OCT 2024

Insider Threat Inside Out

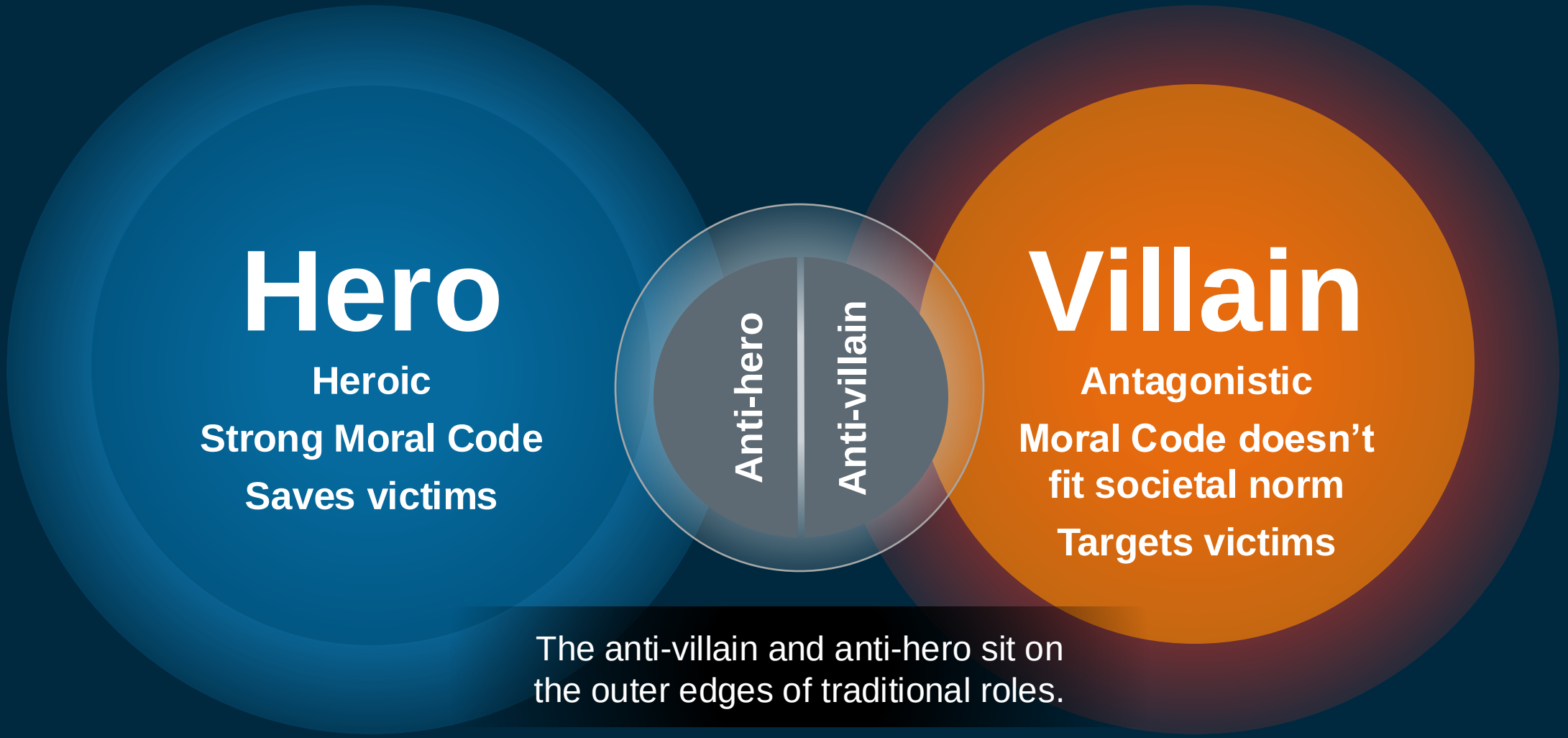
Dale Beauchamp

Focused Operations

Agenda

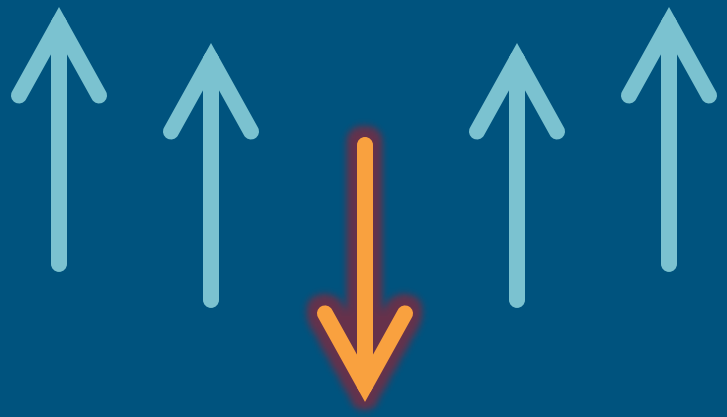
- Insider Threat Baseline
- Changes Based on Trends
- False Employees
- Detection
- Case Review

Hero versus Anti-hero



The anti-villain and anti-hero sit on the outer edges of traditional roles.

Insider Threat Defined

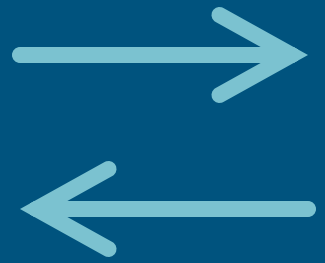


One or more individuals with **access** and/or **insider knowledge** that allows them to exploit vulnerabilities with the intent to cause harm.

This includes direct risks associated with a company's programs and operations, as well as the indirect risks that may compromise critical infrastructure.

