NORTH TEXAS
ISSA
#NTXISSA

How Threat Modeling Can Improve Your IAM Solution

John Fehan
Senior Consultant
OpenSky Corporation

October 2nd, 2015

Agenda

- Evolution of Identity and Access Management (IAM) Solutions
  - An sample IAM contextual architecture
  - A functional walkthrough
  - Security of the IAM solution
- Threat Modeling
- Benefits of Threat Modeling
- Summary

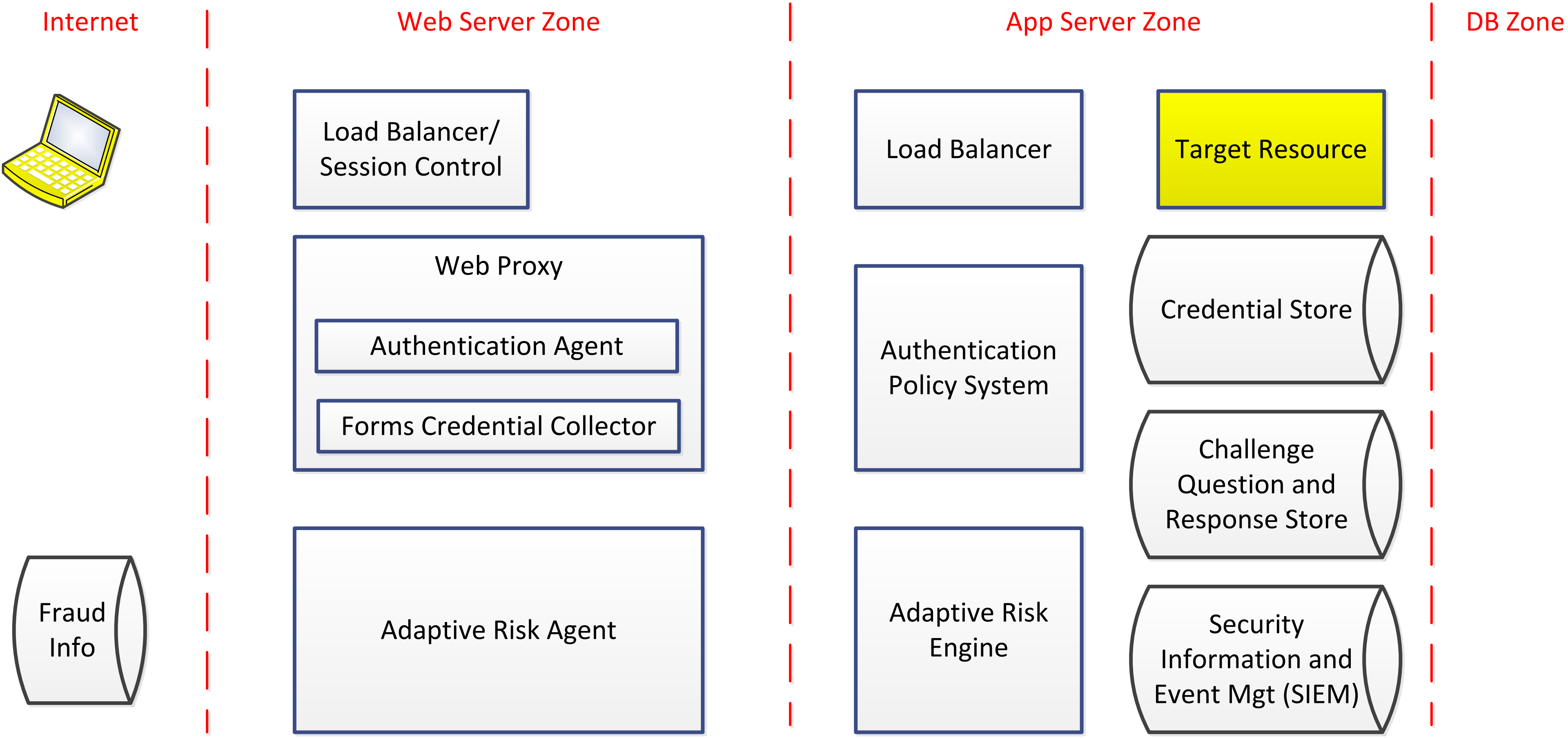
The Evolution of IAM

- Businesses have evolved to have many different, complex relationships…with customers, employees, partners and more
- Businesses must now ask
  - Who do you claim to be?
  - How well can we confirm that?
  - Are you allowed in?
  - Do I know and trust your device?
  - What attributes are associated to your identity?
  - Should you be accessing the system at this time?
  - Are you authorized for that transaction specifically?

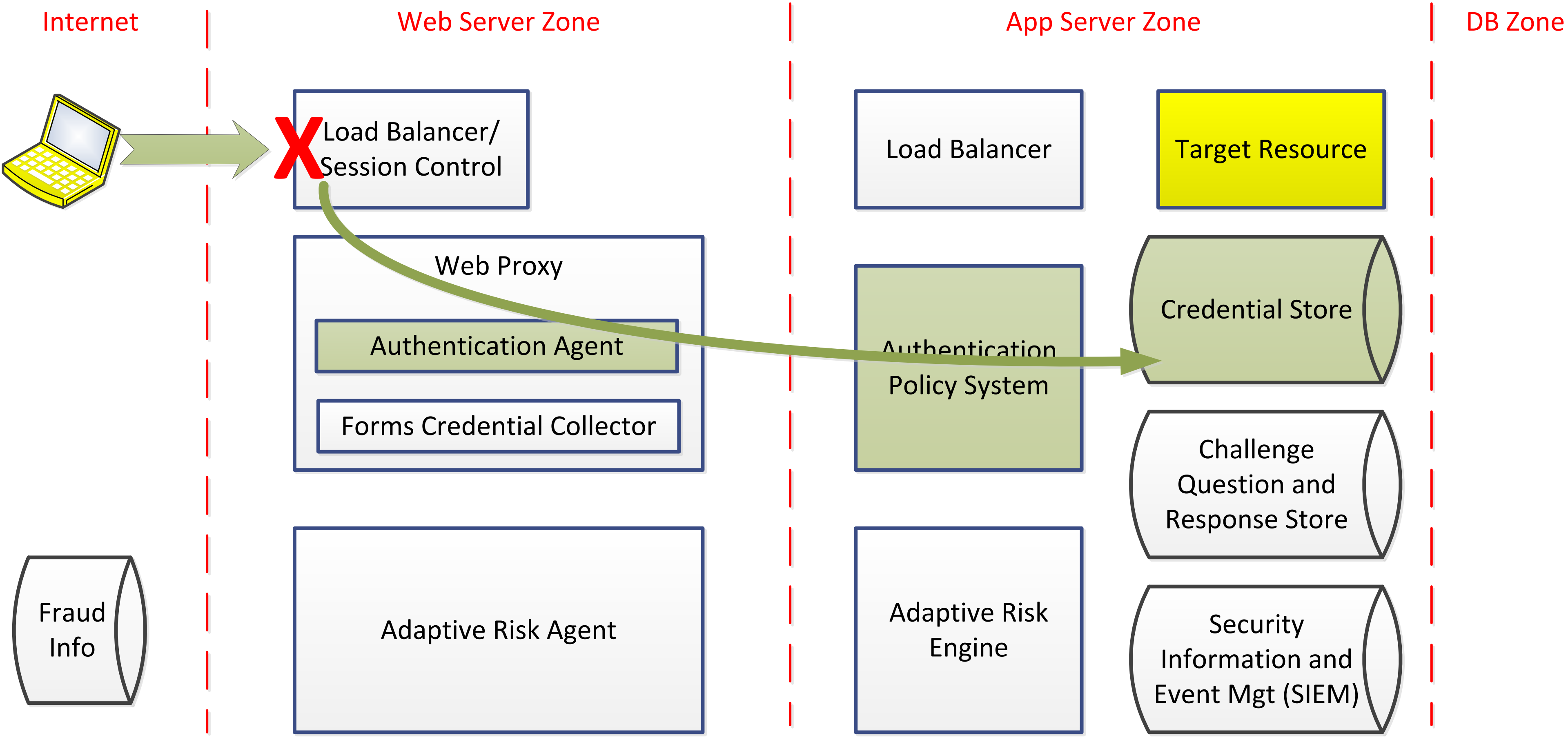
The Evolution of IAM

- Todays Identity and Access Management (IAM) solutions consist of several vendor products, numerous interfaces and identity data elements all with significant impact.
- The fundamental goal is to
  - Provide access per need and policy
  - With security controls that are graduated to match the risk of the moment

