The OODA Loop for CISOs

Roselle Safran
roselle@keycaliber.com

Background

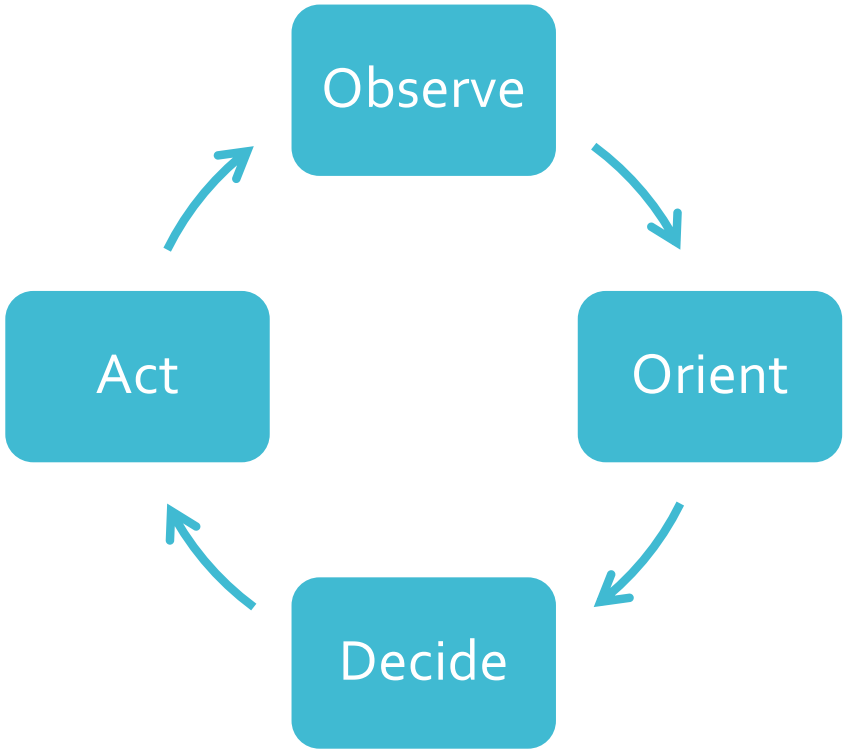
KeyCaliber

Uplevel Security

Executive Office of the President (Obama Administration)

Department of Homeland Security (US-CERT)

What is the OODA Loop?



KEYCALIBER

Benefits of the OODA Loop

- Increases agility
- Optimizes decision-making process
- Ensures continuous knowledge transfer
- Enables constant improvement

Tactical Versus Strategic OODA Loop

Tactical:

- Address immediate threats
- Optimize speed
- "Block & tackle"
- Narrow scope

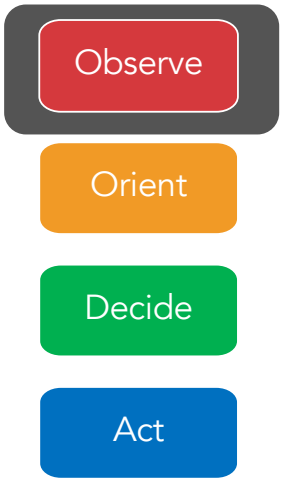
Strategic:

- Achieve long-term goals
- Optimize resource allocation
- Prioritize projects
- "Big picture"

Common Challenges to Strategic OODA Loop Implementation

- Observe/Orient cannot keep up with Decide/Act
- Decide/Act impact cannot be adequately measured
- Act requires collaboration with other teams
- Manual processes create bottlenecks

Thoroughly Observe



Frequency

- Match cadence of decisions-making process

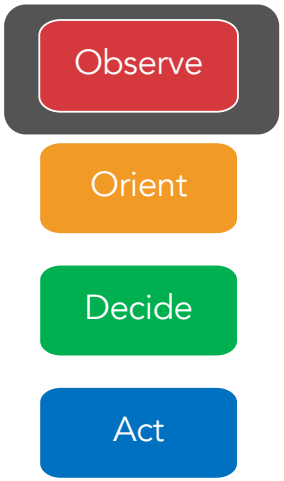
Your Organization

- Leverage existing security stack

Your Adversaries

- Utilize internal and external info

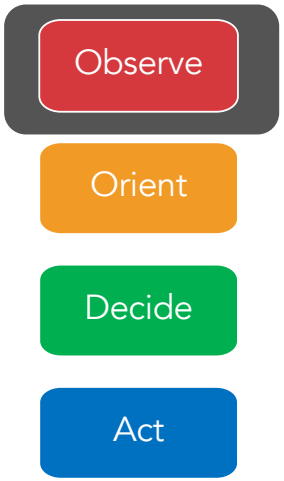
Know Your Organization – Data Sources



GRC Data	Cloud & Network Data	Application Data	Endpoint Data
• Critical assets • Risks	• Firewall • IDS • Cloud mgmt	• Email gateway • Vulnerability scanner	• EDR • AV

