NO FF ONE 2022

Notes of a traveler between realms: IS and IT

Dmitriy Evdokimov

Founder&CTO Luntry

Moscow, August 25, 2022

WhoAmI

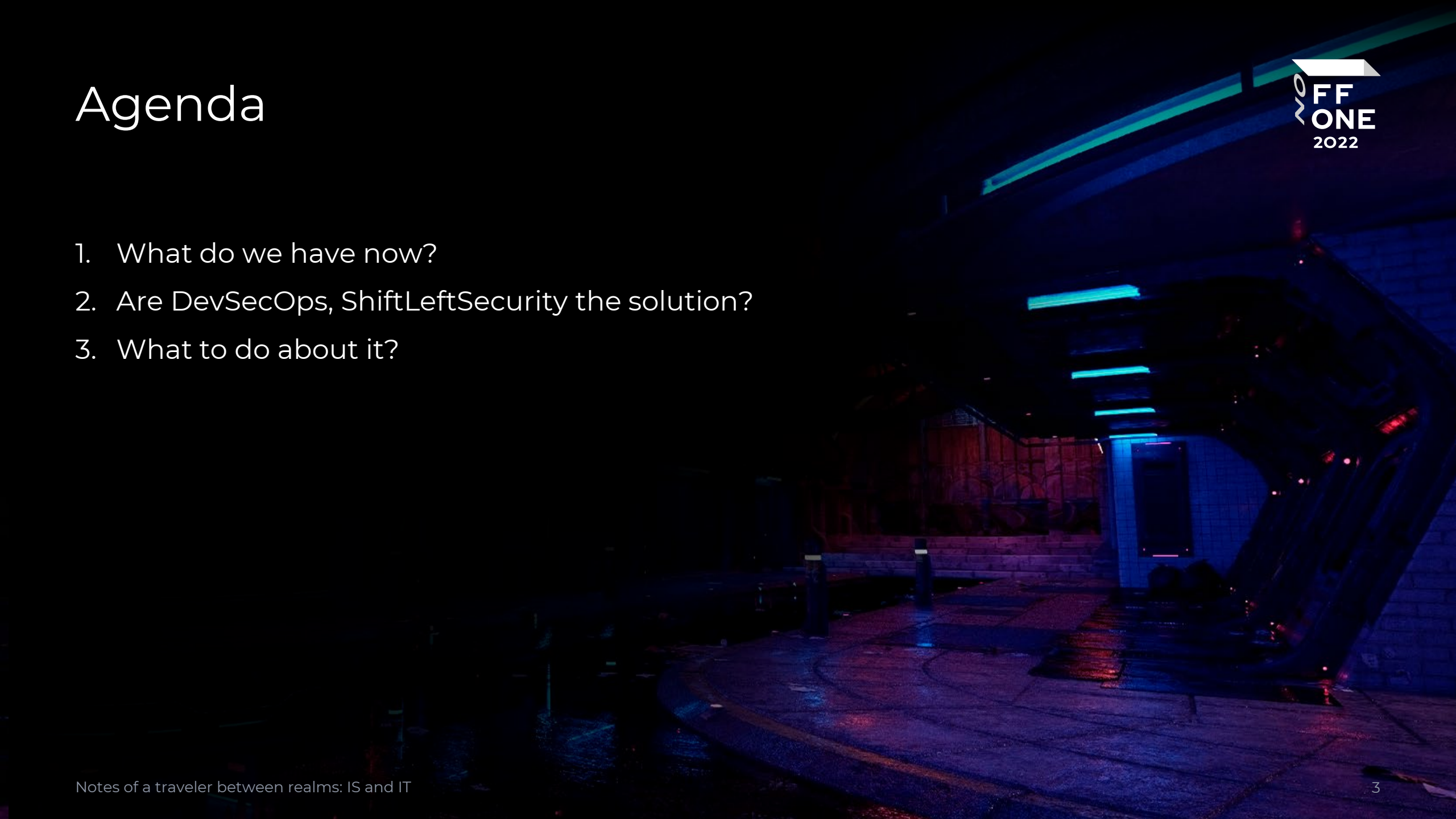
- Founder and CTO of Luntry
- 10+ years in Information Security
- Co-organizer of ZeroNights, DEFCON Russia (#7812) conferences
- “XAKEP” ex-author and editor
- Author of k8s(in)security Telegram channel
- Authored “Cloud-Native Security in Kubernetes” course
- Does not believe that you can make a system secure and reliable without understanding it.
- Talks at BlackHat, HITB, ZeroNights, HackInParis, Confidence, SAS, PHDays, OFFZONE, DevOpsConf, KuberConf, VK Kubernetes Conference, HighLoad++, and others.