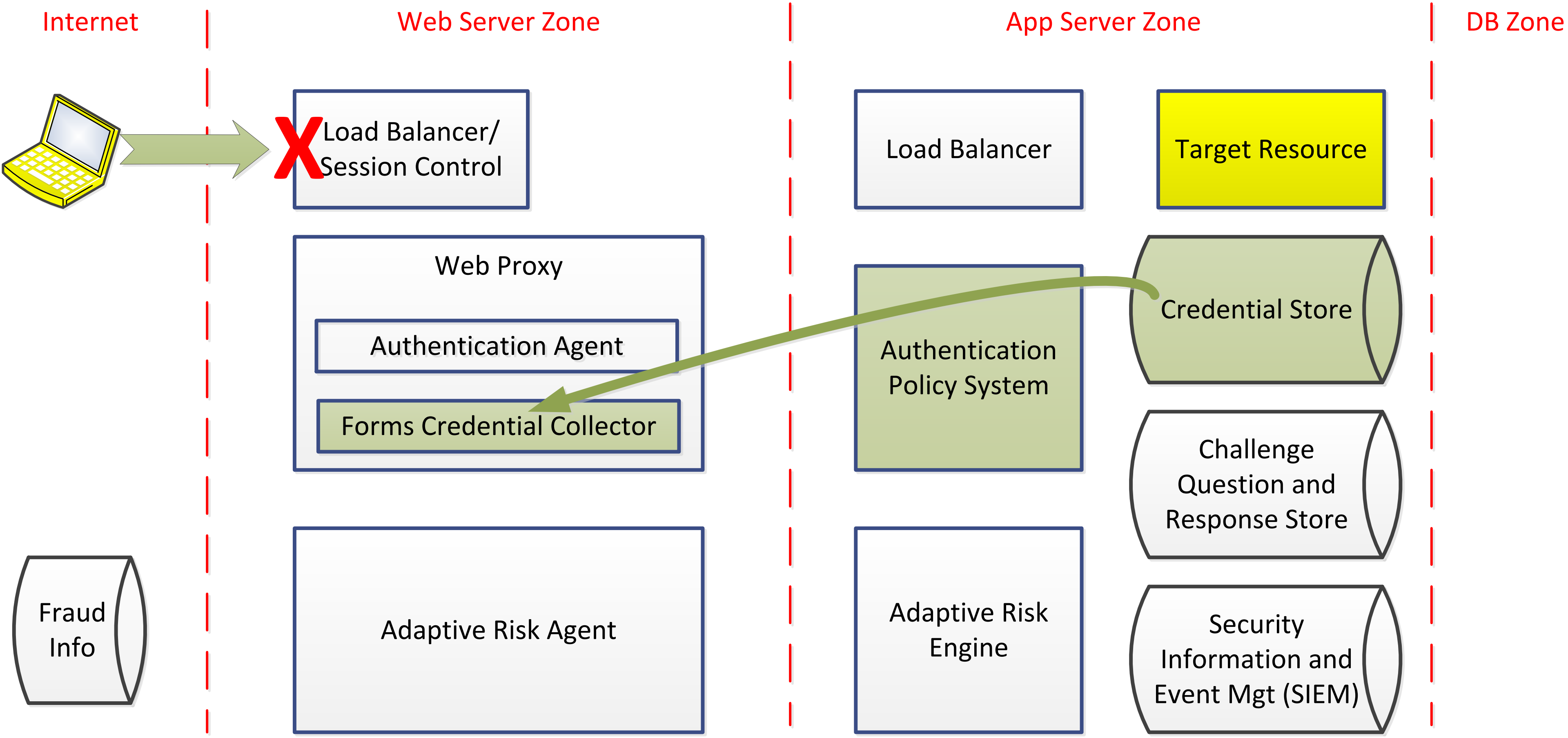
Sample IAM Architecture



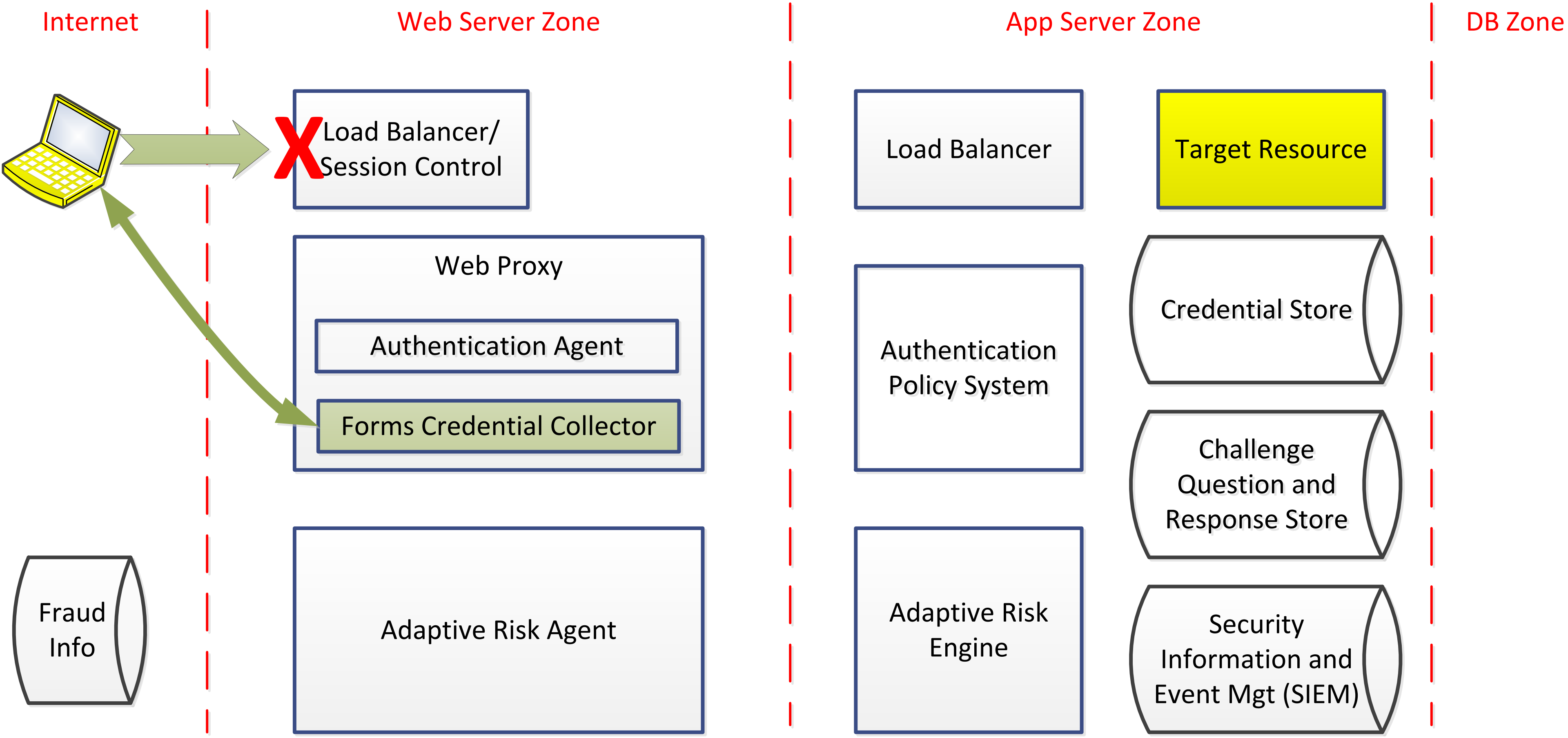
Sample IAM Architecture



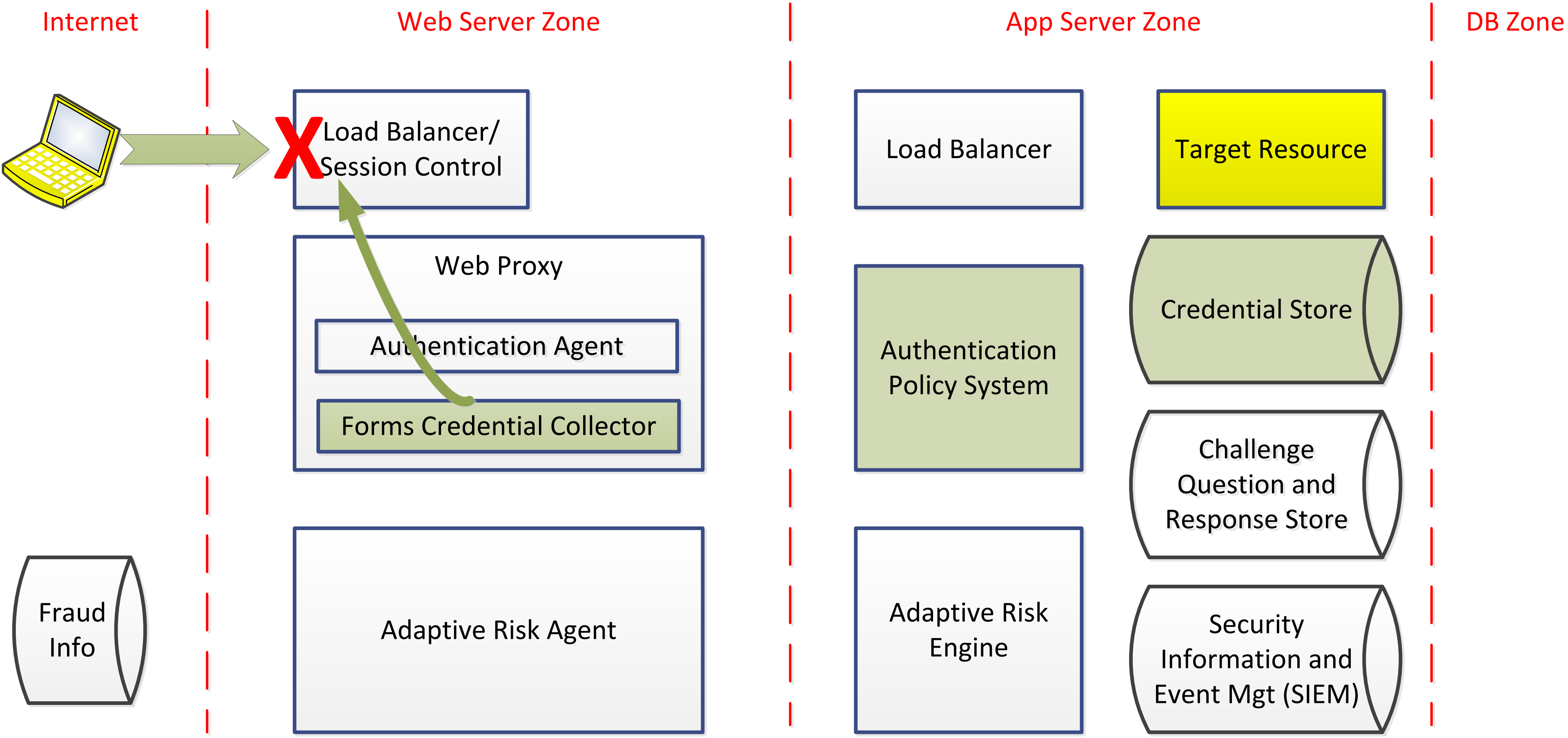
Sample IAM Architecture



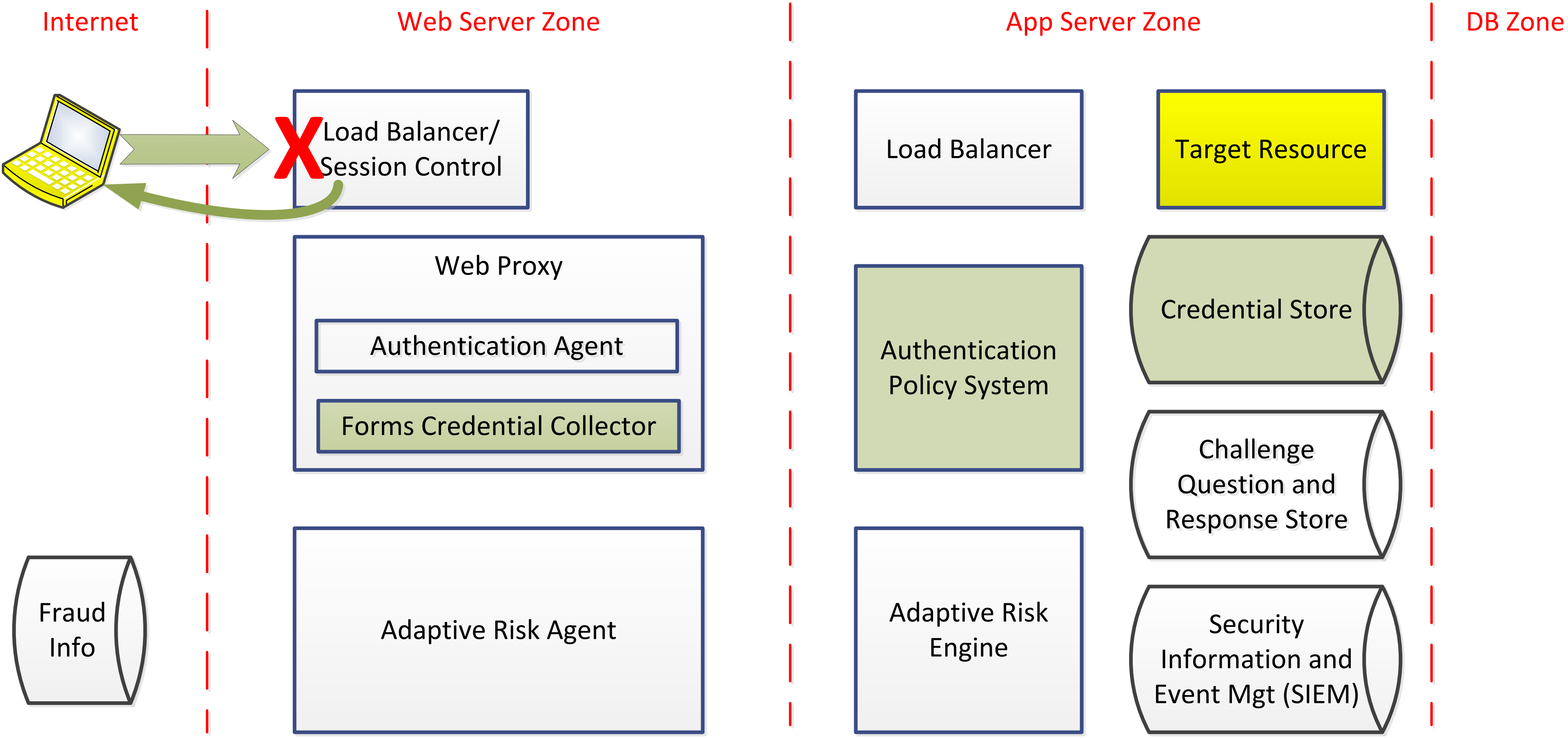
Sample IAM Architecture