KEYCALIBER

Know Your Adversaries – Data Sources



Threat Intelligence

- Tactics, techniques, and procedures (TTPs)
- Internal
- External

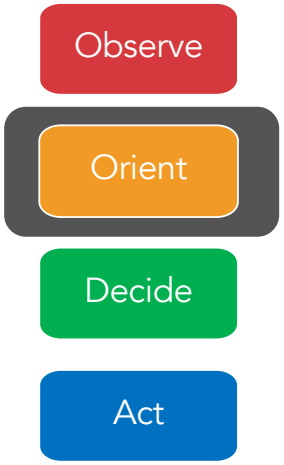
Alert/Incident Data

- Attribution
- Attack type
- Targeted assets

Open Source Data

- Current events
- Industry news

Orient By Strategic Impact



Critical to Operations

- Mission functions
- Business continuity

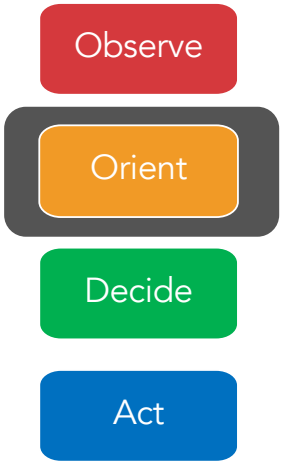
Valuable to Organization

- Intellectual property
- Financial data
- Customer data
- PII / PHI

Monetary Savings

- Risk reduction

Slice and Dice Observed Data



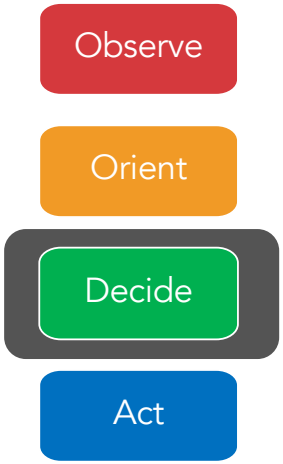
Aggregates

- Asset types
- Business units
- Locations

Trends

- Monthly
- Quarterly
- Yearly

Decide Based on the Numbers



Increase Revenue

- Added capability
- Differentiator

Reduce Risk

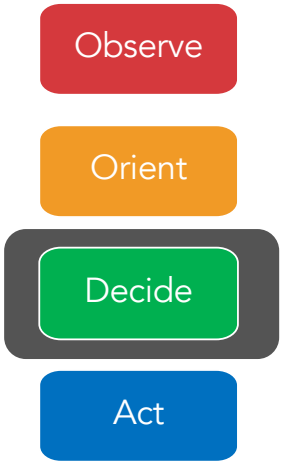
- Quantified current state
- Quantified future state

Reduce Costs

- Technology
- People
- Processes

KEYCALIBER

Decide Based on Comparisons



Frameworks

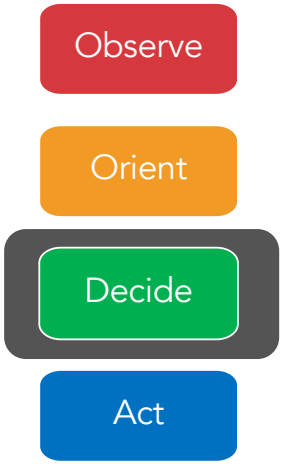
- NIST CSF
- CMMC
- CIS 20

Industry Peers

- Open source data
- Sector information sharing centers

KEYCALIBER

Decide Based on Priorities of Others



Board

- Fiduciary responsibilities

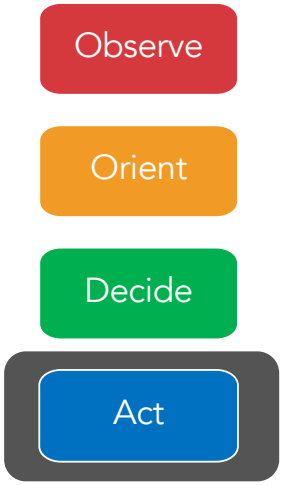
CEO

- Bottom line

CIO/ CSO/ CRO

- Regulations
- Accountability

Define Actions with OODA Loop Data



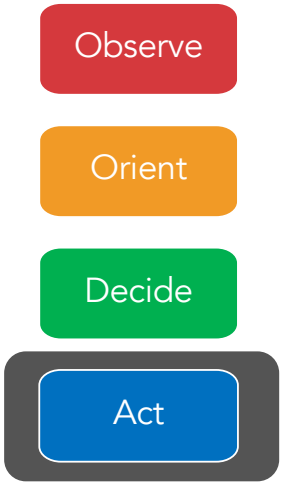
We have X [Observe],

which means Y [Orient],

so we will accomplish Z [Decide]

by doing A [Act].

Track Actions



What	Why	Who	When
• Decide & Act (project/task)	• Observe & Orient	• Responsible individual/ group	• Deadline

KEYCALIBER

Implementation Tips

- Develop each step of the process
- Measure with key performance indicators (KPIs) and metrics
- Document procedures with other business units
- Automate, automate, automate

Thank You!

Roselle Safran
roselle@keycaliber.com
https://www.linkedin.com/in/rosellesafran/
@rosellesafran