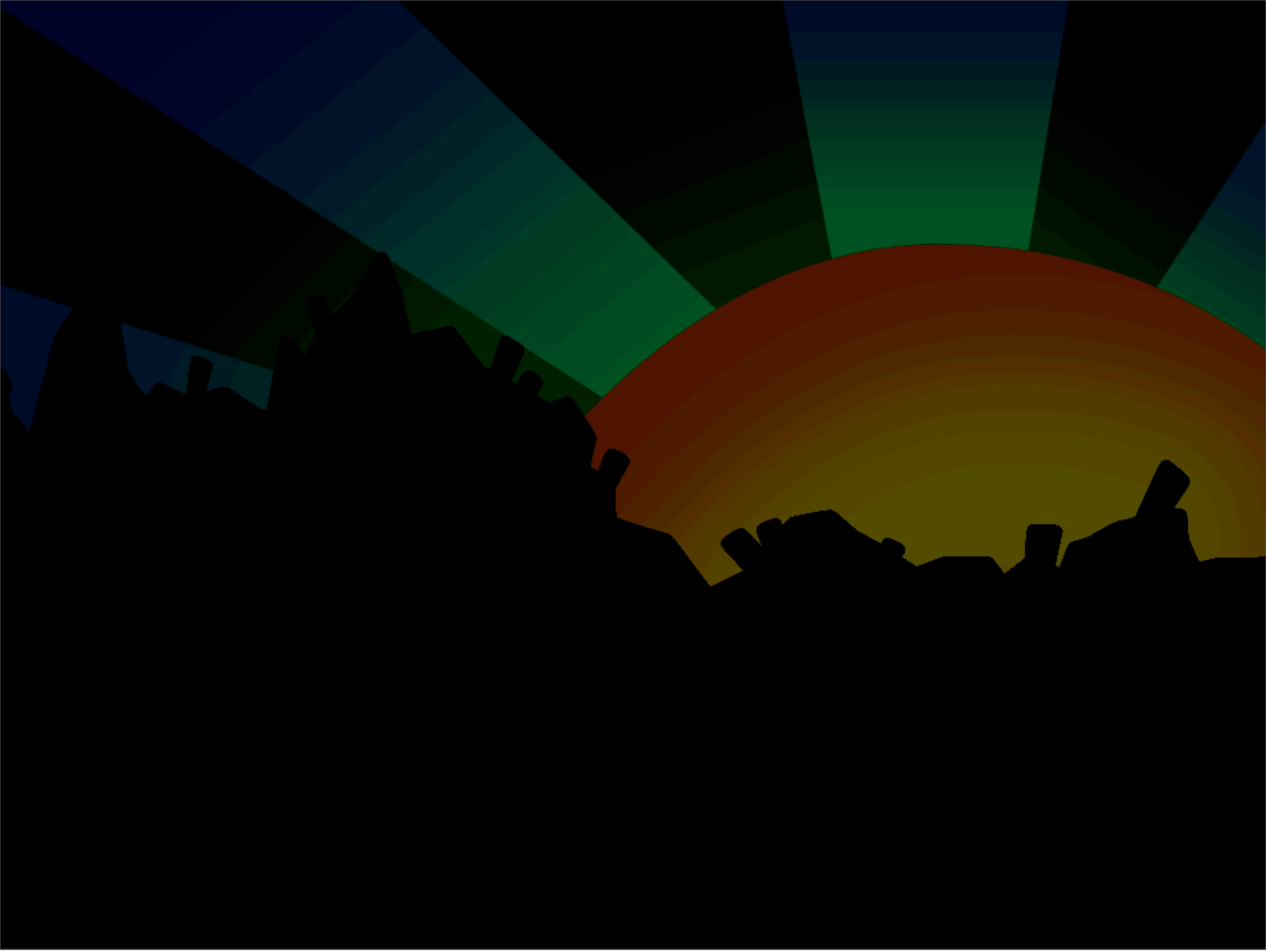
"What's Important Today?"