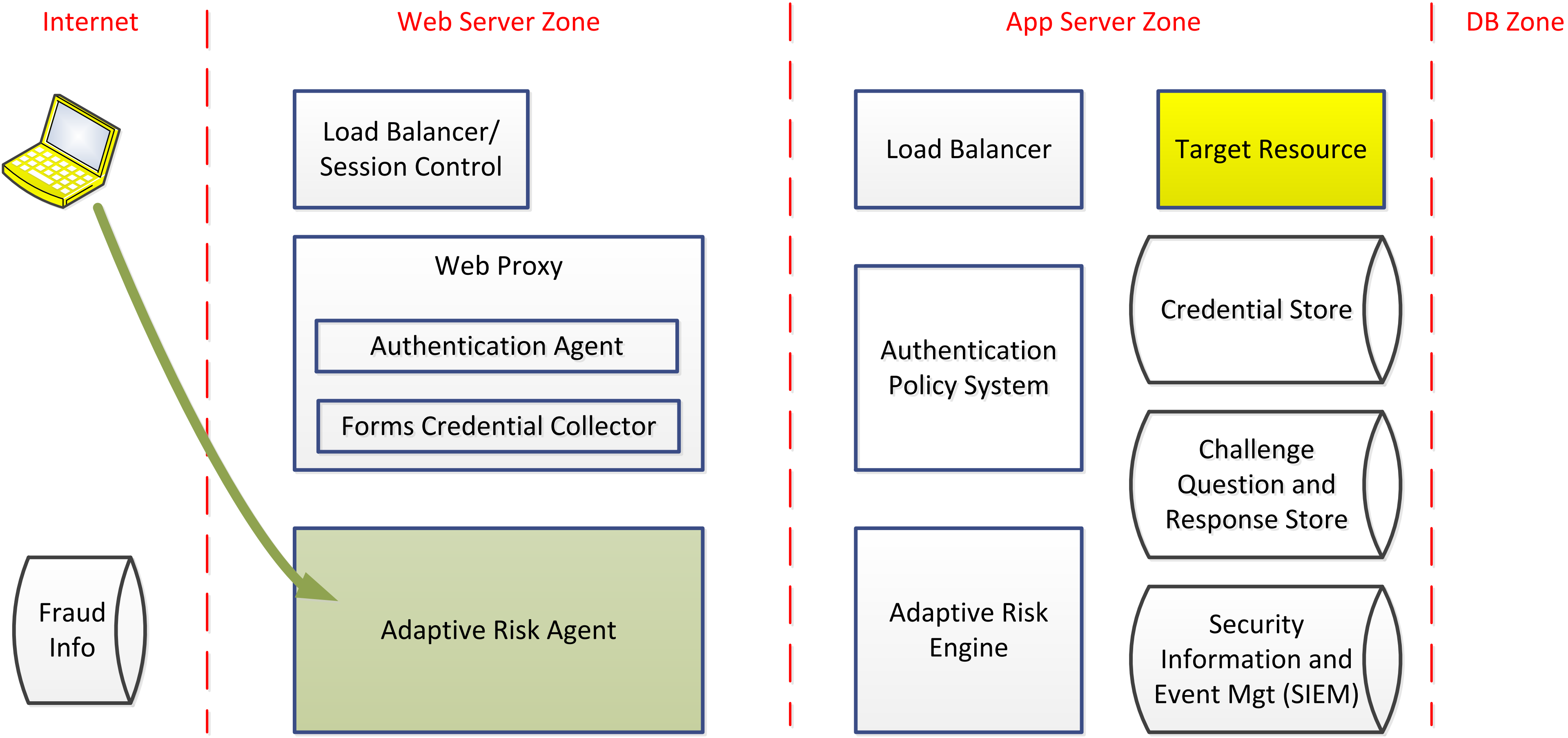
Sample IAM Architecture



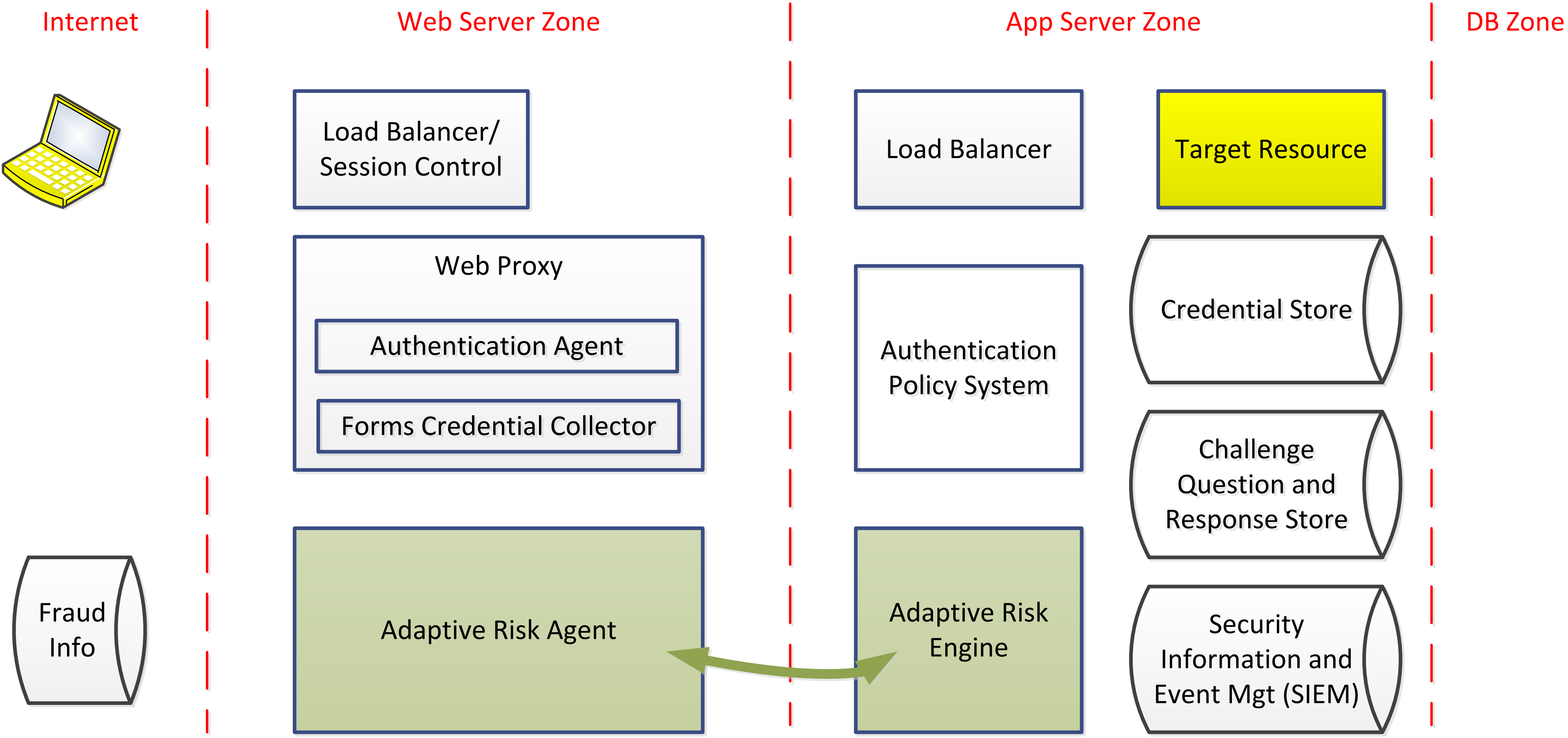
Sample IAM Architecture



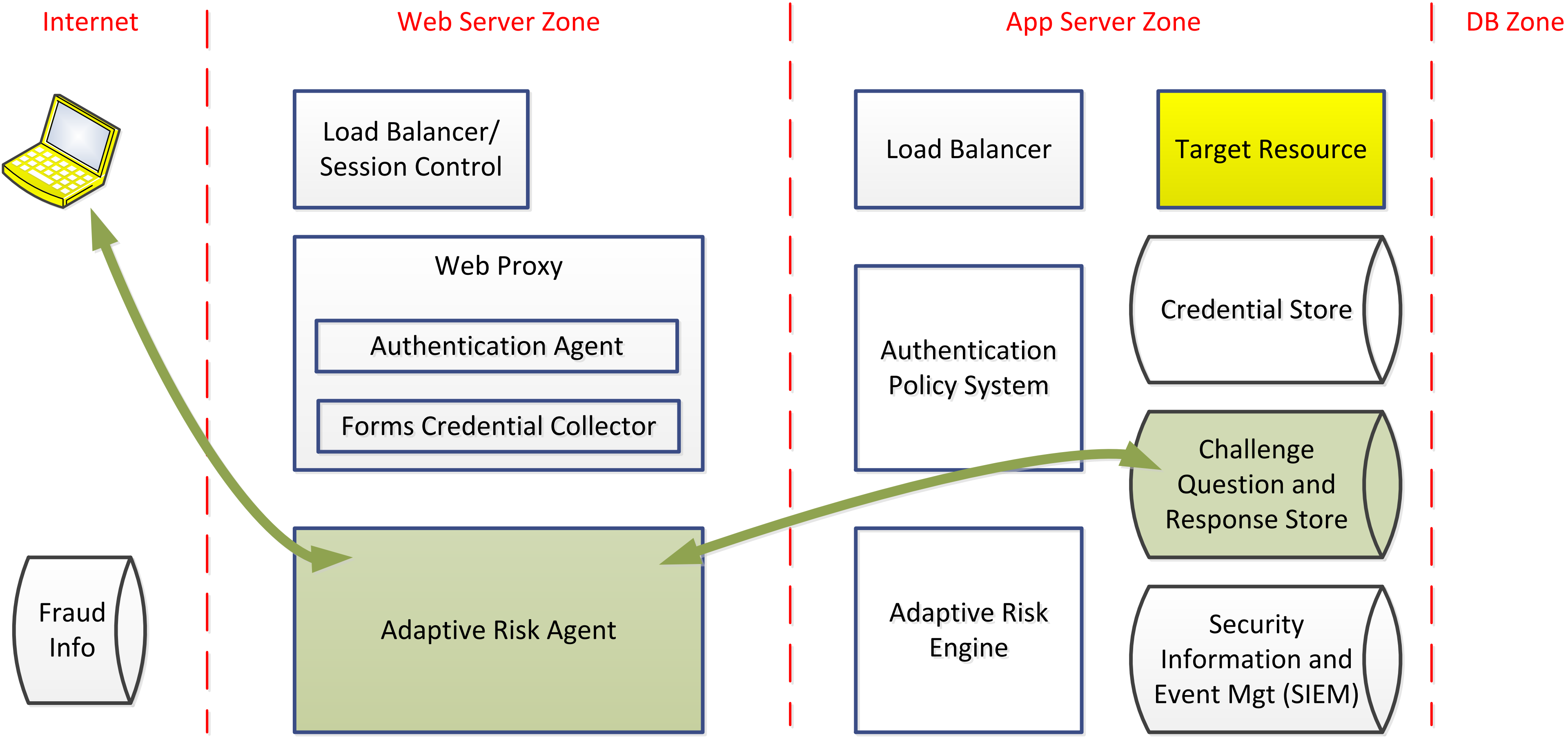
Sample IAM Architecture



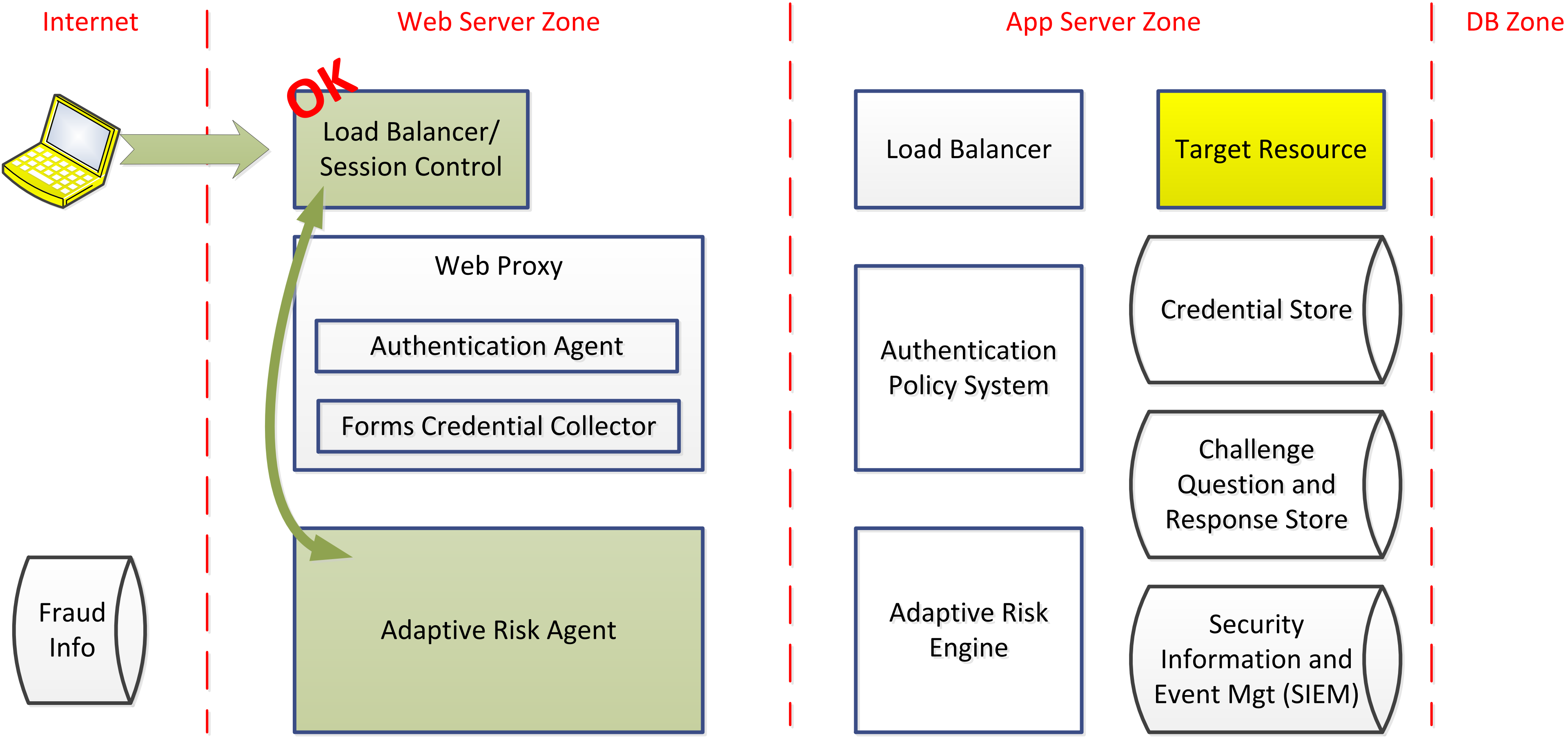
Sample IAM Architecture



