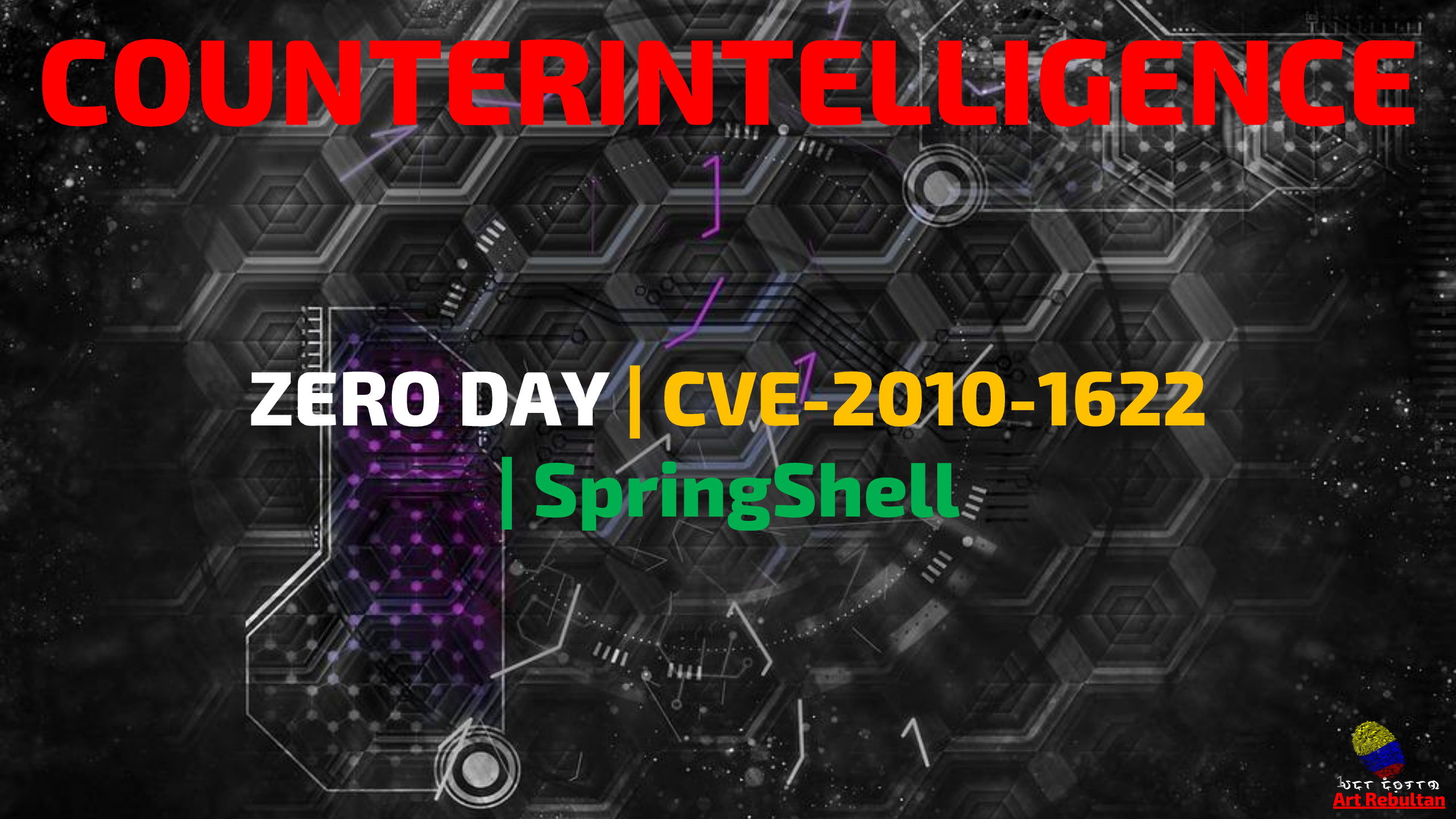
COUNTERINTELLIGENCE

ZERO DAY | CVE-2010-1622 | SpringShell



CVE-2010-1622 | Unpatched SpringShell bug threatens web app security

SUMMARY

A new critical remote code execution bug, dubbed "SpringShell" by some in the community, has been identified by security researchers. The vulnerability impacts the spring-core artifact, a popular framework used extensively in Java applications, specifically with JKD9 or newer. Sonatype explained, "the vulnerability affects anyone using spring-core, a core part of the Spring Framework, to perform logging, and anyone using software built on Spring, which is a large population of enterprise Java software.".