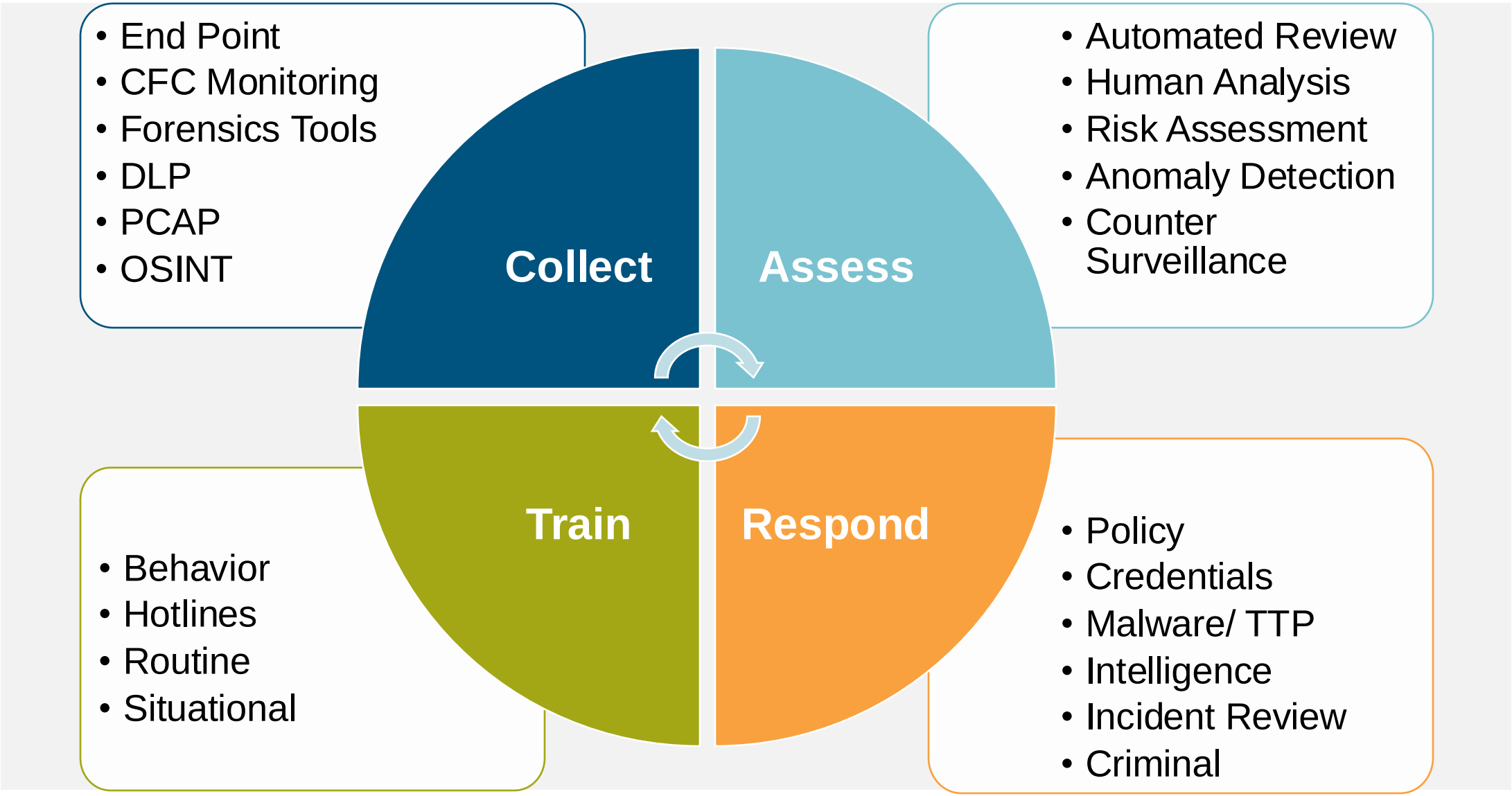
Insider Types

What Changed?



- **COVID-19 created increased need for remote work**
  - Hiring, managing, and working remote require new skills
  - Identity and work validation
  - Manage to outcome vs output
- **Generative AI**
  - Document review and creation (resumes)
  - Image/video creation and enhancement

Insider Threat Detection Cycle C.A.R.T.



Pre-Employment Phase Anomalies

Identity

- Has identity documents that are **forged or stolen**.
- Has online presence and social media **profiles that conflict or don't match resume** details.

Background

- **Provides fraudulent credentials** - professional or educational.
- Has **vague descriptions** of past jobs with employers that have no online presence.
- **Past roles and skillsets don't match.**

Behavior

- Uses **different names** on multiple professional accounts.
- Has intermediaries apply for jobs on their behalf.

Onboarding Phase Anomalies

Identity

- Has identity documents that:
  - Show signs of **tampering or digital alteration.**
  - **Don’t match** information from verification services.

Background

- **Provides conflicting details** or explanations for resume gaps or reasons for leaving past employers.
- **Cannot verify credentials** or provide references.
- Has history of **short tenures** with multiple employers.

Behavior

- **Reluctant to use video** communications, possibly to avoid identity verification.
- Requests payment before start date.
- Has **odd banking details** or requests payment through unconventional means.

Employment Phase Anomalies

Asset Misuse

- **Hides actual location** with remote or VPN services
- Uses unapproved remote access tools.
- Accesses or downloads **sensitive data unrelated to their work.**
- Transfers large amounts of data without authorization.
- Manipulates code, software, or **introduces vulnerabilities.**

Violations

- **Violates security policies.**
- Attempts to **bypass security measures** or gain access to sensitive areas of the IT infrastructure.
- Installs **unauthorized software or hardware** that could gather information or grant external access to the network.

Behavior

- Has **inconsistent work patterns** (time, location).
- Requests **early payment** or advance for no clear reason.
- Changes bank account details for deposits often.
- Struggles to build normal professional **relationships**.
- Expresses frustration if denied access to **specific projects.**

https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat

Thank You!

Dale Beauchamp

AMTRAK®