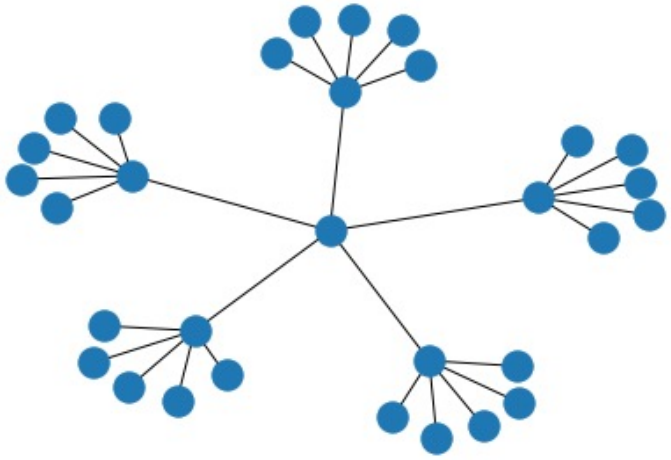
Economics of Continuous Assurance in Cybersecurity

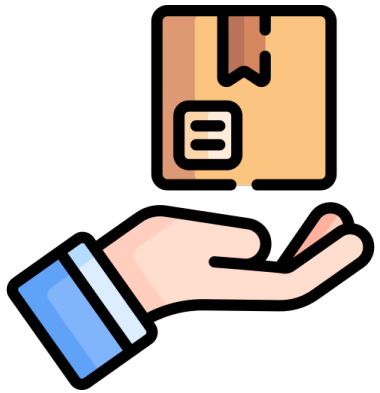
Macro and Micro Features in Tension

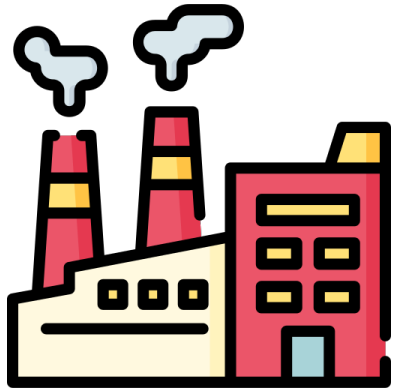
Interdependence



Decentralization

Elements of a Functioning Market





Market Failure Basics

Pursuit of Individual Incentives…

Leads to Sub-Optimal Group Outcomes

Reasons For Market Failure

Nature of the Market

Nature of the Goods

Nature of the Exchange

Two Obstacles to Efficient Markets in Security

Rational Inattention

Bargaining Costs

Rational Inattention Example

Scenario	Loss from Attack	P(Loss)	Expected Loss	Research Cost	Total Expected Loss
No Research	$10	50%	$5	$0	$5
Research	$10	10%	$1	$5	$6

Rational Inattention Example

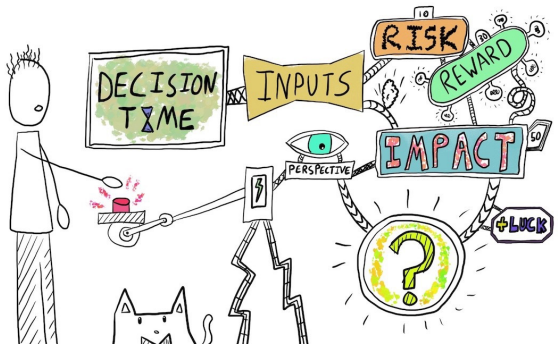
Scenario	Loss from Attack	P(Loss)	Expected Loss	Research Cost	Total Expected Loss	100x
No Research	$10	50%	$5	$0	$5	$500
Research	$10	10%	$1	$5	$6	$600

Rational Inattention Example

Scenario	Loss from Attack	P(Loss)	Expected Loss	Research Cost	Total Expected Loss	100x
No Research	$10	50%	$5	$0	$5	$500
Research	$10	10%	$1	$5	$6	$600
BigCo	100	50%	$50		$50	$5,000
BigCo (Pro Forma)	100	10%	$10		$10	$1,000