Credit: Unpatched SpringShell bug threatens web app security- IT Security Guru

DESCRIPTION

SpringSource Spring Framework 2.5.x prior to 2.5.6.SEC02, 2.5.7 prior to 2.5.7.SR01, and 3.0.x prior to 3.0.3 allows remote malicious users to execute arbitrary code via an HTTP request containing class.classLoader.URLs[0]=jar: followed by a URL of a crafted .jar file.

EXPLOIT

- ✓ Spring Framework - Arbitrary code Execution - Multiple webapps Exploit (exploit-db.com)

CVSS ASSESSMENT

Base 7.1 | Temporal 7.1 | Environmental 7.1 | High

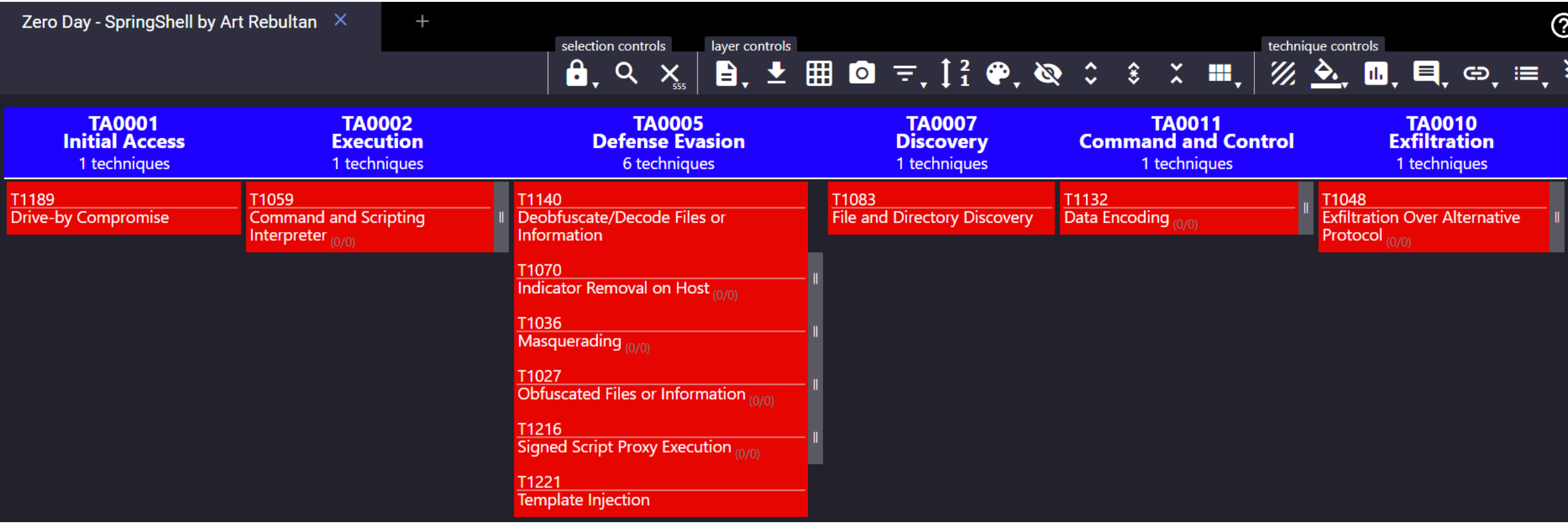
WEAKNESS ENUMERATION & VECTORS

- ✓ CWE-94
  - ❖ Improper Control of Generation of Code ('Code Injection')
  - ❖ The software constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

Access Vector (AV):	NETWORK
Access Complexity (AC):	MEDIUM
Authentication (Au):	SINGLE
Confidentiality (C):	PARTIAL
Integrity (I):	PARTIAL
Availability (A):	PARTIAL

ATT&CK IDENTIFICATION

TACTICS, TECHNIQUES, & PROCEDURES (High-Level)



Detailed MITRE ATT&CK Mapping

- RFI
  - artrebultan@gmail.com

DEFENSE-in-DEPTH

MITIGATION

- Patch Exploited CVE
- Exploit Protection
- IEC62443 Standard for Network Segmentation
- Leverage Threat Intelligence Provider
- Data Loss Prevention
- Filter Network Traffic
- Network Intrusion Prevention

