Cyber Threat Intelligence Management

Agenda for the next 13:37 minutes

Where does this talk fit?

Intermediate

Expert

Intro

Advanced

1337 Tier

Was that a fat joke?

You aren't my manager pal!

Proactive

Context

Contribute

Response times

Cyber Threat Intelligence Common Language

01 Observable

02 Threat Actor

03 Tactics, Techniques and Procedures

04 Indicator

05 Campaign

Lockheed Martin Cyber Kill Chain ®

06 Lockheed Martin Cyber Kill Chain®

07 Traffic Light Protocol

08 Intelligence Disciplines (*INT)

09 STIX, TAXII, CybOX & OASIS

10 F3EAD Framework

F3EAD Framework

F3EAD Framework related to IR

Operations

Find
SIEM

01

Fix
SIEM

02

Finish
IR

03

Intelligence

Exploit
TIC

04

Analyze
MAS

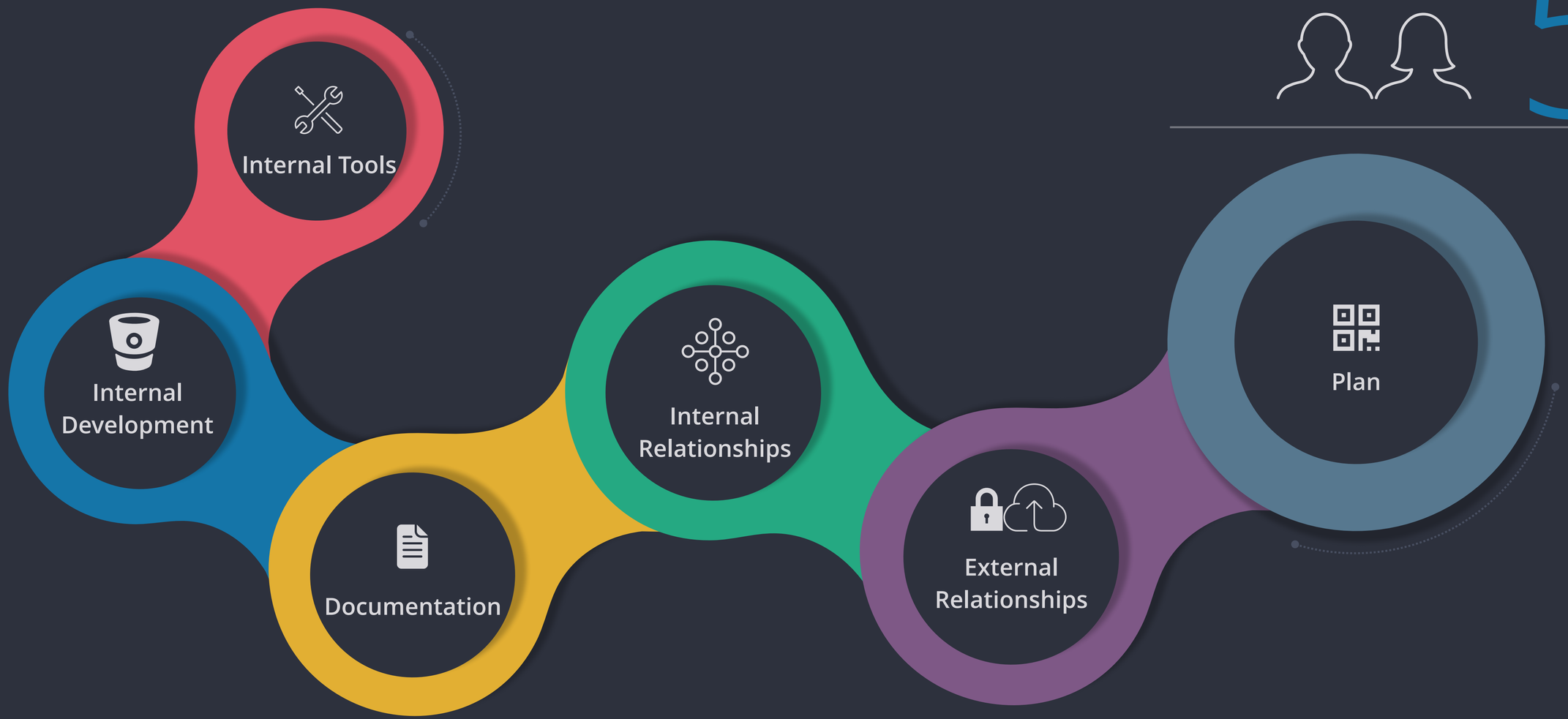
05

Disseminate
SIEM

TIC

06

How to build a Threat Intelligence Center (TIC)



50%

50%

The tools to build an Open Source Threat Intelligence Center (TIC)

STIX	TAXII	Development	Malware
CRITs	SOLTRA	GitLab	Cuckoo
STIX friendly	CRITs friendly	Developer friendly	CRITs friendly
Mongo	Eats whatever you feed it	Local Version Control	STIX Friendly
Python Friendly	TAXII Gateway for partners	Track Issues	Python Friendly
Over 30 Services	FS-ISAC	Locally crowdsource dev	Automated Malware Analysis
CTI repository	Utilizes TLP	Integrates with Slack	Win/OSX/Linux Analysis
Campaign Tracking	Notifications	For teams of 1 - 30K	Volatility
crits.github.io	soltra.com	gitlab.com	cuckoosandbox.org

TIC.SecKC.org:443

Powered By: Threat Note

cory@seckc.org


IT’S MY TIC IN A BOX.