Bargaining Cost Examples

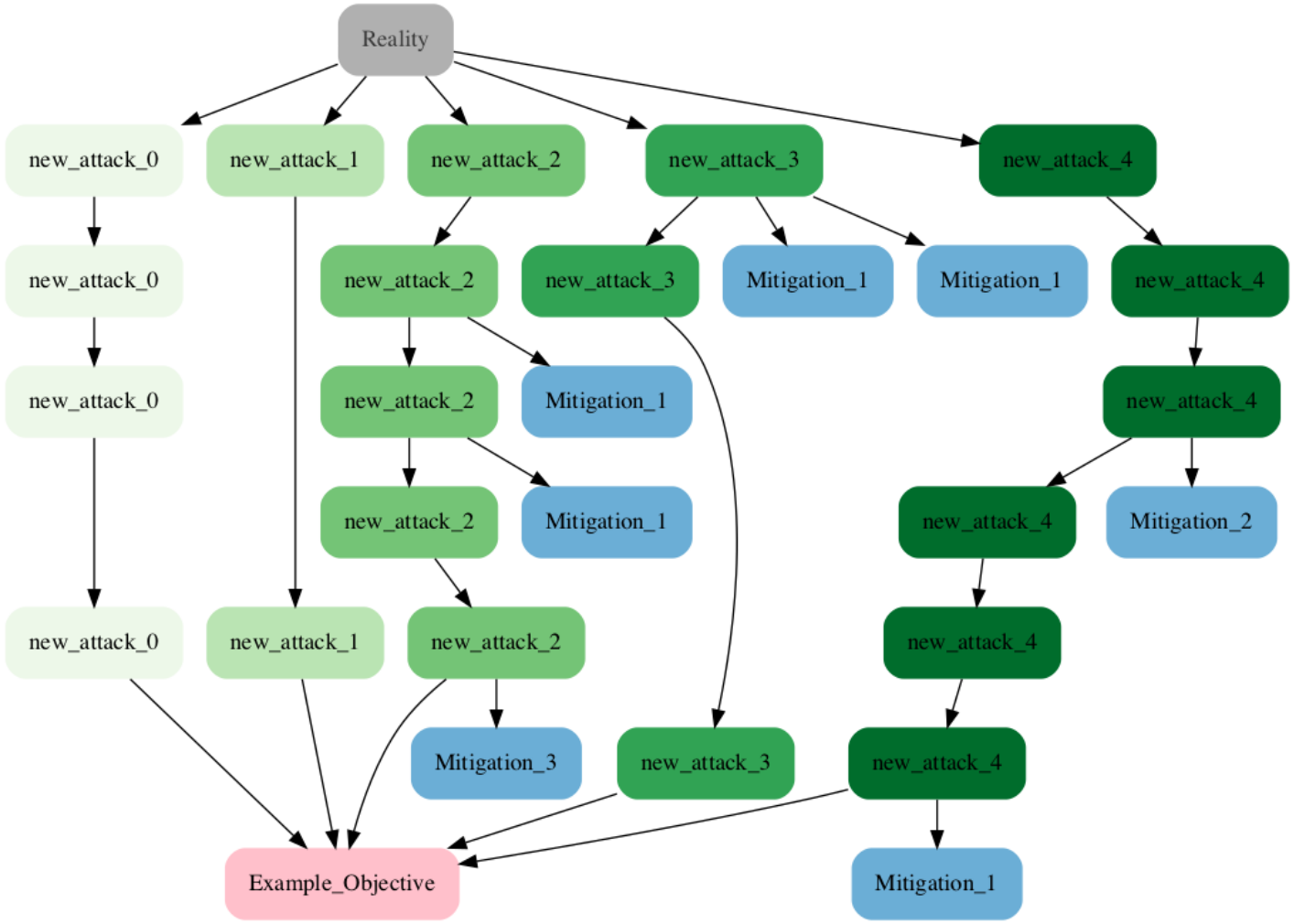
Search & Information Costs



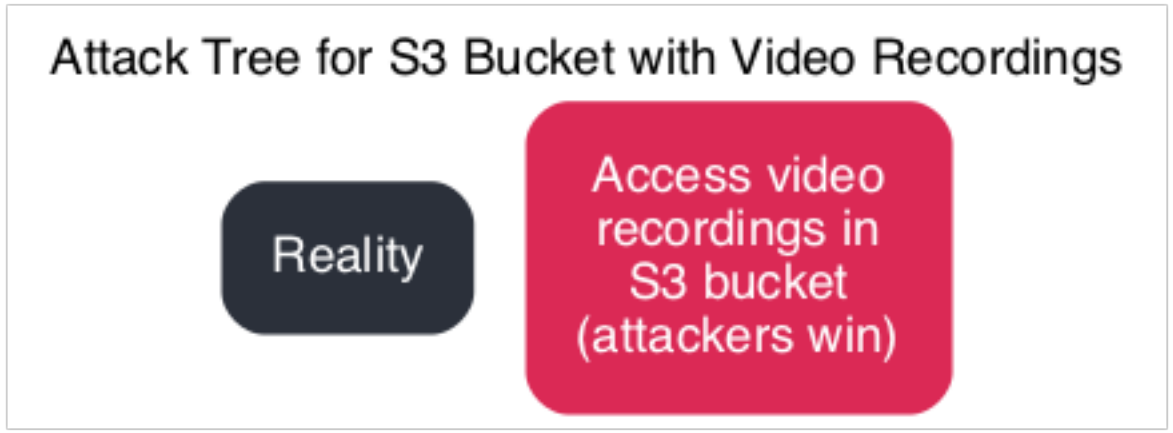
Decision & Coordination

Monitoring & Enforcement