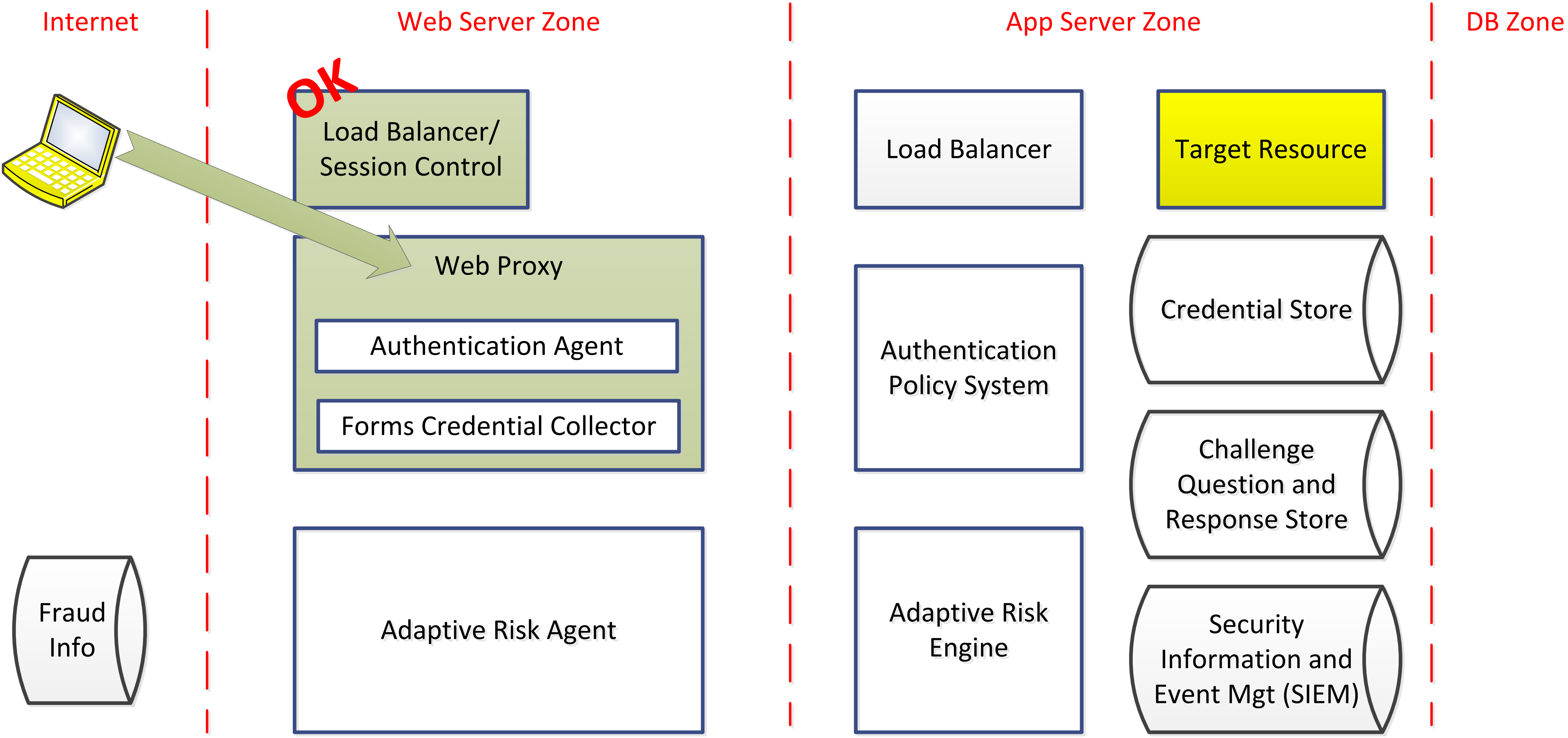
Sample IAM Architecture



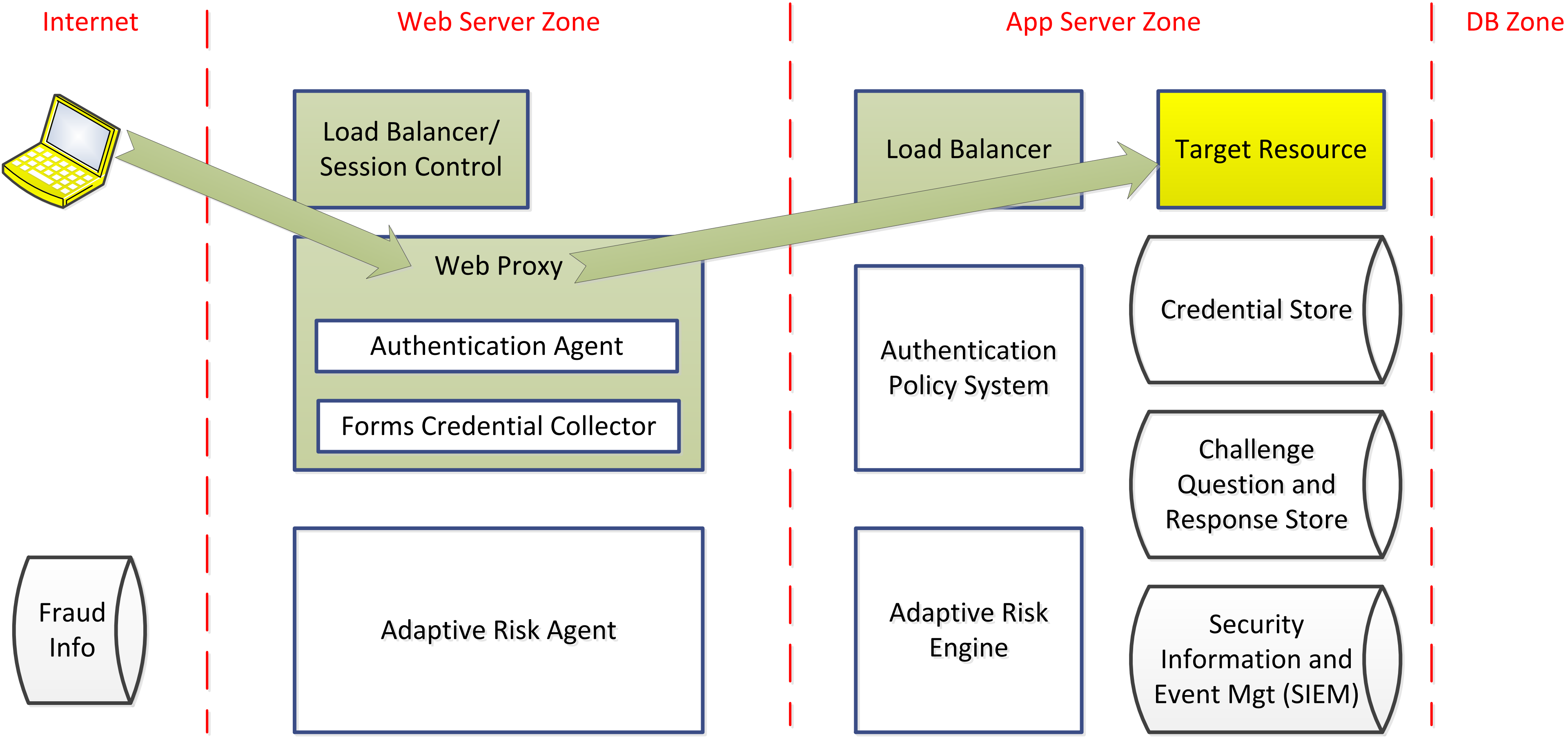
Sample IAM Architecture



Sample IAM Architecture



Sample IAM Architecture



Security of the IAM Solution

- User experience must be appropriate for the particular amount of risk
- Keep this system working and keep it secure
- Common to focus on functionality and go light on the non-functional security review
- A **threat modeling** review for attack vectors and vulnerabilities inherent to the design is required. It must be:
  - objective
  - focused on the threat.