LUNTRY

luntry.ru

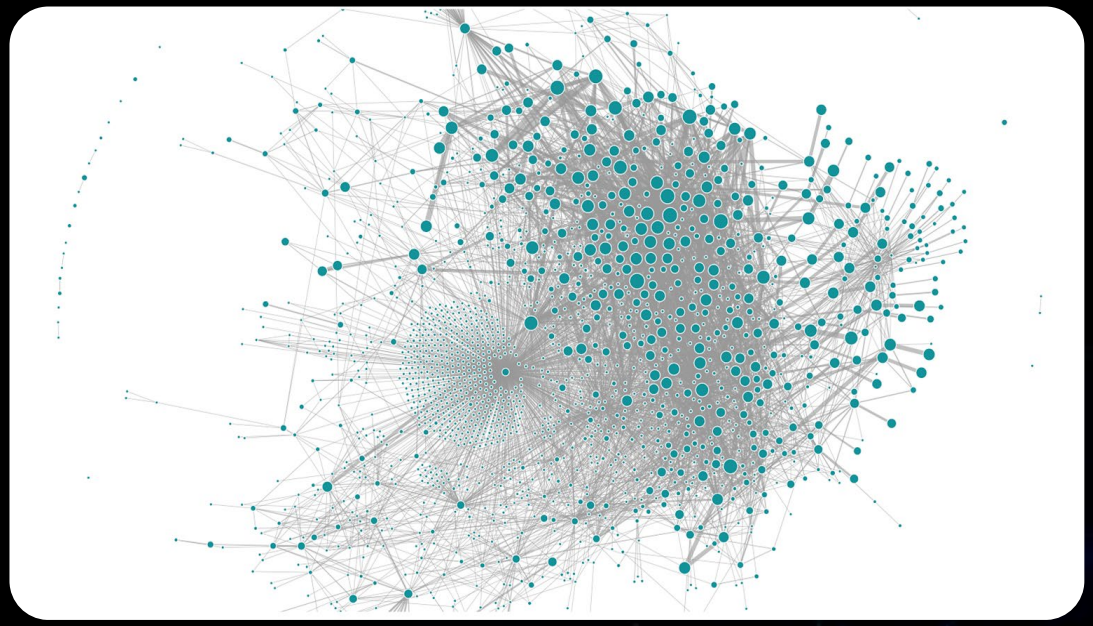
Agenda

1. What do we have now?
2. Are DevSecOps, ShiftLeftSecurity the solution?
3. What to do about it?



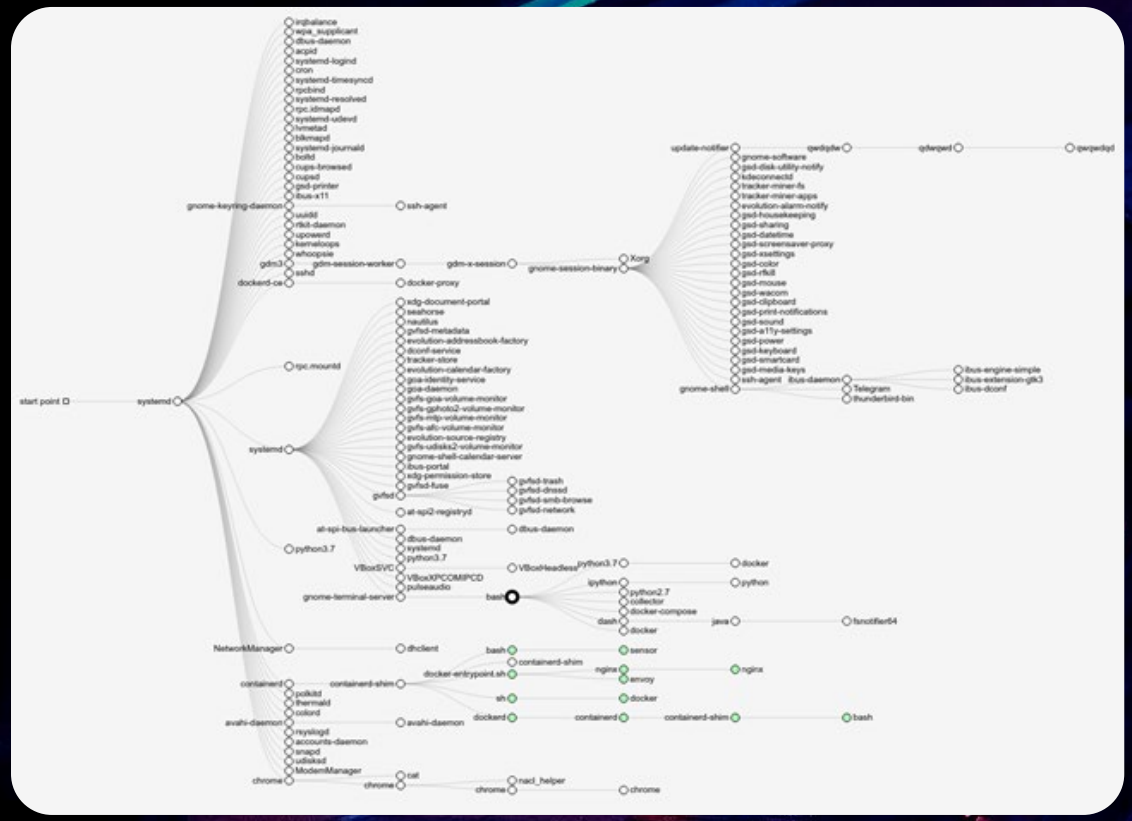

ON
FF
ONE
2022
What Do We Have Now?
LUNTRY

Unexplored and Complex World



"Complexity is the worst enemy of security, and our systems are getting more complex all the time"

Bruce Schneier



"The only thing that ever yielded real security gains was controlling complexity"

Thomas Dullien / Halvar Flake

Static Systems

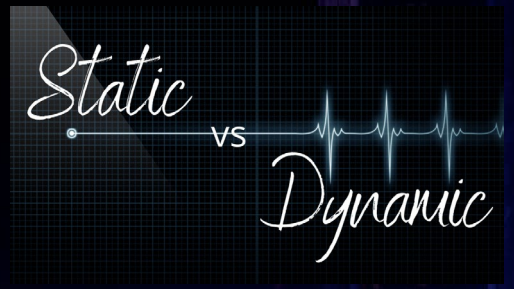
A majority of systems

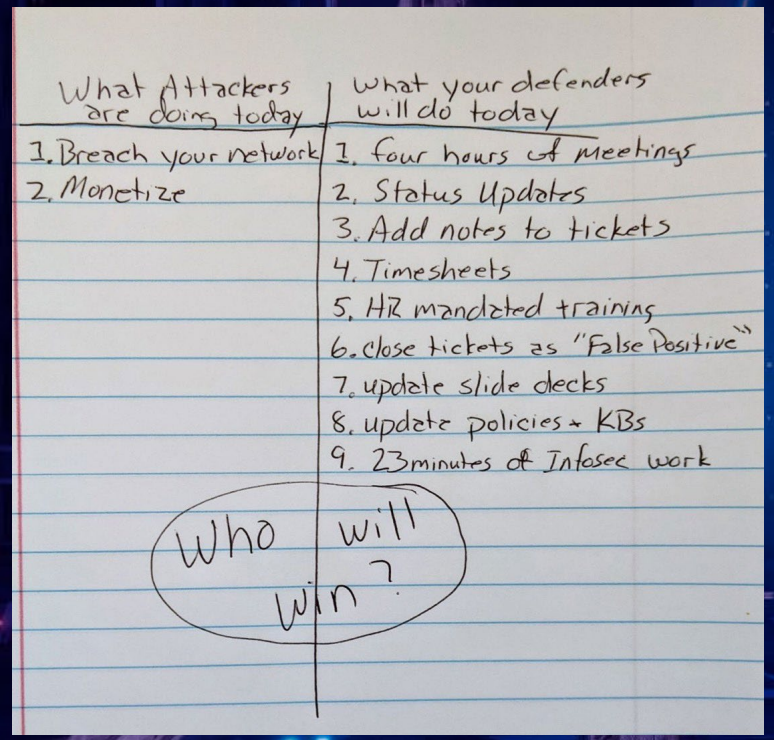
The attacker can:

1. Find a system
2. Gather intel about this system
3. Analyze the collected intel
4. Scrupulously prepare an attack
5. Launch a successful attack

All this time, the owner of the system:

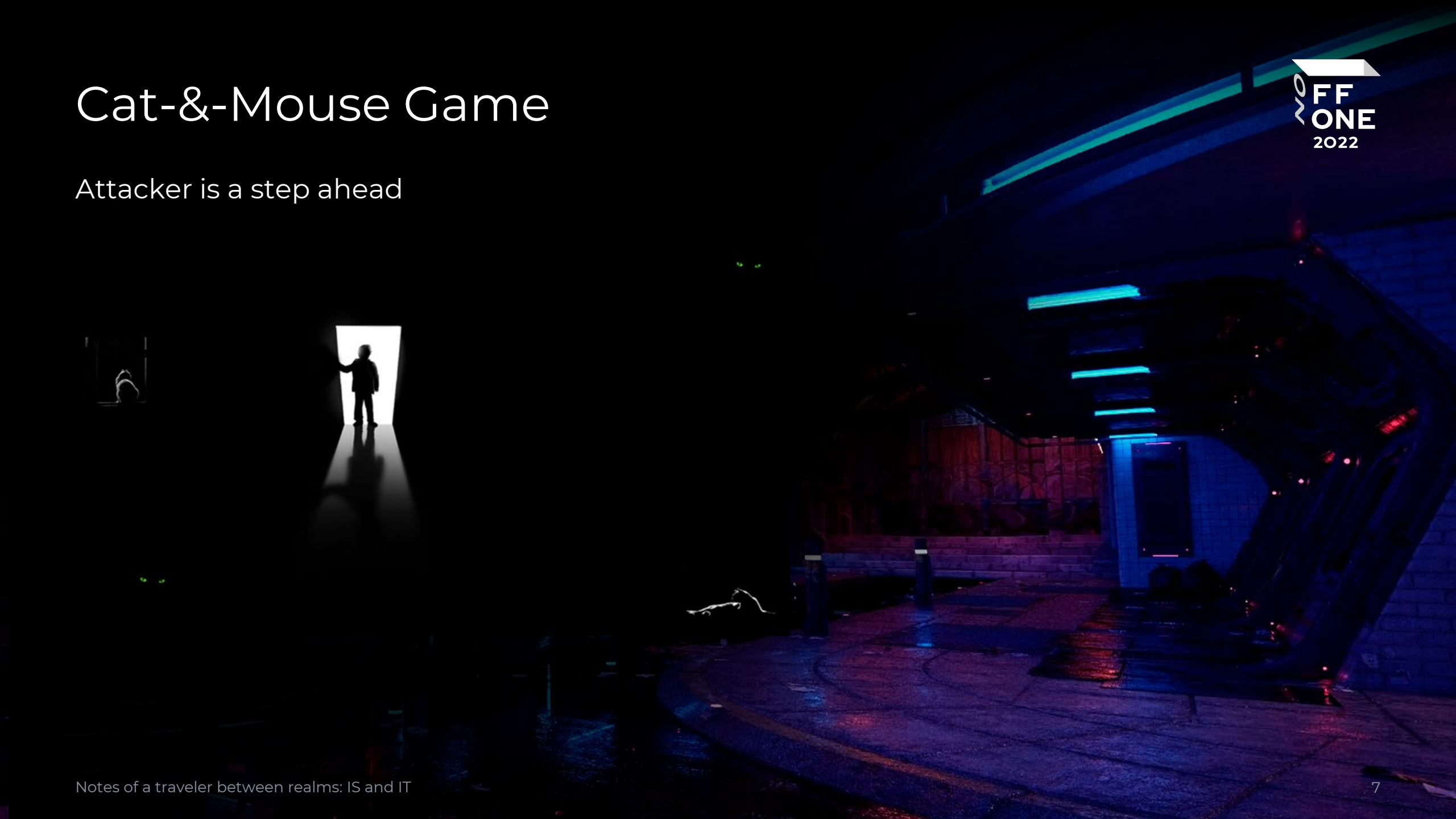
- Isn't even close to detecting the attacker
- Doesn't try to spoil the attacker's game