Attack Trees Map Attacker Paths

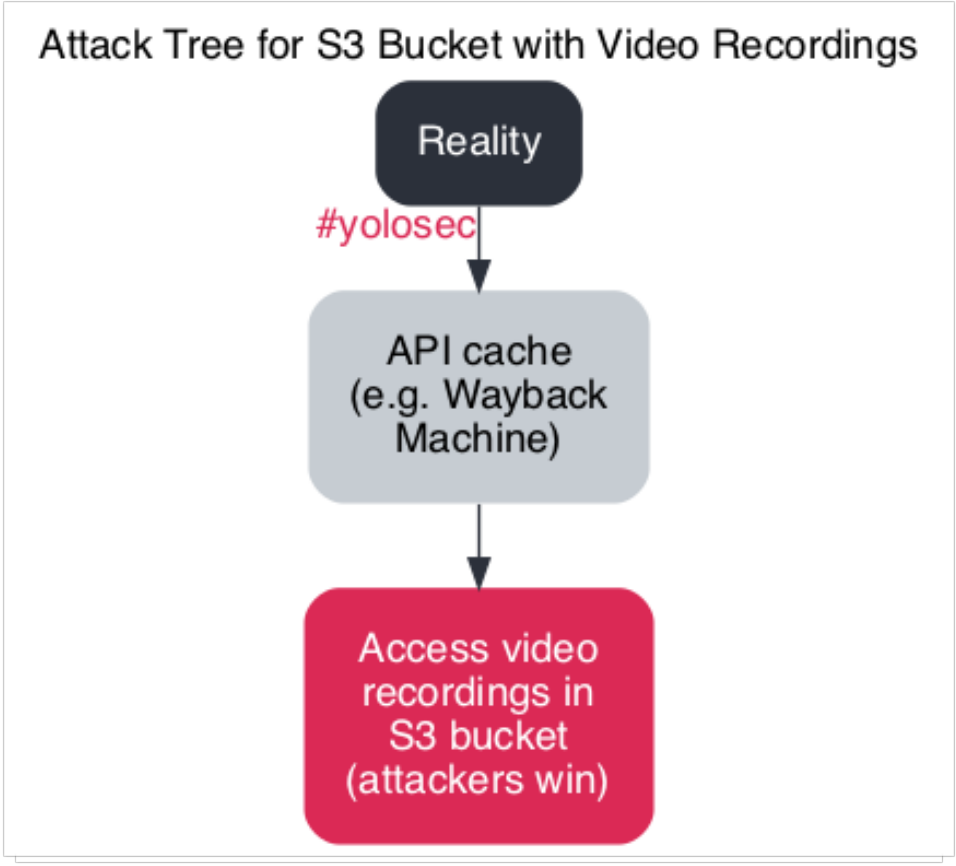


Building an Attack Tree



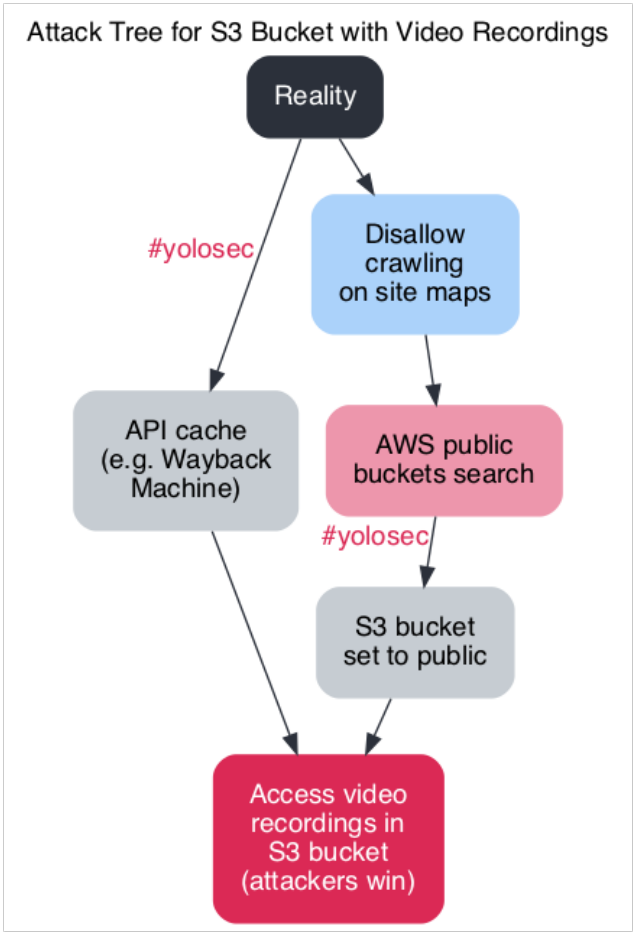
Source: https://swagitda.com/blog/posts/security