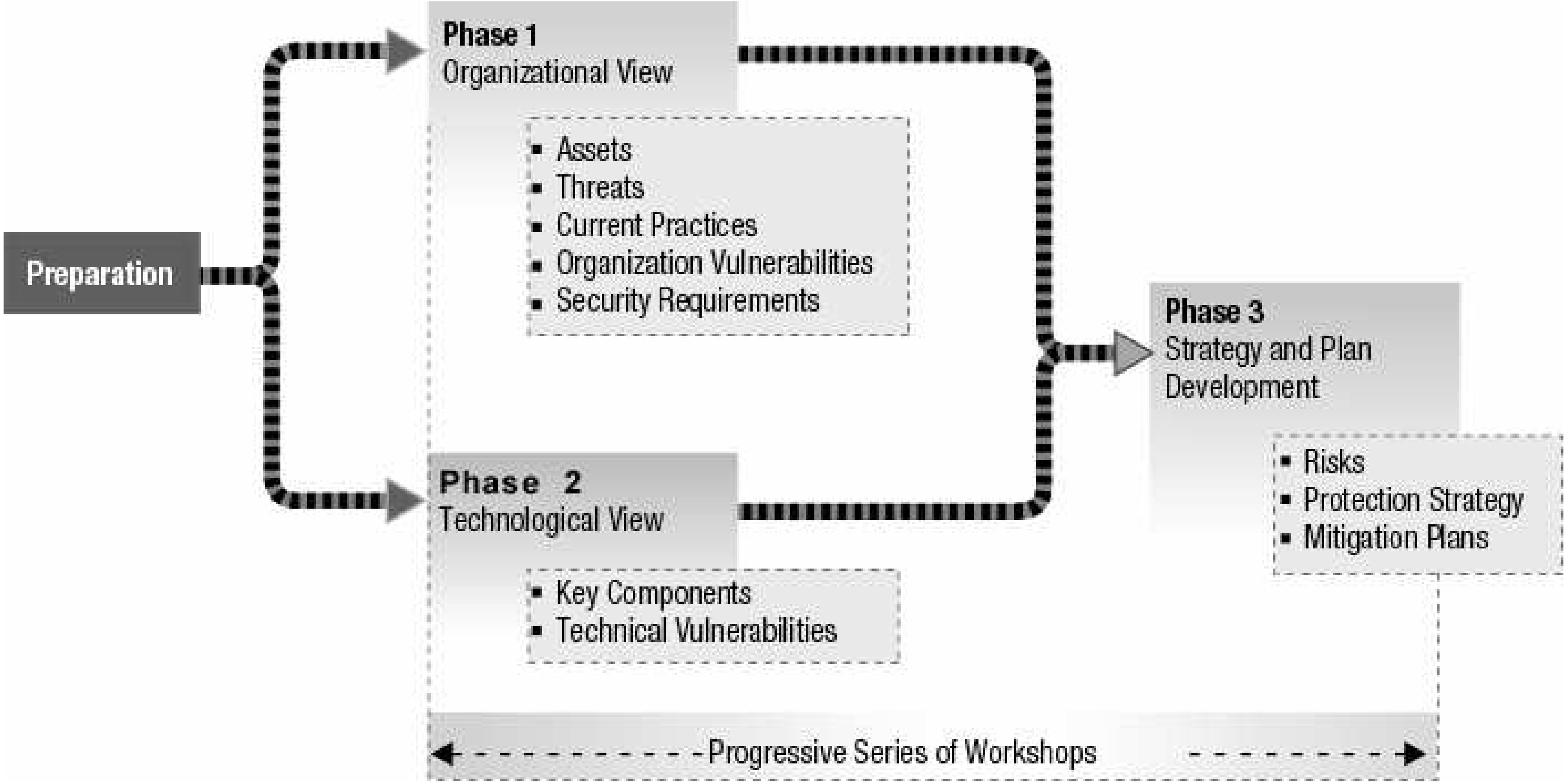
Threat Modeling

- Threat modeling is the exploration of the threats to which your environment is vulnerable—in this case, the company's IAM system
- OCTAVE® method—Operationally Critical Threat, Asset, and Vulnerability Evaluation is the standard methodology.

Reference: " Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process."
Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson.
Canegie Mellon Software Engineering Institute. May 2007.

Threat Modeling

- OCTAVE Allegro methodology (image copyright SEI Canegie-Mellon University)



Threat Modeling

- The Threat Modeling approach
  - Capture of the IAM contextual architecture; contextual level of detail is vendor agnostic
  - Define certain environmentals and security controls
  - Identify and resolve differences b/w design and as built
- Connects the conceptual vision approved by stakeholders to the technical detail typically documented and used by engineers

Threat Modeling

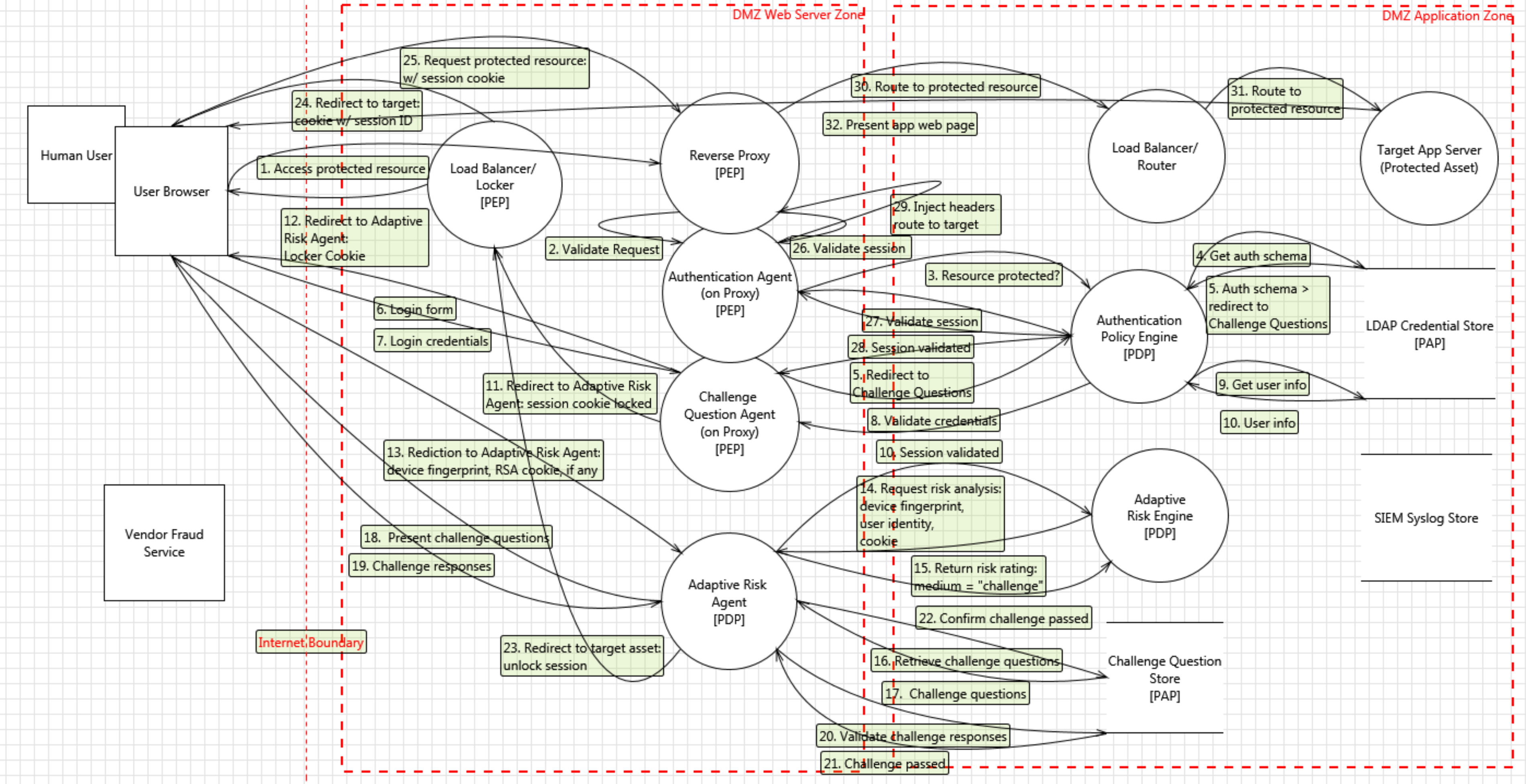
- The Threat Modeling approach
  - Analyze threats
  - Plan mitigations
- Contextual detail aligns everyone involved in delivery and allows threat modelers and threat modeling tools to assess natural attack vectors
- Track the status of each threat - not started, needs investigation, not applicable and mitigated - and adjust the priority
- A traceability matrix of controls to threats is maintained