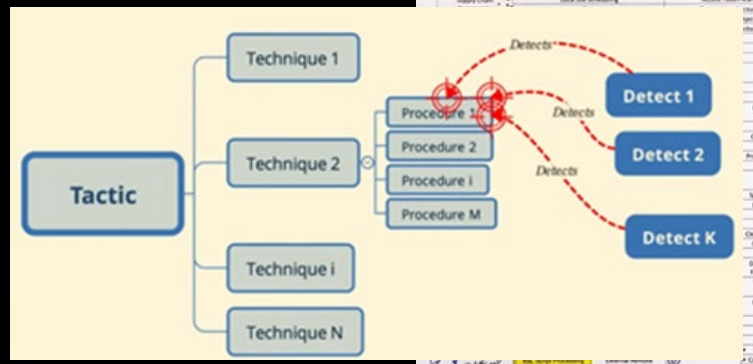
Cat-&-Mouse Game

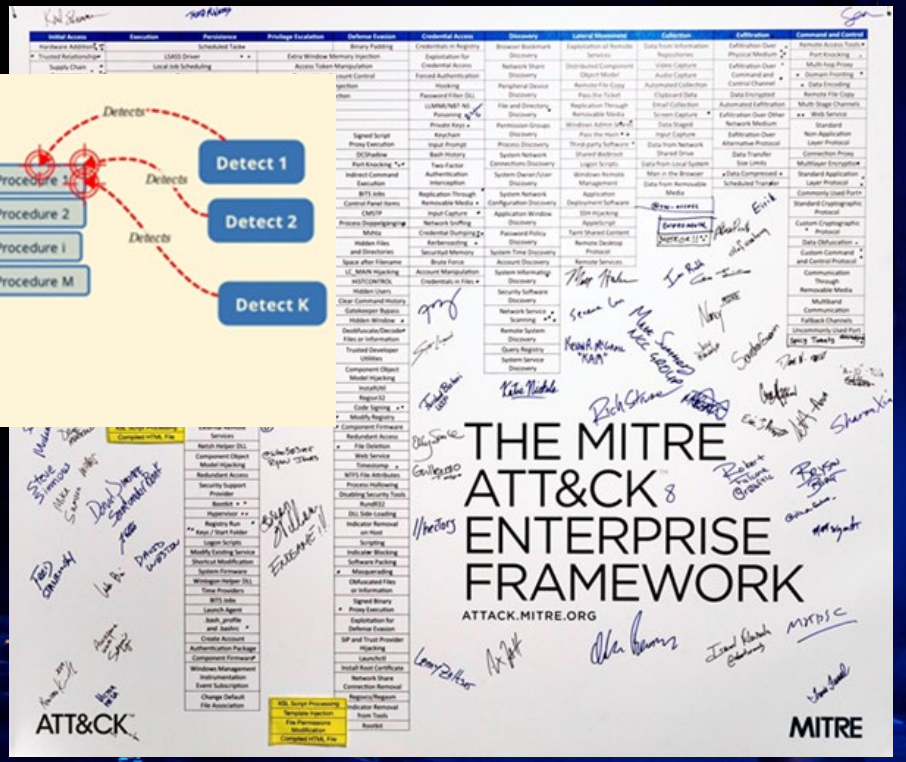
Attacker is a step ahead

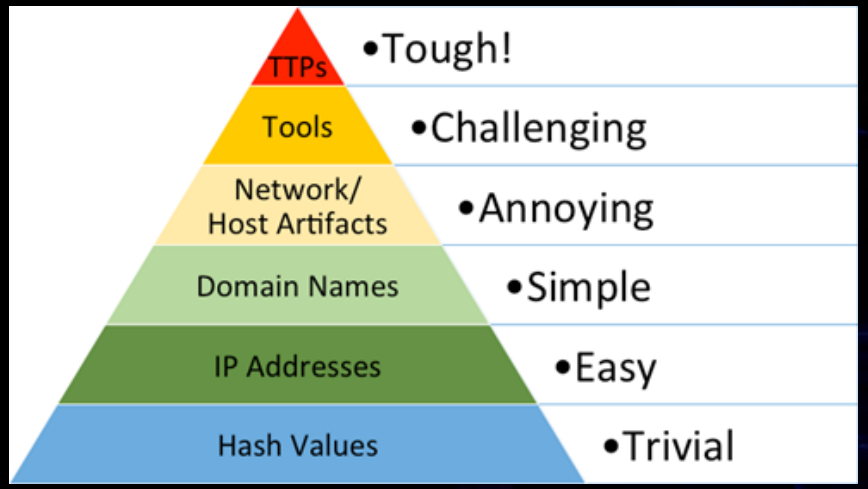


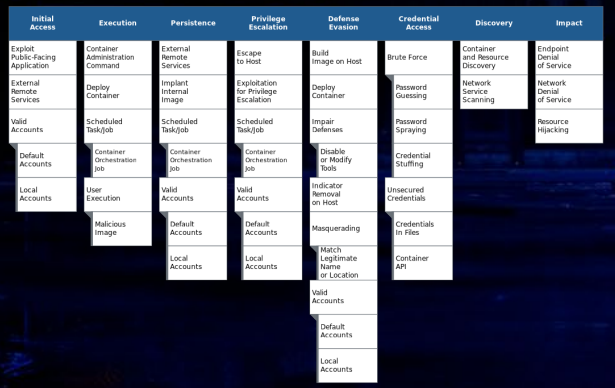
MITRE ATT&CK Matrix

- Adversarial Tactics, Techniques & Common Knowledge
- Reactive approach …
  - KNOWN ATTACKS ONLY!









Legitimate Software in Service

LOLBAS

☆ Star 4,616

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.

GTFOBins

☆ Star 7,188

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

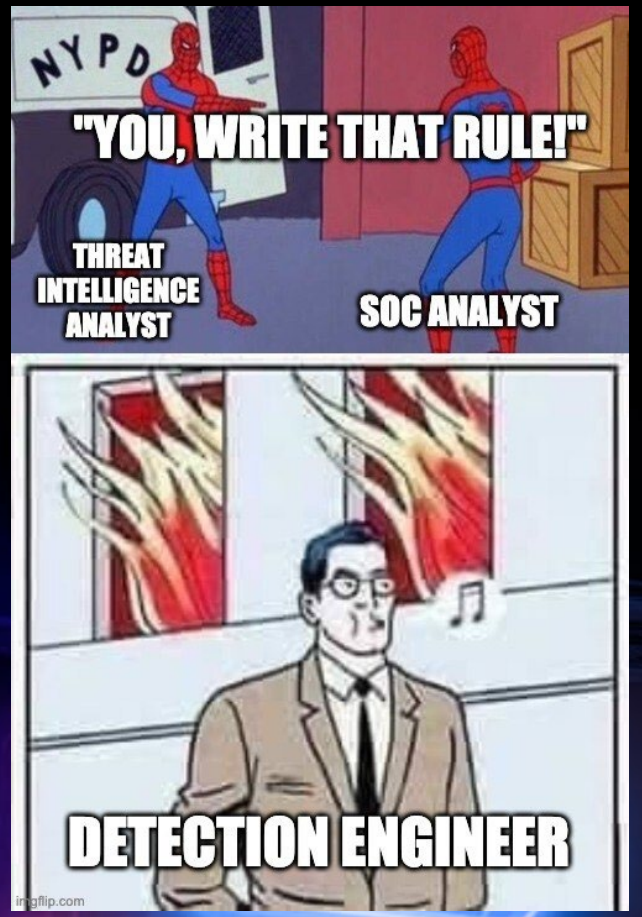
If you are looking for Windows binaries you should visit LOLBAS.

Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks

Written by **Nicole Fishbein** - 8 September 2020

Rules, Signatures, …

Based on a person's predefined knowledge

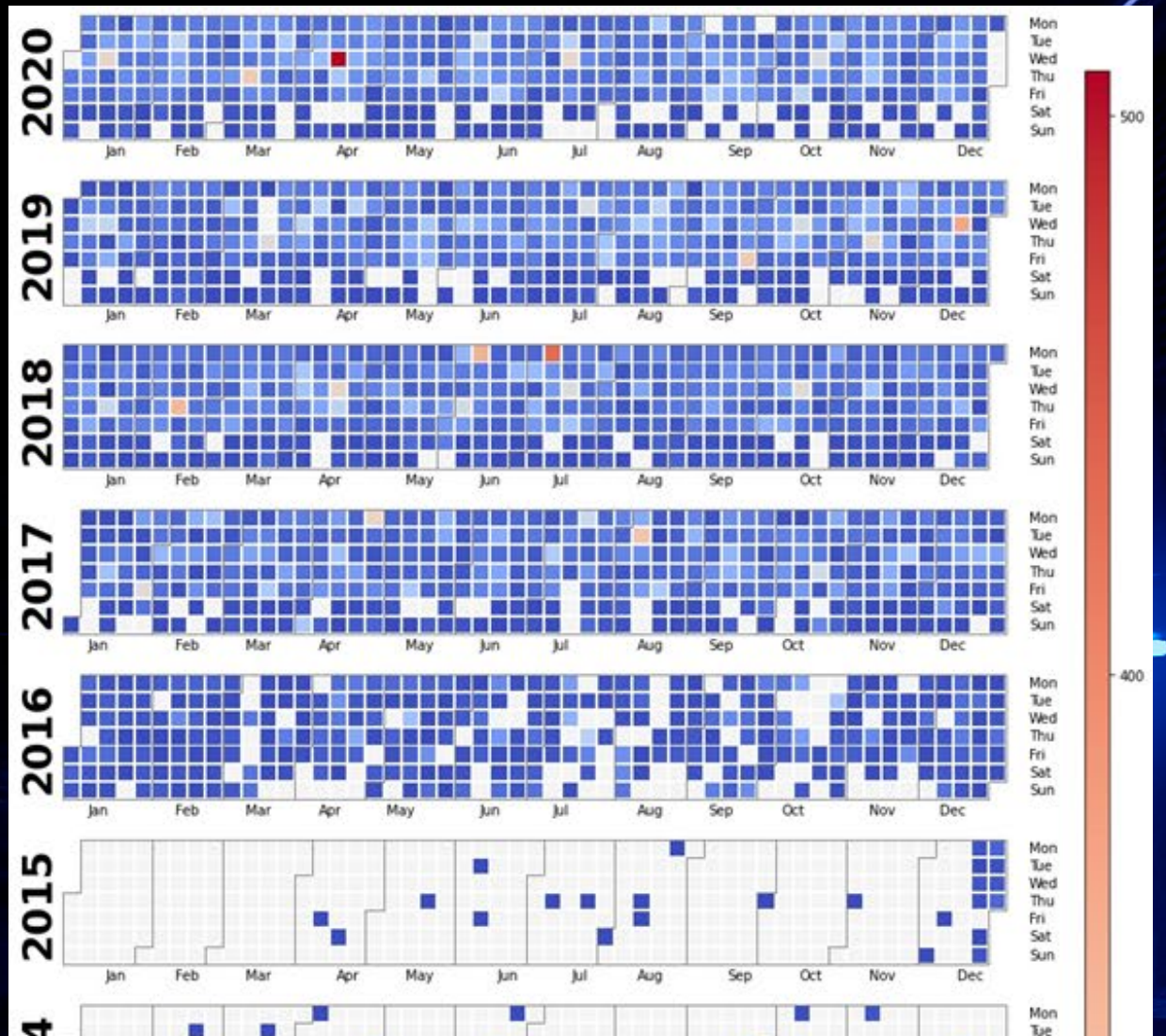


> The behavior of a piece of software does not determine whether it is malicious or not. The true defining line between malicious and non-malicious software is whether software ***does what the user expects it to do***.
>
> ***The question of malicious / non-malicious software is a question of alignment between user expectations and software behavior.***

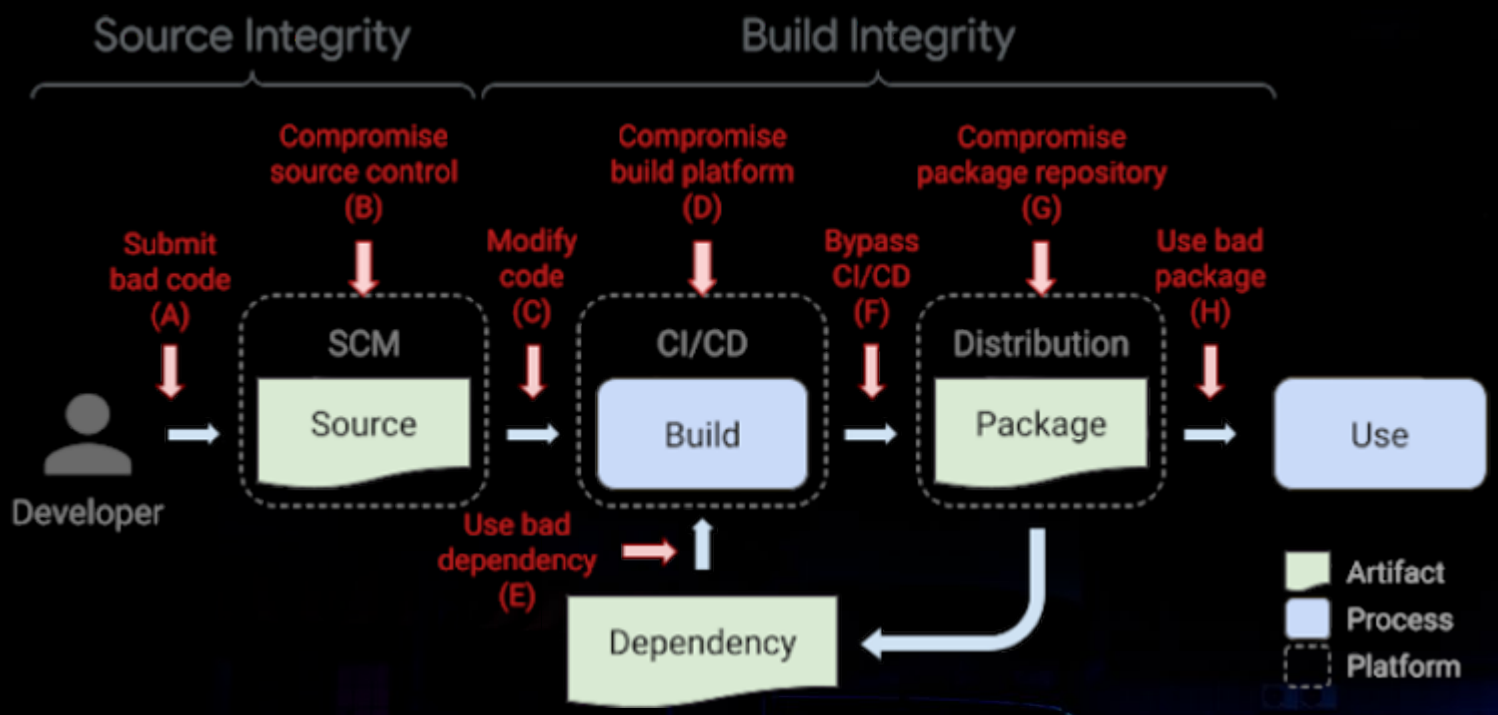
Halvar Flake

Vulns?! Backdoors?!

- Don’t be afraid of vulns.
- Know how to manage them.
- Know how to manage incidents.