-decision-trees-with-graphviz/

Building an Attack Tree



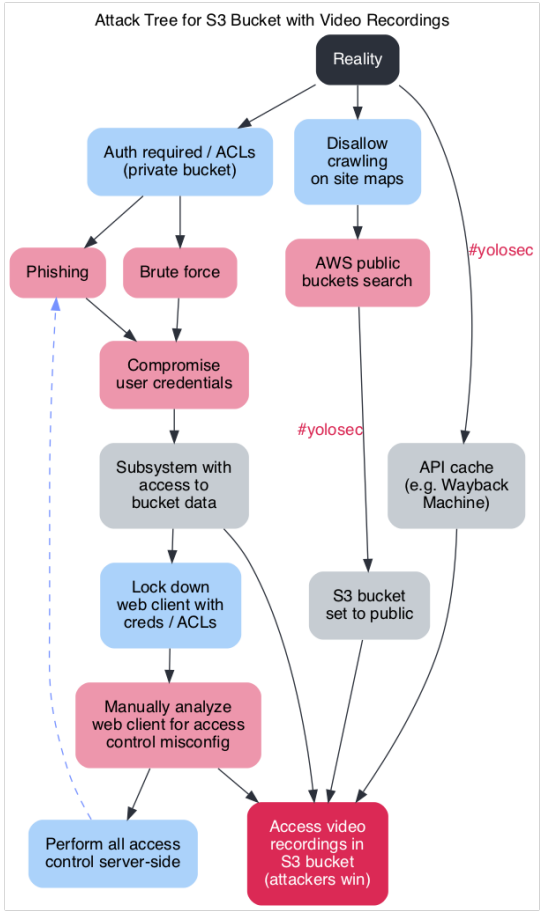
Source: https://swagitda.com/blog/posts/security-decision-trees-with-graphviz/