GOVERNANCE, RISK, & COMPLIANCE

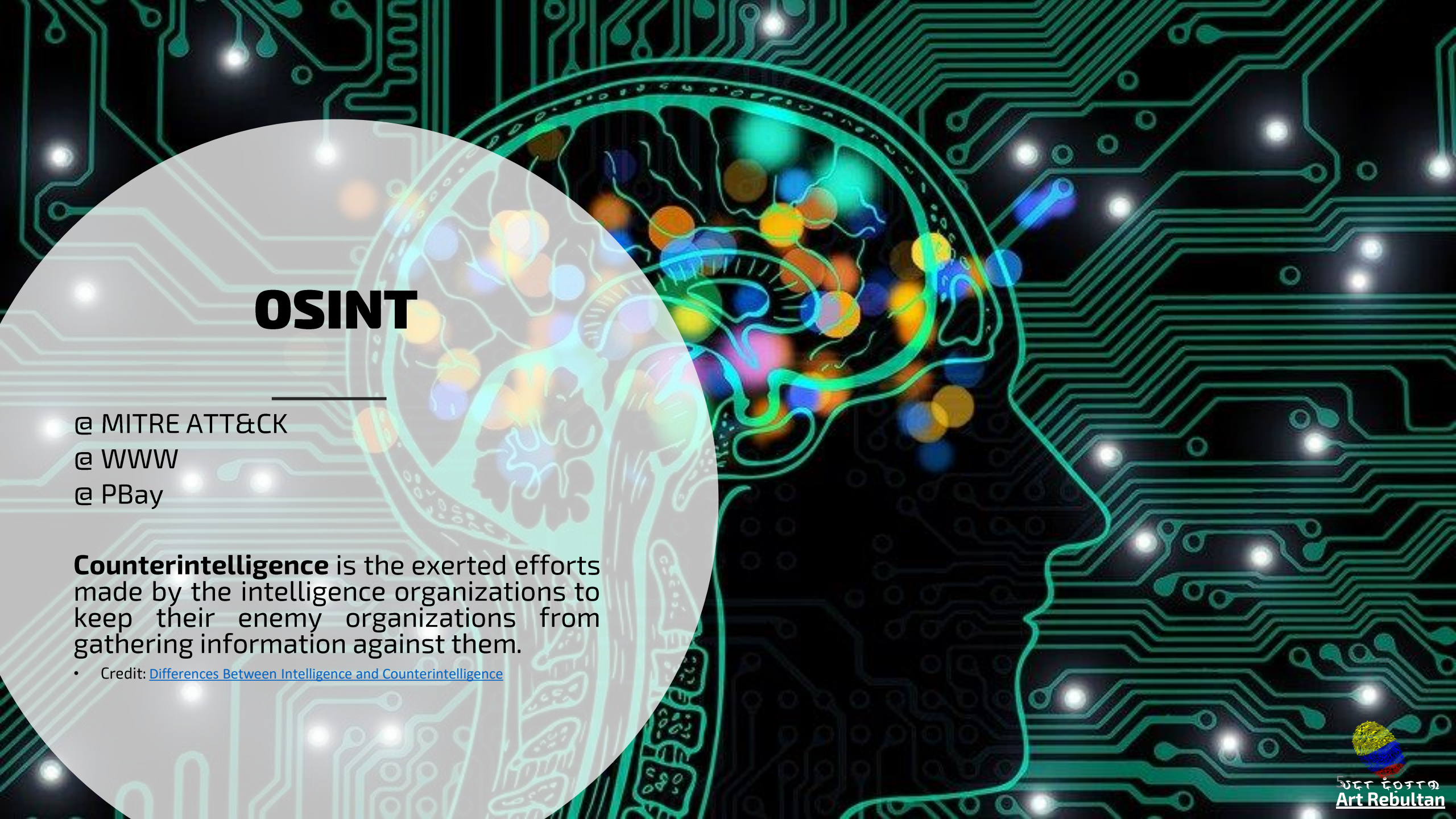
- Ensure 3rd Party Policy In Place
  - Security Assessment Questionnaire
- Privileged Account Management

DETECTION & THREAT HUNTING

- Command Execution – Leaving of the Land Binaries and Scripts (LoLBAS)
- File Access
- Anomalous Network Activities and Exfiltration

PEOPLE

- Continuous Training and User Awareness
- Proactive Mindsets for SOC and DFIR
- Threat Hunting



OSINT

@ MITRE ATT&CK
@ WWW
@ PBay

Counterintelligence is the exerted efforts made by the intelligence organizations to keep their enemy organizations from gathering information against them.

- Credit: Differences Between Intelligence and Counterintelligence