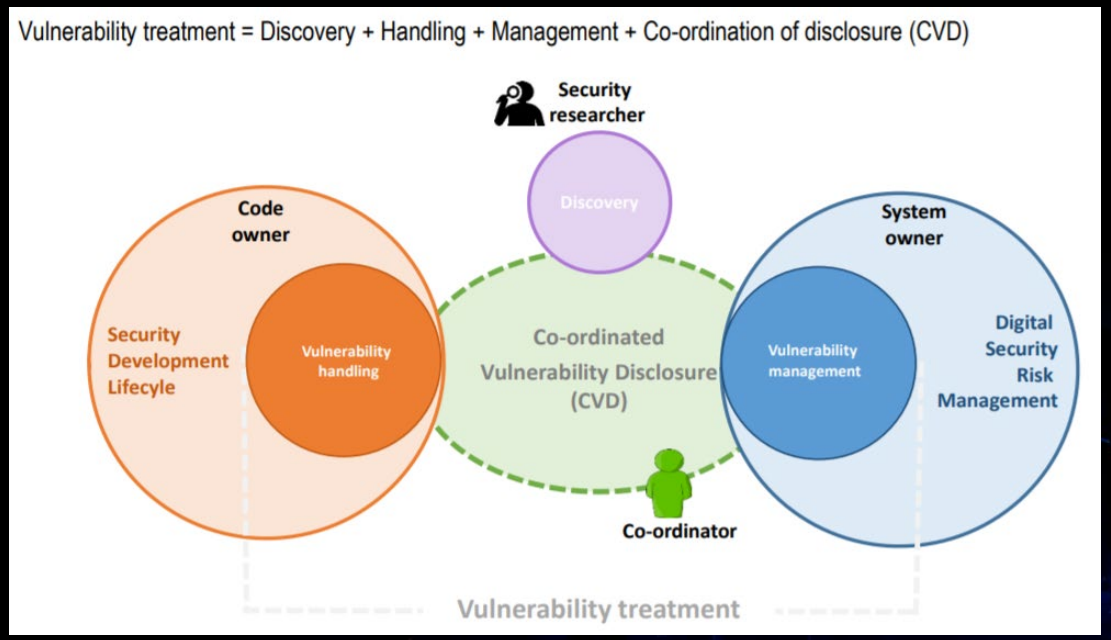
Supply Chain Attacks



"Introducing SLSA, an End-to-End Framework for Supply Chain Integrity"

Updates …

It’s not enough to update software to the latest version, it’s also necessary to make sure that fixed vulnerabilities have not been exploited before they’re fixed!



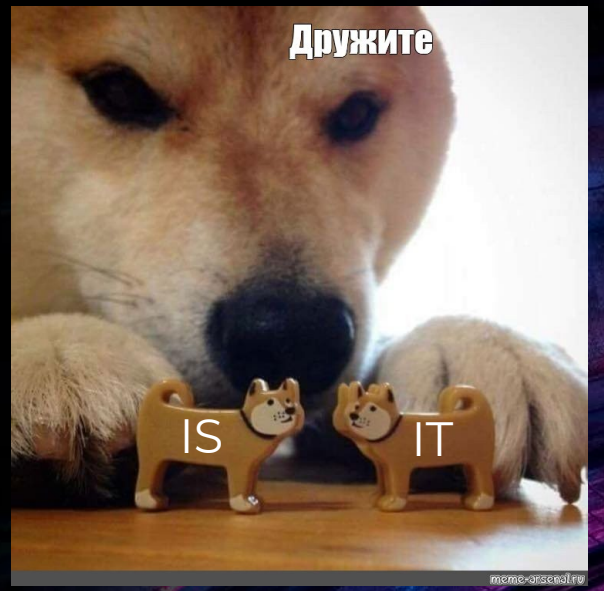
[ENCOURAGING VULNERABILITY TREATMENT]
[Responsible management, handling and disclosure of vulnerabilities]

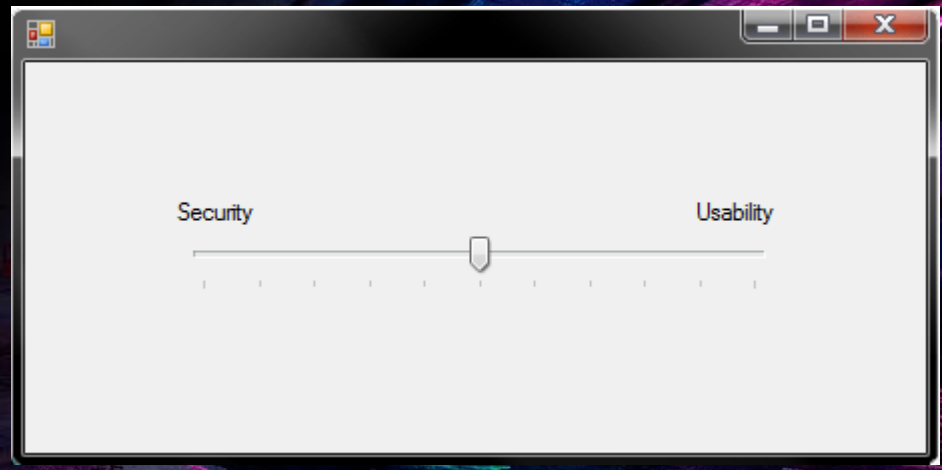
Conflict IS and IT

- Agile
- Time to market

For IT: speed, efficiency, cost-effectiveness, reliability

For IS: security






ON
FF
ONE
2022
Are DevSecOps, ShiftLeftSecurity the Solution?
LUNTRY

NEW: SecDevSecOpsSec

Marketing ...

- SecDevOps
- DevSecOps
- DevOpsSec

blog.sqreen.com › secdevops ▾ Перевести эту страницу

What is SecDevOps and why should you care? - Sqreen Blog

19 июл. 2017 г. — What is **SecDevOps**? **SecDevOps** (also known as DevSecOps and DevOpsSec) is the process of integrating secure development best practices ...

www.altexsoft.com › blog › w... ▾ Перевести эту страницу

What is SecDevOps and Why is It So Important? | AltexSoft

12 дек. 2019 г. — **SecDevOps** is the process of integrating security right into the development and deployment workflows. Learn how your product and team can ...

resources.whitesourcesoftware.com › ... ▾ Перевести эту страницу

DevSecOps VS SecDevOps: What Are The Differences?

21 мая 2020 г. — **SecDevOps** Puts Security First, Literally. For those who argue there is a difference between DevSecOps and **SecDevOps**, it is about putting ...

www.acunetix.com › blog › d... ▾ Перевести эту страницу

DevSecOps vs. SecDevOps | Acunetix

24 сент. 2019 г. — It is an extension of DevOps (Development + Operations) that includes security. The order of component terms in the DevSecOps name, however, ...

www.csoonline.com › article ▾ Перевести эту страницу

DevOpsSec, SecDevOps, DevSecOps: What's in a Name ...

18 окт. 2016 г. — The world is awash in DevOps, but what does that really mean? Although DevOps can mean several things to different individuals and ...

www.capgemini.com › secdev... ▾ Перевести эту страницу

SecDevOps: Cybersecurity Innovation - Capgemini

11 нояб. 2019 г. — I'm delighted today to be joined by Capgemini cybersecurity expert Luis Delabarre. This topic is known as **SecDevOps**. It's the process of ...

blog.newrelic.com › technology ▾ Перевести эту страницу

SecDevOps: Injecting Security Into DevOps Processes

16 июл. 2018 г. — Think of **SecDevOps**—practitioners are sometimes called "Security DevOps Engineers"—as a set of best practices designed to help organizations ...

blog.ariacybersecurity.com › ... ▾ Перевести эту страницу

DevSecOps vs. SecDevOps vs. DevOpsSec: Is there really a ...

14 июн. 2018 г. — **SecDevOps**: To borrow from "Goldilocks and the Three Bears," this approach is just right! According to this insightful article on CSO.com, ...