Threat Modeling

- Threats are organized by Microsoft's Security Development Lifecycle (SDL) **STRIDE** categories:
  - **S**poofing
  - **T**ampering
  - **R**epudiation
  - **I**nformation Compromise
  - **D**enial of Service
  - **E**scalation of Privilege
- OpenSky recommends and leverages STRIDE in combination with OCTAVE Allegro in our general approach for threat modeling.
- These methodologies are described on the OWASP site: https://www.owasp.org/index.php/Threat_Risk_Modeling

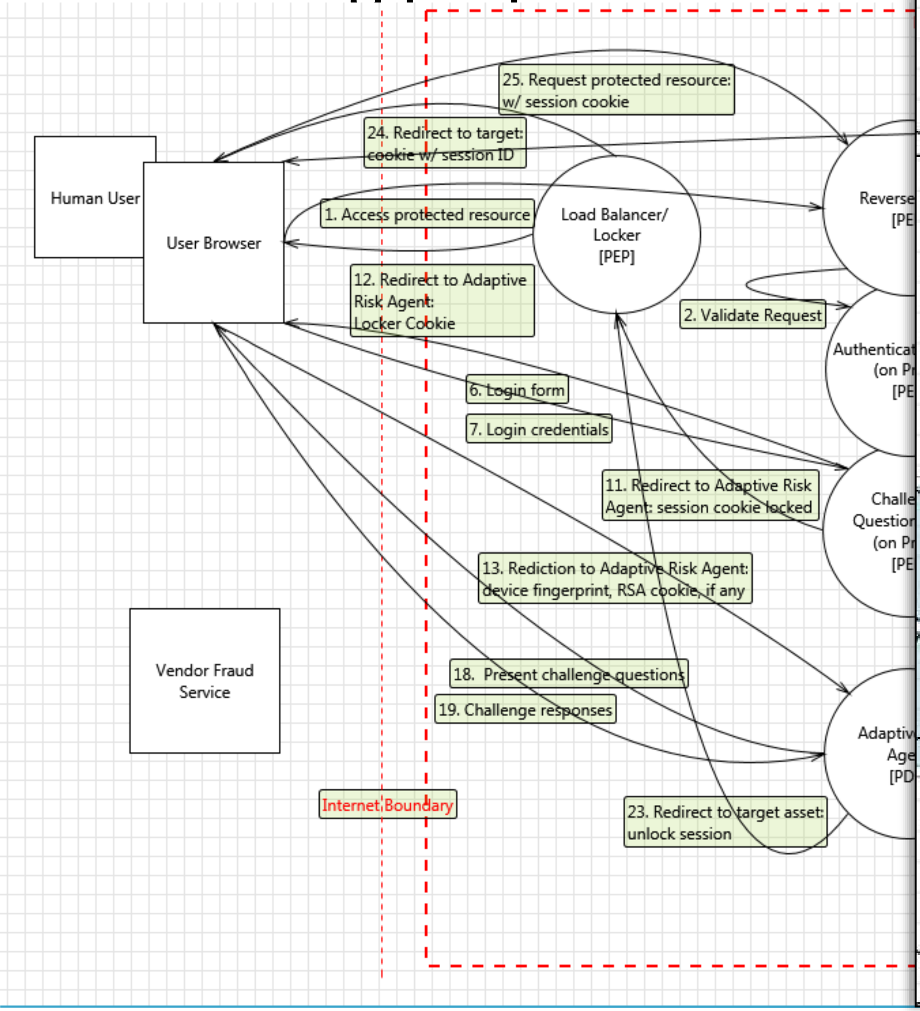
The Evolution of IAM

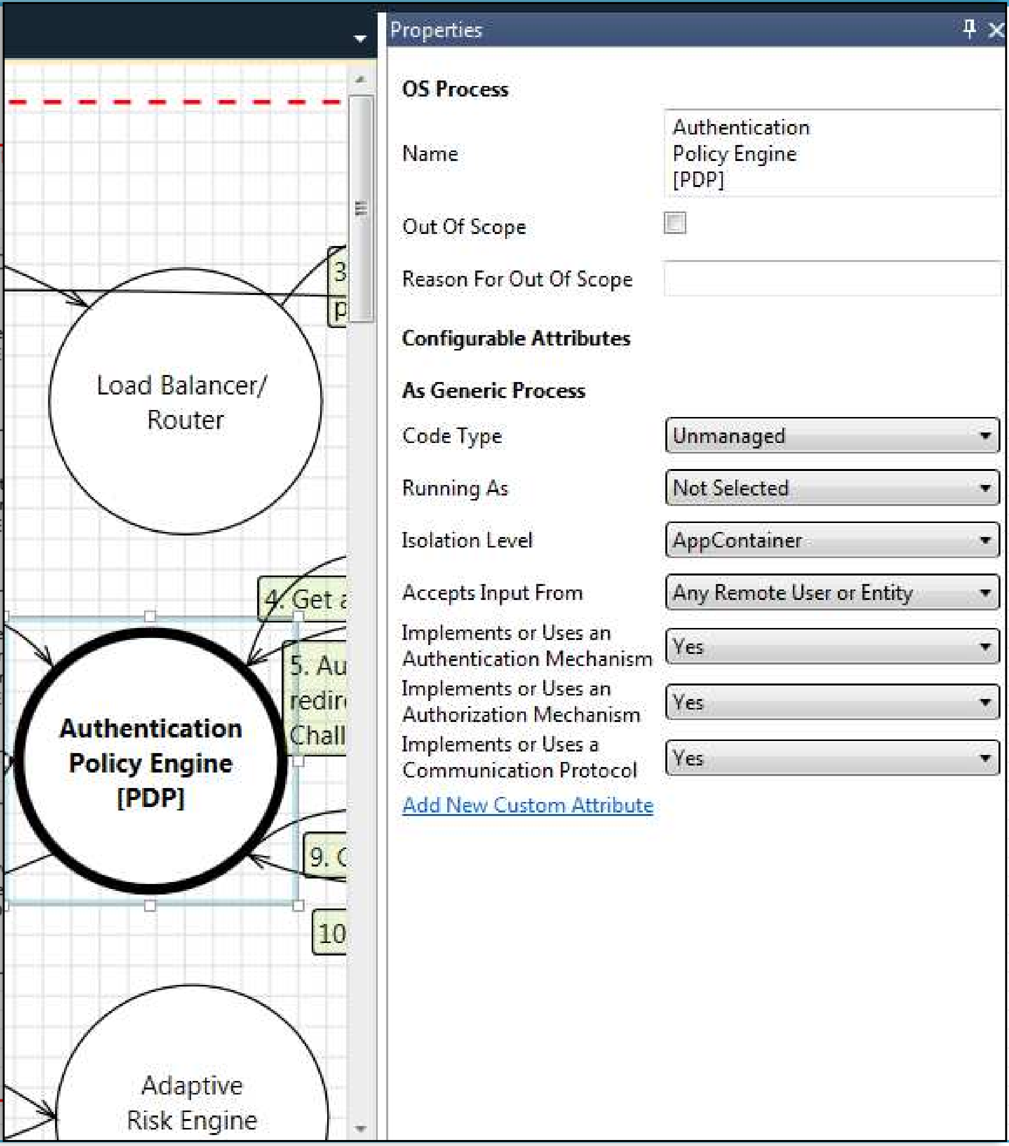
- Contextual architecture within the MS Threat Modeling


DMZ Web Server Zone
DMZ Application Zone
Human User
User Browser
Vendor Fraud Service
Internet Boundary
Load Balancer/ Locker [PEP]
Reverse Proxy [PEP]
Authentication Agent (on Proxy) [PEP]
Challenge Question Agent (on Proxy) [PEP]
Adaptive Risk Agent [PDP]
Load Balancer/ Router
Target App Server (Protected Asset)
Authentication Policy Engine [PDP]
LDAP Credential Store [PAP]
Adaptive Risk Engine [PDP]
SIEM Syslog Store
Challenge Question Store [PAP]
1. Access protected resource
2. Validate Request
3. Resource protected?
4. Get auth schema
5. Auth schema > redirect to Challenge Questions
5. Redirect to Challenge Questions
6. Login form
7. Login credentials
8. Validate credentials
9. Get user info
10. User info
10. Session validated
11. Redirect to Adaptive Risk Agent: session cookie locked
12. Redirect to Adaptive Risk Agent: Locker Cookie
13. Rediction to Adaptive Risk Agent: device fingerprint, RSA cookie, if any
14. Request risk analysis: device fingerprint, user identity, cookie
15. Return risk rating: medium = "challenge"
16. Retrieve challenge questions
17. Challenge questions
18. Present challenge questions
19. Challenge responses
20. Validate challenge responses
21. Challenge passed
22. Confirm challenge passed
23. Redirect to target asset: unlock session
24. Redirect to target: cookie w/ session ID
25. Request protected resource: w/ session cookie
26. Validate session
27. Validate session
28. Session validated
29. Inject headers route to target
30. Route to protected resource
31. Route to protected resource
32. Present app web page