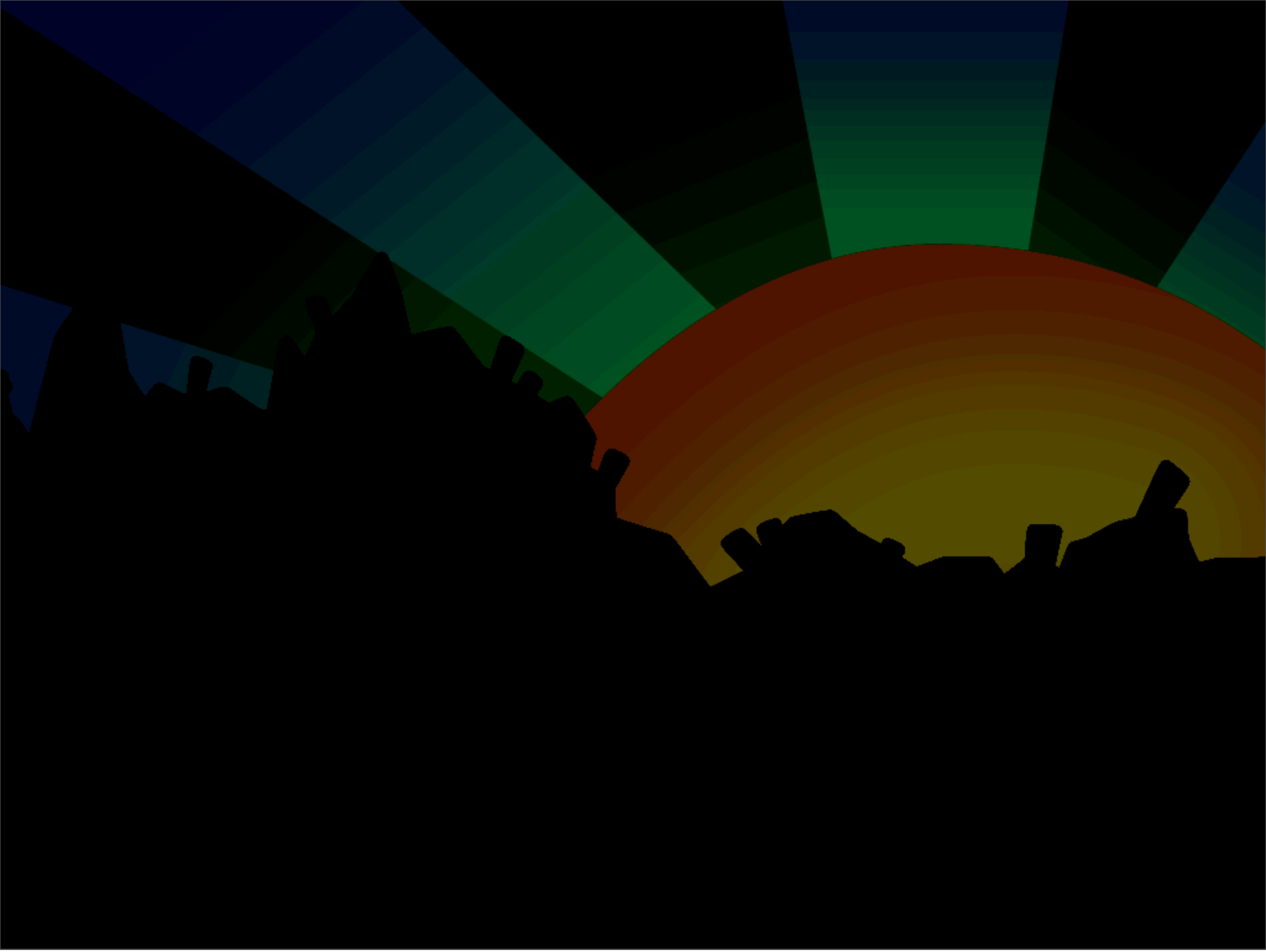
SID & MARTY
KROFFT
PRESENT
LAND
OF THE
LOST



“Manager’s Toolkit”