Tabitha Sable
@TabbySable

LRT: DevSecOps doesn't exist, because when you actually do it... that's called DevOps

7:02 PM · 15 апр. 2021 г. · Twitter for iPhone

DEVOPS IS DEAD

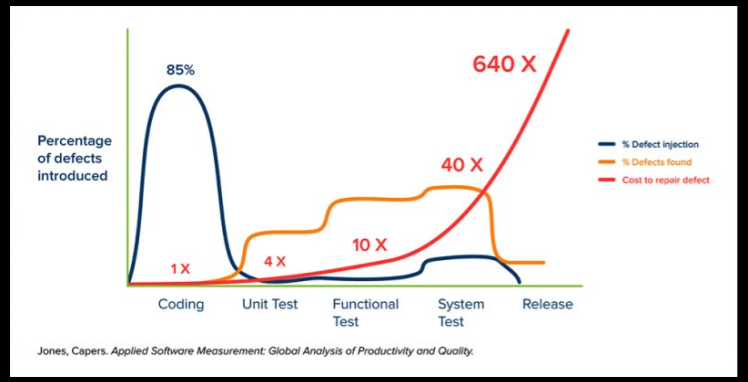
LONG LIVE DEVOPS

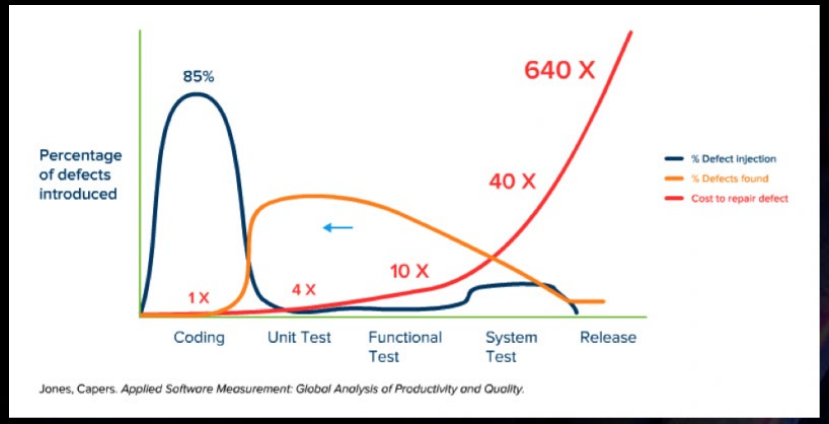
- GitOPS
- DevSecOPS
- SecDevOps
- Configuration as CODE

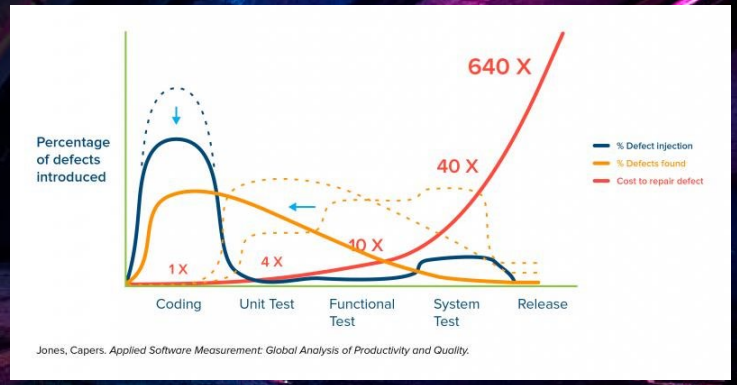
Dr. Anton Chuvakin
@anton_chuvakin

So, it turns out that because somebody coined the acronym "DevSecOps", now there are clowns who assume that "DevSecOps" includes security operations (like SOC, etc), because the silly word DevSecOps includes SecOps. WTH and perhaps even WTAF...

Shift Left Testing







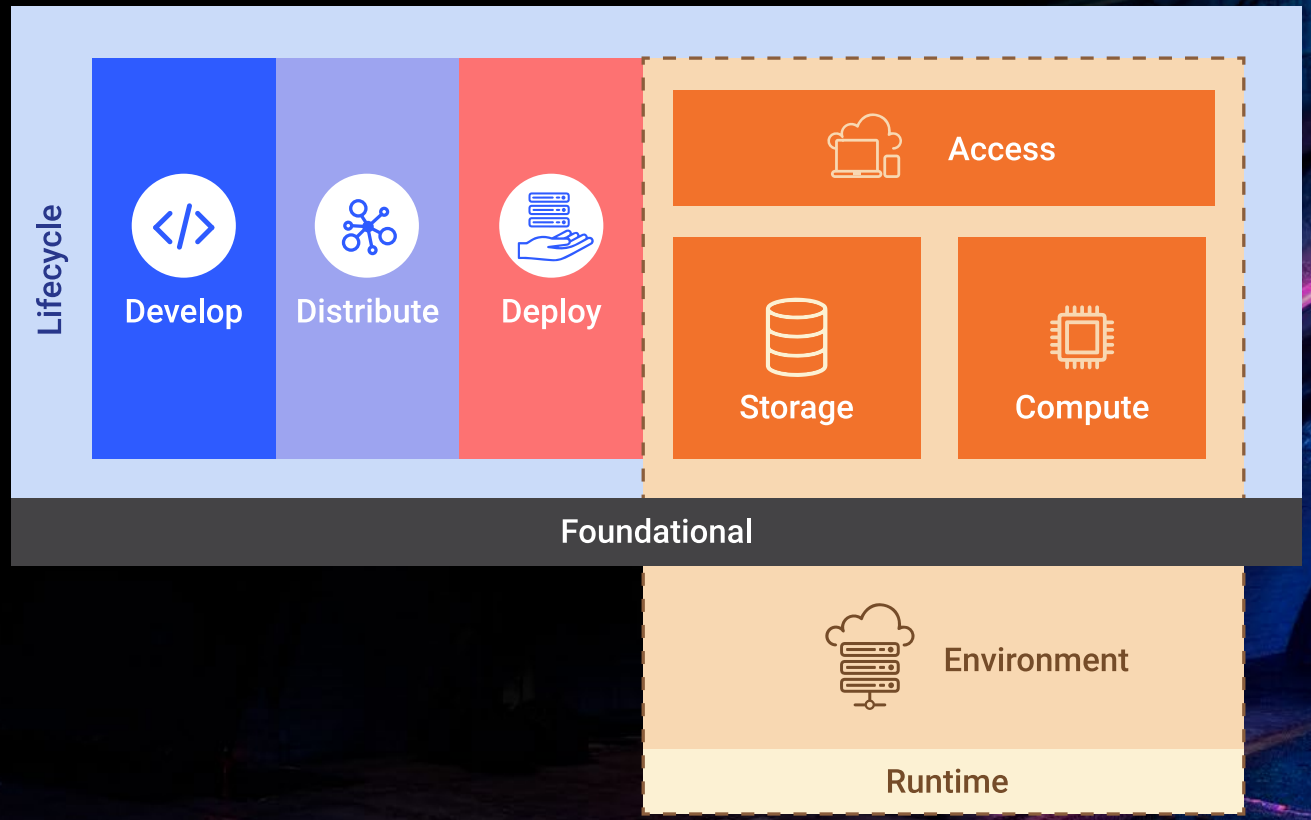
Shift ~~Left~~ Everywhere Security

"Shift Left" is becoming "Shift Everywhere."

- Although shift left has been promoted as doing some security testing during development, that is a large simplification of what we meant. More accurately today, some secure software development lifecycles (SSDLs) seek to conduct an activity as quickly as possible with the highest fidelity as soon as the artifacts on which that activity depend are made available. Sometimes, that's to the left of where you're doing things today, but often times, it's to the right. In addition, technology trends naturally require shifting right to produce rapid and accurate telemetry from modern languages, frameworks, and software orchestration.
- Established practices such as secure code review are leveraging enhanced source code management features to allow review during multiple phases. For example, shift left to initial code commits and shift right to augment metadata offered as part of pull requests sent to repository maintainers when code is finished and tested. These options reflect a desire to present results both where they can be achieved the soonest and where they will be most impactful.
- Some organizations evaluating defect discovery tools and services are showing a growing preference for continuous event-based security telemetry throughout a value stream rather than a single point-in-time analysis.
- Those organizations attempting to maintain accurate software inventory data are discovering the need to align efforts across source code content management, the build process, the deployment process, and the operations environment, where inventory granularity and content will likely be different with each view and will also change frequently. Such organizations are struggling to maintain the effectiveness of their existing inventory efforts while also adapting to new software lifecycles, software architecture changes and any underlying software, deployment, and cloud technologies changes happening in response to the engineering self-service trends and the digital transformation sea change.