Building an Attack Tree



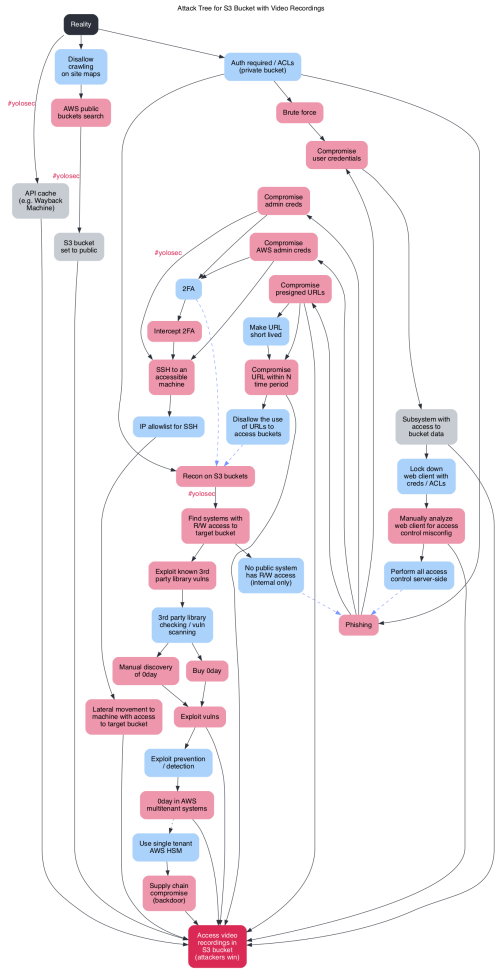
Source: https://swagitda.com/blog/posts/security-decision-trees-with-graphviz/

Building an Attack Tree



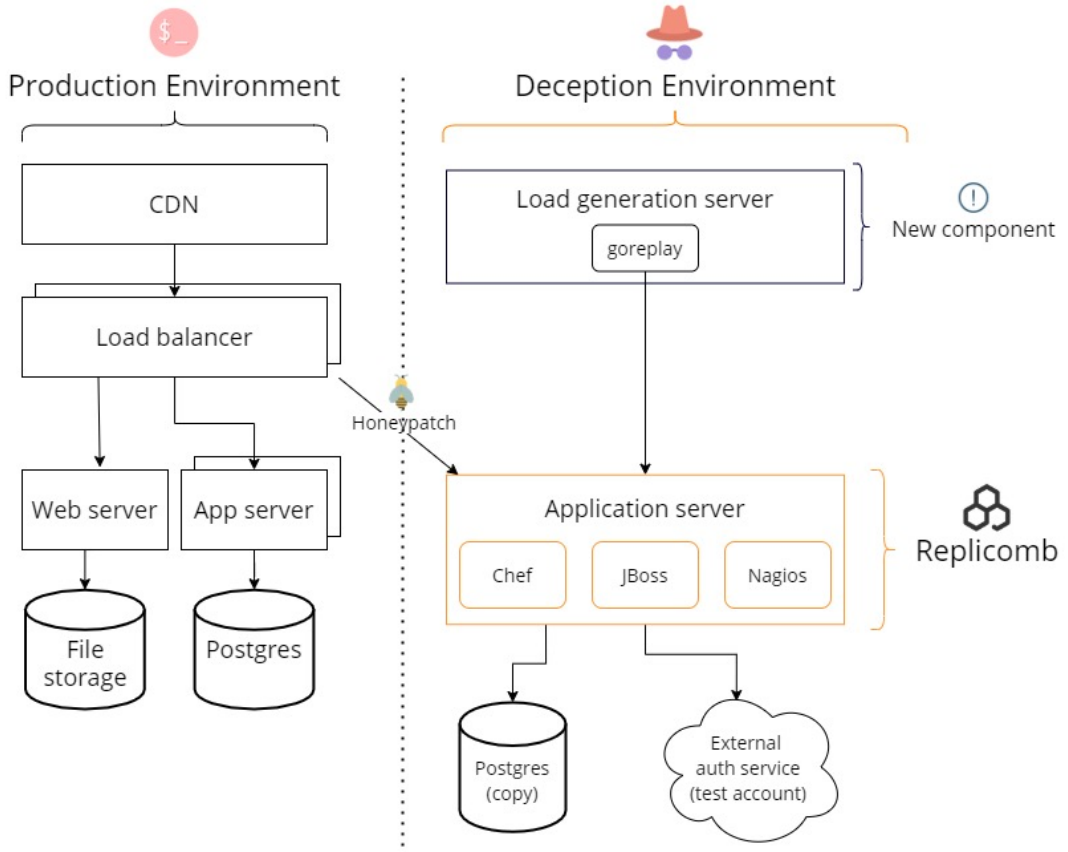
Source: https://swagitda.com/blog/posts/security-decision-trees-with-graphviz/

Building an Attack Tree



Source: https://swagitda.com/blog/posts/security-decision-trees-with-graphviz/

Deception Environments



Source: https://queue.acm.org/LamboozlingAttackers

A Market for Continuous Assurance