Bi-weekly, practitioner-based
online technical gatherings



What they need to know

Integrate it into their workflow

4. CUSTOMIZED

3. CONTINUOUS

2. COMPELLING

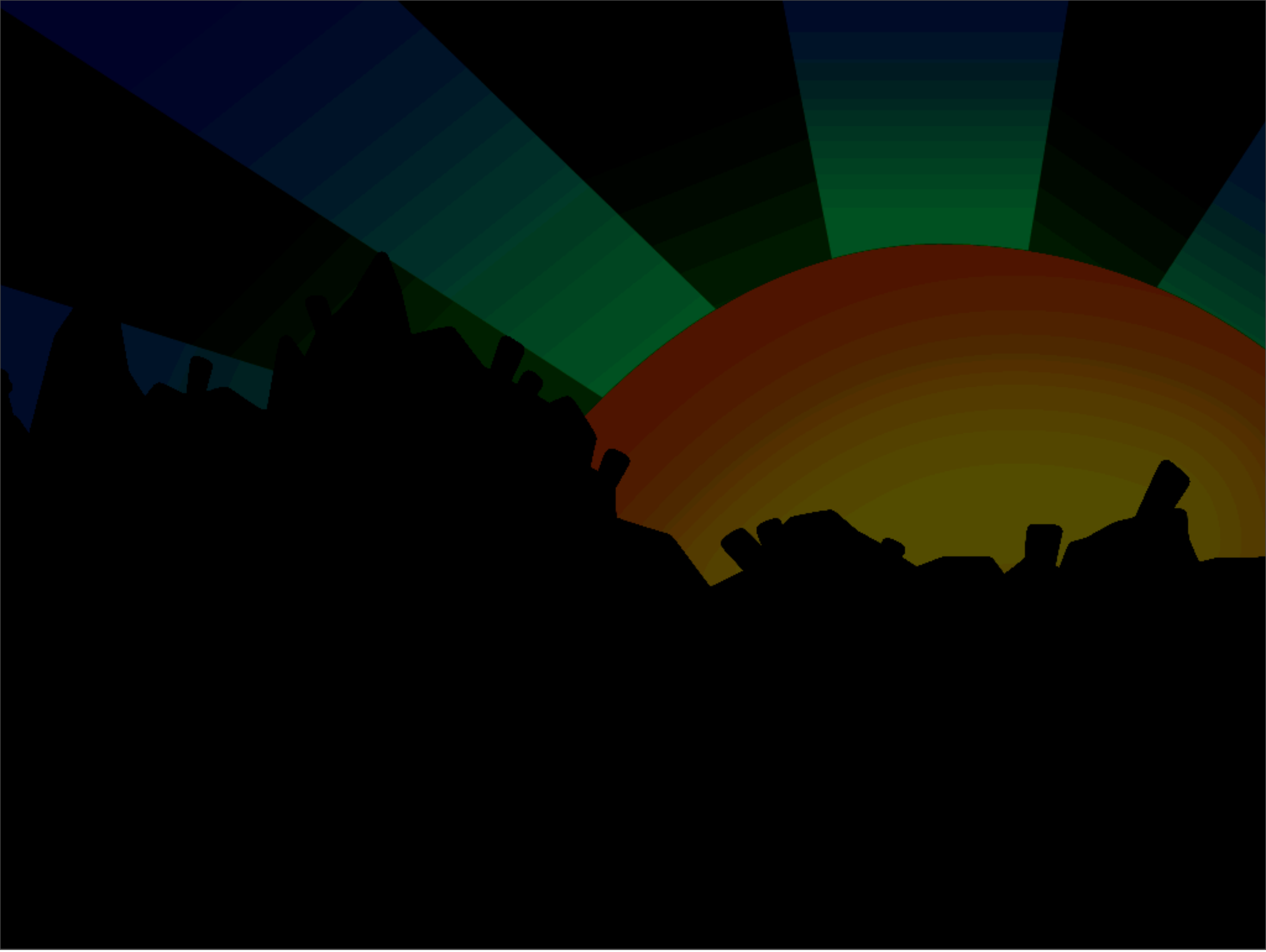
1. CREATIVE

4. CUSTOMIZED

3. CONTINUOUS

2. COMPELLING

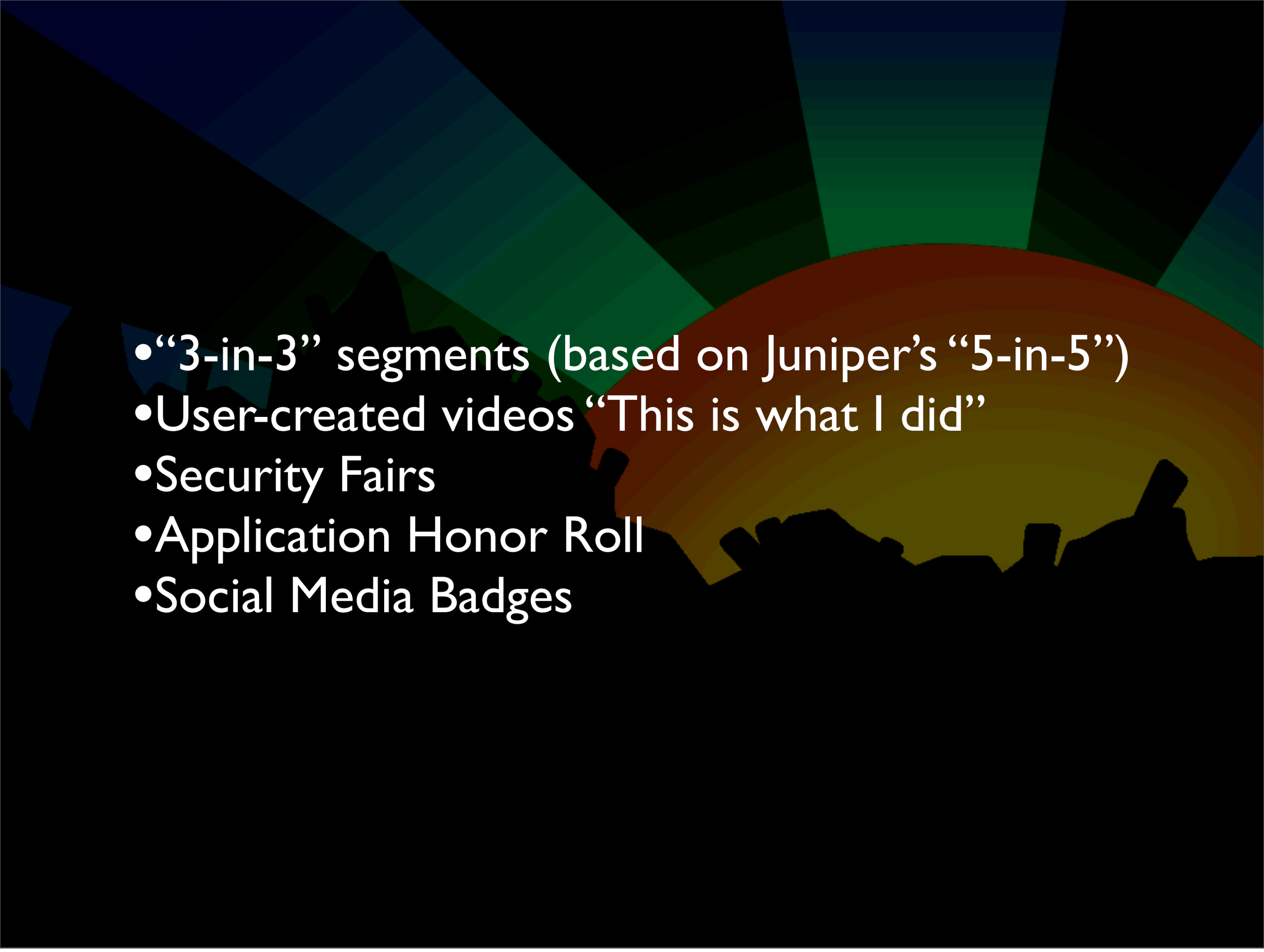
1. CREATIVE



- You **CANNOT** do it alone
- You **NEED** Senior Management Support
- You **MUST** partner with:
  - ➡Corporate Compliance
  - ➡Corporate Legal
  - ➡IT Communications
  - ➡Enterprise Communications
  - ➡Developer Community
  - ➡SBUs
- You **HAVE TO** strive for professionalism

SECURITY AWARENESS
SPACE

SECURITY AWARENESS
SPACE



- "3-in-3" segments (based on Juniper's "5-in-5")
- User-created videos "This is what I did"
- Security Fairs
- Application Honor Roll
- Social Media Badges

https://www.surveymonkey.com/sourceboston12