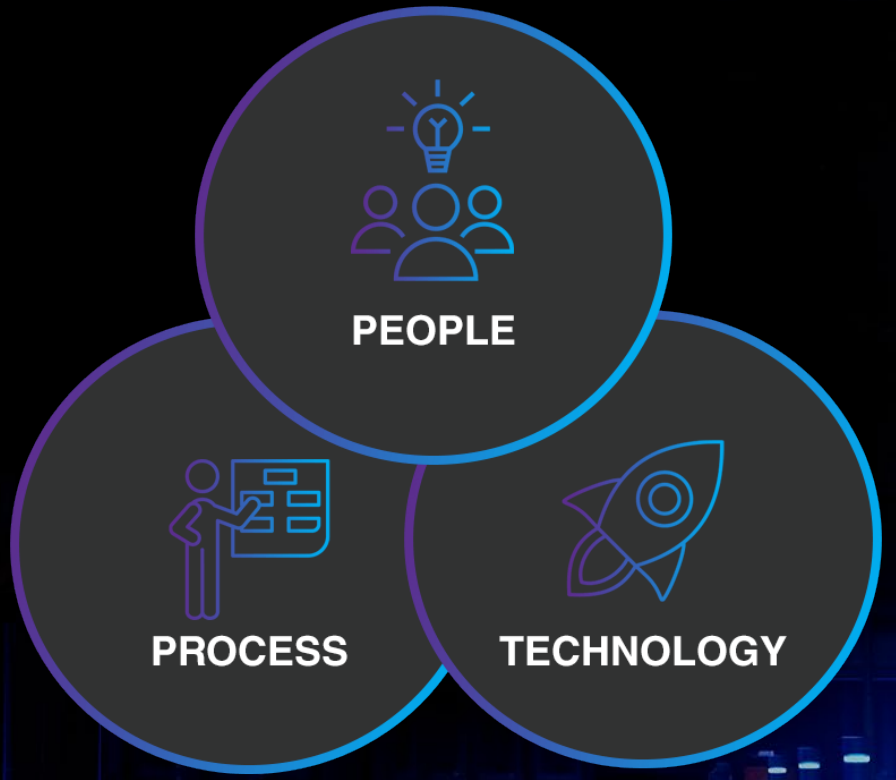
Building Security In Maturity Model (BSIMM) 11

Runtime Security




ON
FF
ONE
2022
What to Do About It?
This is where my love for containers and Kubernetes begins
LUNTRY

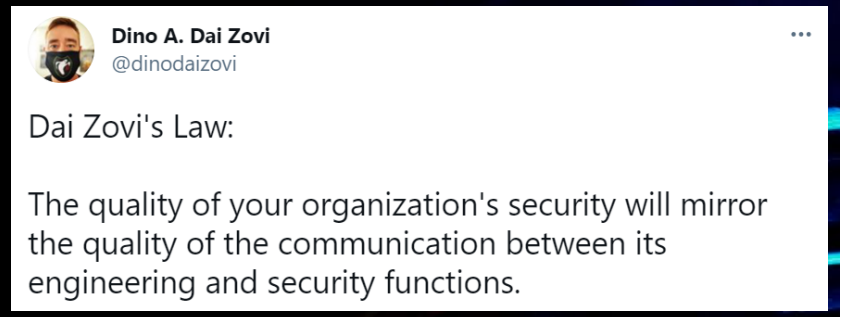
People, Process, Technology

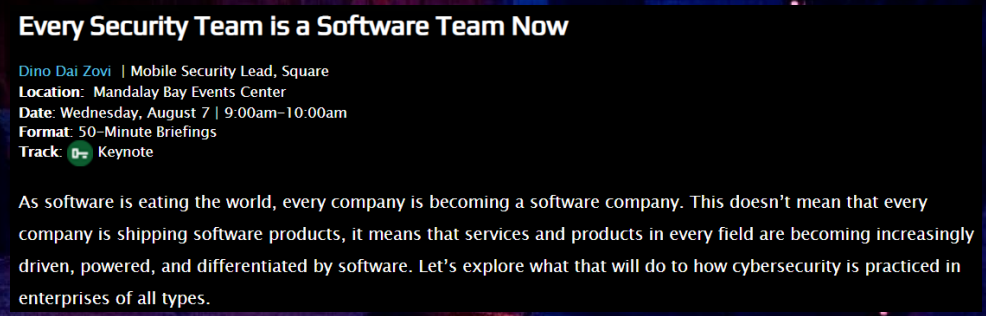


Synergy of Two Worlds

IS vs IT

- Orchestration
  - SOAR
- Declarative approach
  - Policy\Security-as-Code
- Unification
  - Templating, Immutable infrastructure
- Optimization
  - Attack surface reduction
- Micro segmentation
  - ZeroTrust





Security Observability

“Observability” is being able to fully understand our systems. In control theory, observability is a measure of how well internal states of a system can be inferred from knowledge of its external outputs. The observability and controllability of a system are mathematical duals.”

You can’t make something that is hidden from your eyes safe and secure

Environment without blind spots.

Simply put, advanced inventory.

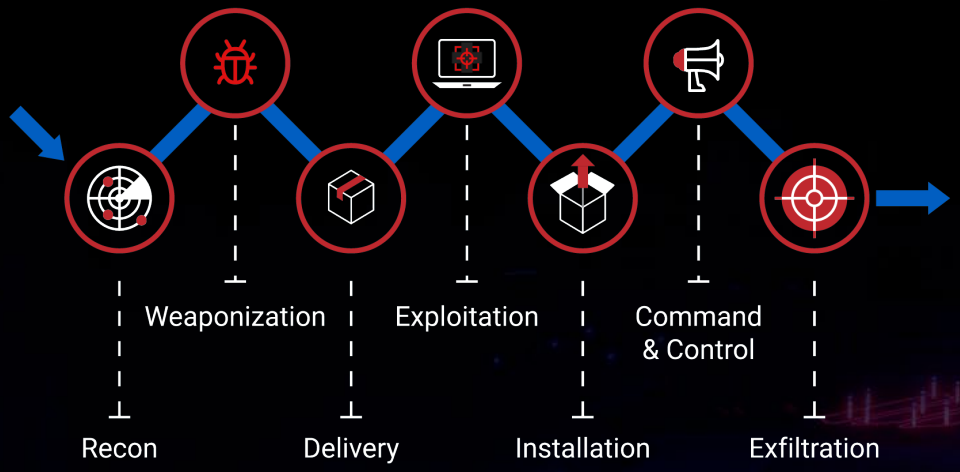
Continuous inventory -> Continuous security (an addition to CI\CD)

Active Systems

From reactive to active security

Modern age – modern approaches

- A defender only has to make one mistake to get compromised.
- An attacker only has to make one mistake to get detected.