Threat Modeling

- Setting properties


25. Request protected resource: w/ session cookie
24. Redirect to target: cookie w/ session ID
Human User
User Browser
1. Access protected resource
Load Balancer/ Locker [PEP]
Reverse [PE
12. Redirect to Adaptive Risk Agent: Locker Cookie
2. Validate Request
Authenticat (on Pr [PE
6. Login form
7. Login credentials
11. Redirect to Adaptive Risk Agent: session cookie locked
Challe Question (on Pr [PE
13. Rediction to Adaptive Risk Agent: device fingerprint, RSA cookie, if any
Vendor Fraud Service
18. Present challenge questions
19. Challenge responses
Adaptiv Age [PD
Internet Boundary
23. Redirect to target asset: unlock session



Properties

OS Process

Name	Authentication Policy Engine [PDP]
Out Of Scope	□
Reason For Out Of Scope	

Configurable Attributes

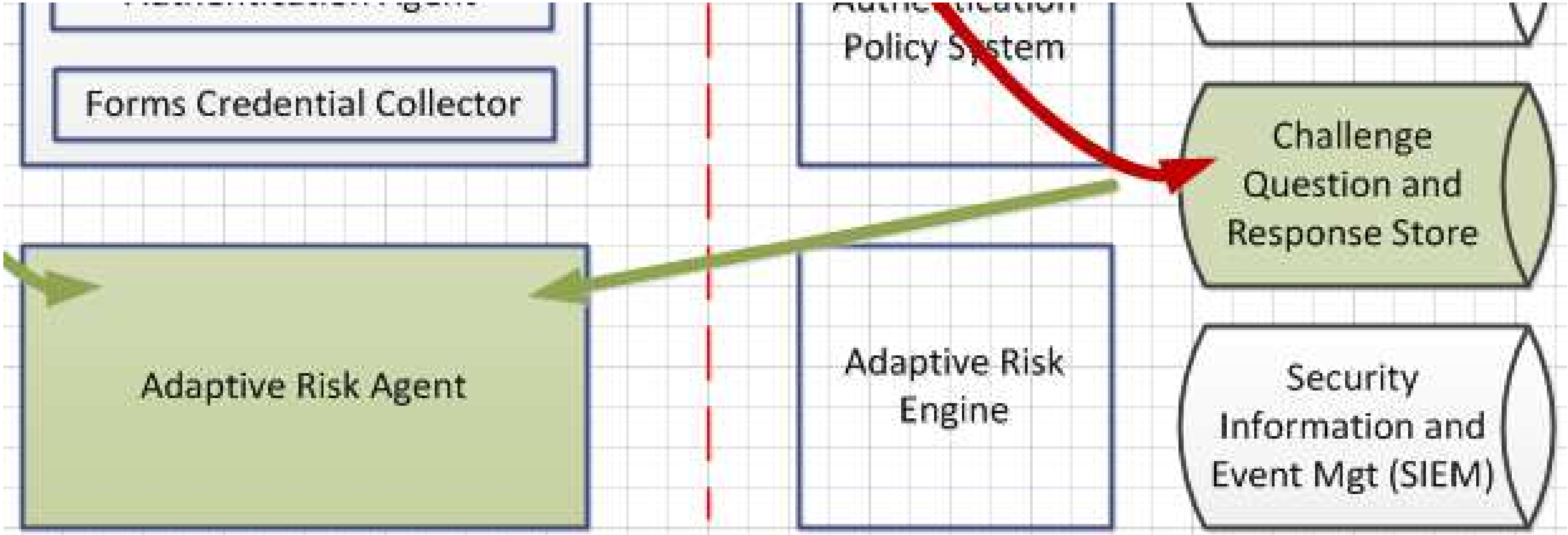
As Generic Process

Code Type	Unmanaged
Running As	Not Selected
Isolation Level	AppContainer
Accepts Input From	Any Remote User or Entity
Implements or Uses an Authentication Mechanism	Yes
Implements or Uses an Authorization Mechanism	Yes
Implements or Uses a Communication Protocol	Yes

Add New Custom Attribute

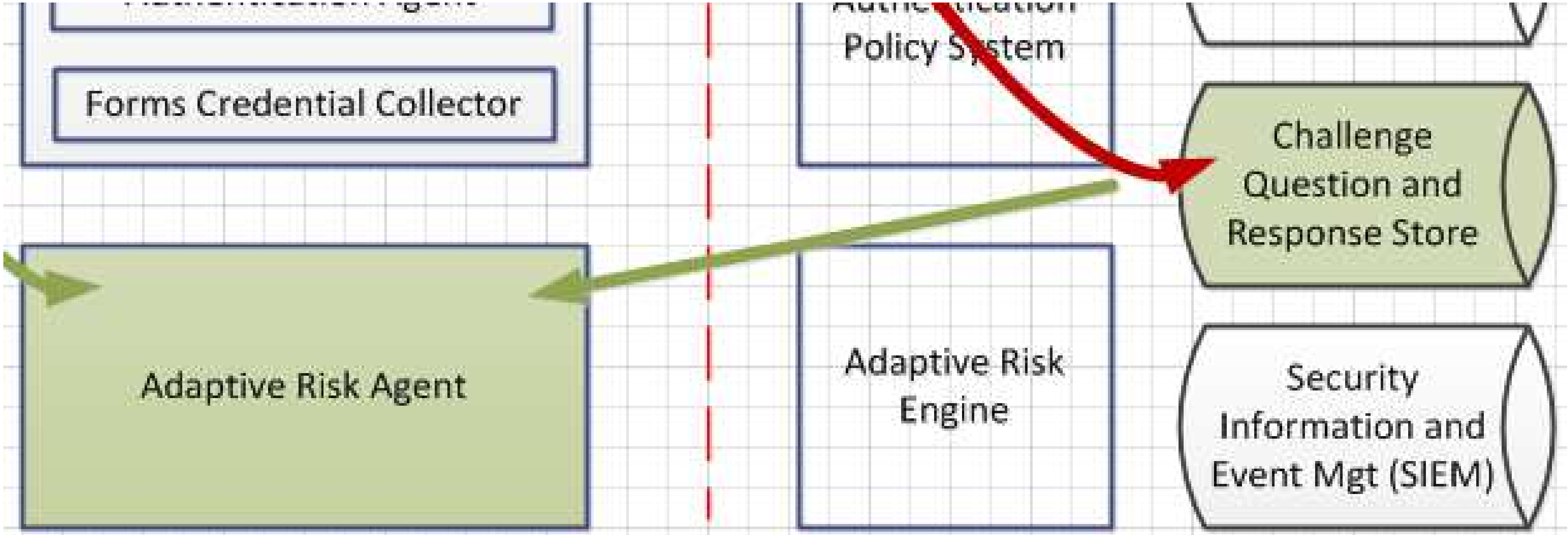
Threat Modeling

- Each threat can be evaluated and mitigation strategies developed.
- For example, the Adaptive Risk Agent may be spoofed by an attacker which could lead to information disclosure by the Challenge Question Store.


Forms Credential Collector
Policy System
Challenge Question and Response Store
Adaptive Risk Agent
Adaptive Risk Engine
Security Information and Event Mgt (SIEM)

Threat Modeling

- The mitigation strategy could include the use of authentication between the Adaptive Risk Agent and the data store.



Authentication Agent
Forms Credential Collector
Authentication Policy System
Challenge Question and Response Store
Adaptive Risk Agent
Adaptive Risk Engine
Security Information and Event Mgt (SIEM)

Benefits of Threat Modeling

- Organizations will be shifting from compliance to threat-oriented security programs
- Demonstrating the priority and value of control investments and maintenance is crucial

Benefits of Threat Modeling

- An independent list of threats that lead to a set of beneficial questions about the security of the IAM solution
- A mature and reasonable process for analyzing and maintaining the security posture of the IAM solution and controls
- A process for sound, joint prioritization and decision making related to the most important improvements to make to the security controls
- An improved understanding of the true as-built state of the IAM solution

Summary

- Threat modeling has emerged as an important tool for security architects
- Threat modeling provides valuable information to design the critical IAM systems for cyber resilience
- Straight-forward way to validate the security of your IAM architecture
- Provides a process for prioritization and sound decision making to enhance the security controls

The Collin College Engineering Department

Collin College Student Chapter of the North Texas ISSA

North Texas ISSA (Information Systems Security Association)

Thank you