Dynamic Systems

Moving Target Defense (MTD)

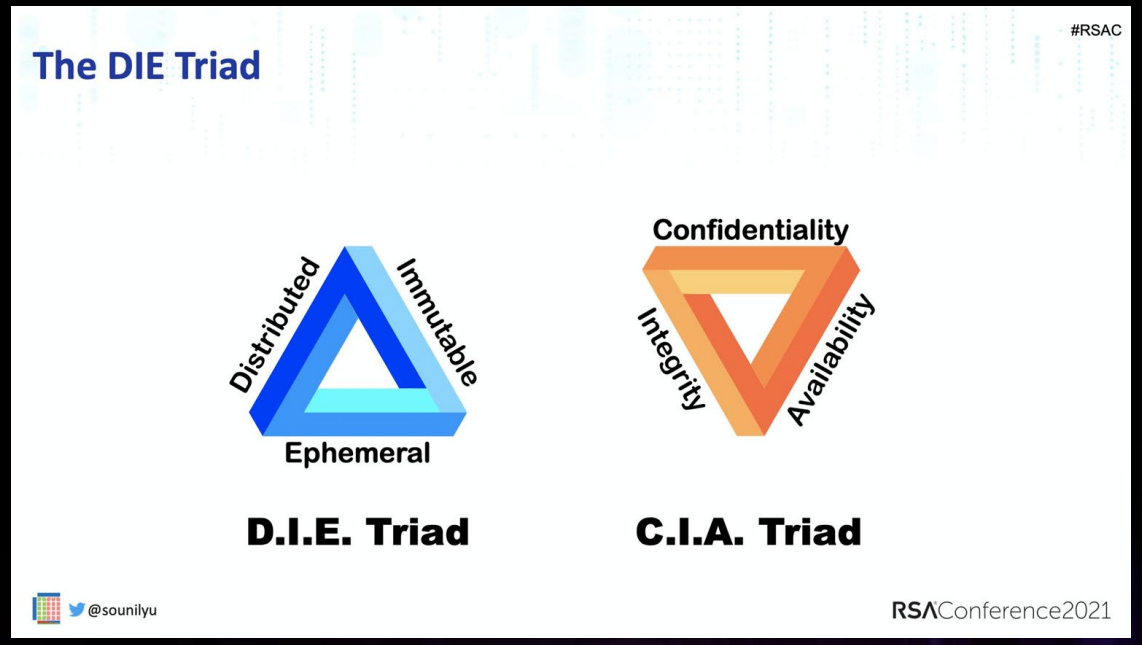
Key "DevSecOps" Ingredients

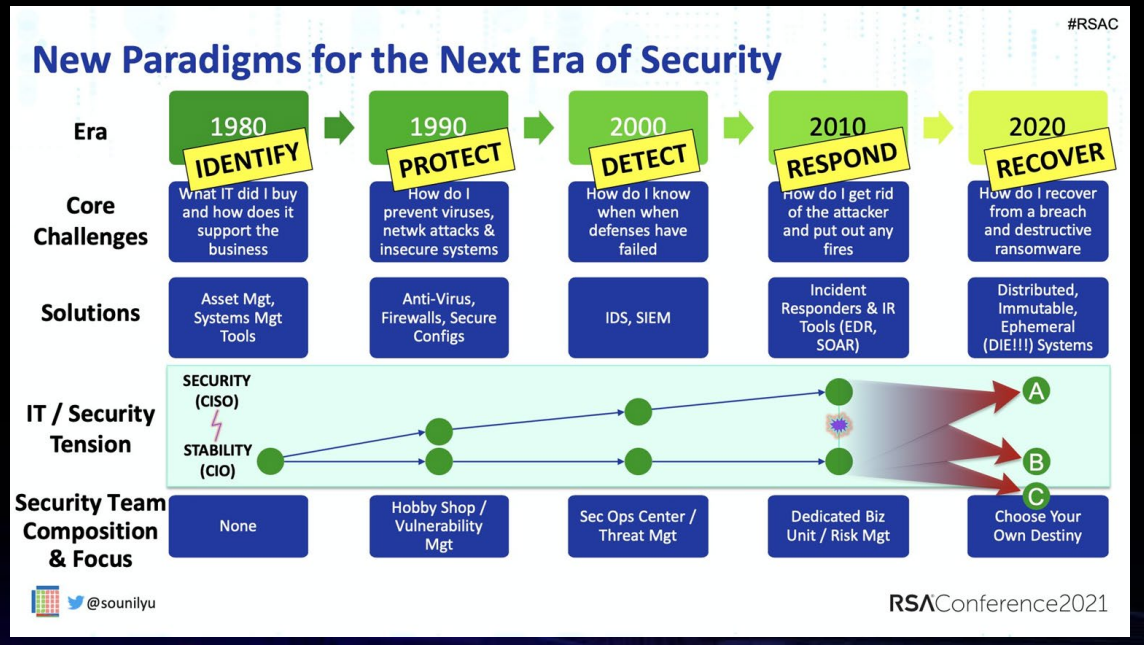
- **Abstracted**: to avoid drifts, be agnostic to environment (Cloud/on-premise/classified/disconnected…) and prevent lock-ins with Cloud or Platform layers, we leverage CNCF compliant Kubernetes and OCI compliant containers - open source stacks with U.S eyes on code and continuous scanning,
- **GitOps / Infrastructure as Code (IaC):** no drift, everything is code (including configuration, networking etc.) Instantiate entire stack automatically,
- **Continuous Integration/Continuous Delivery pipeline (CI/CD)**: fully containerized and using Infrastructure as Code (IaC),
- **Hardened Containers**: hardened "Lego blocks" to bring options to development teams (one size fits all lead to shadow IT)
- **Software Testing**: mandated high test coverage,
- **Baked-in Security**: mandated static/dynamic code analysis, container security, bill of material (supply chain risk) etc.
- **Continuous Monitoring:**
  - **Centralized logging and telemetry**,
  - Automated alerting,
  - **Zero trust**, leveraging Service Mesh as Sidecar (part of SCSS), down to the container level,
  - **Behavior detection** (automated prevention),
  - CVE scanning,
- **Chaos engineering**: Dynamically kills/restarts container with moving target defense.

Integrity - Service - Excellence

"How did the Department of Defense move to Kubernetes and Istio?"

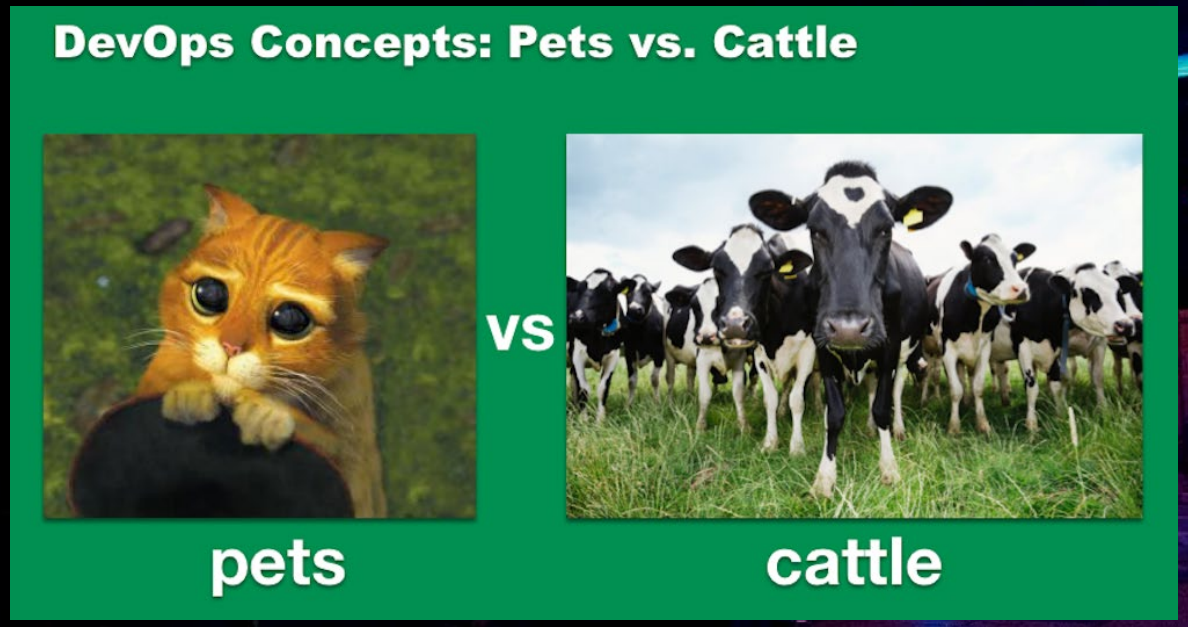
DIE Paradigm





"Death to CIA! Long live DIE! How the DIE Triad Helps Us Achieve Resiliency", Sounil Yu

Cattle and Pets



Our best countermeasure is to **avoid pet creation** (that requires CIA) and **promote cattle creation** (built to DIE)


ON
FF
ONE
2022
In Lieu of Conclusion ;)
LUNTRY

Thank you for your attention!

Contacts:

- Email: de@luntry.ru
- Twitter: @evdokimovds
- Tg: @Qu3b3c
- Channel: @k8security
- Site: www.luntry.ru