



Secure Cloud

Zero-trust Cloud Computing
and
Threat Intelligence System

MARIST

*Public
Internet*

*Private
Intranet*

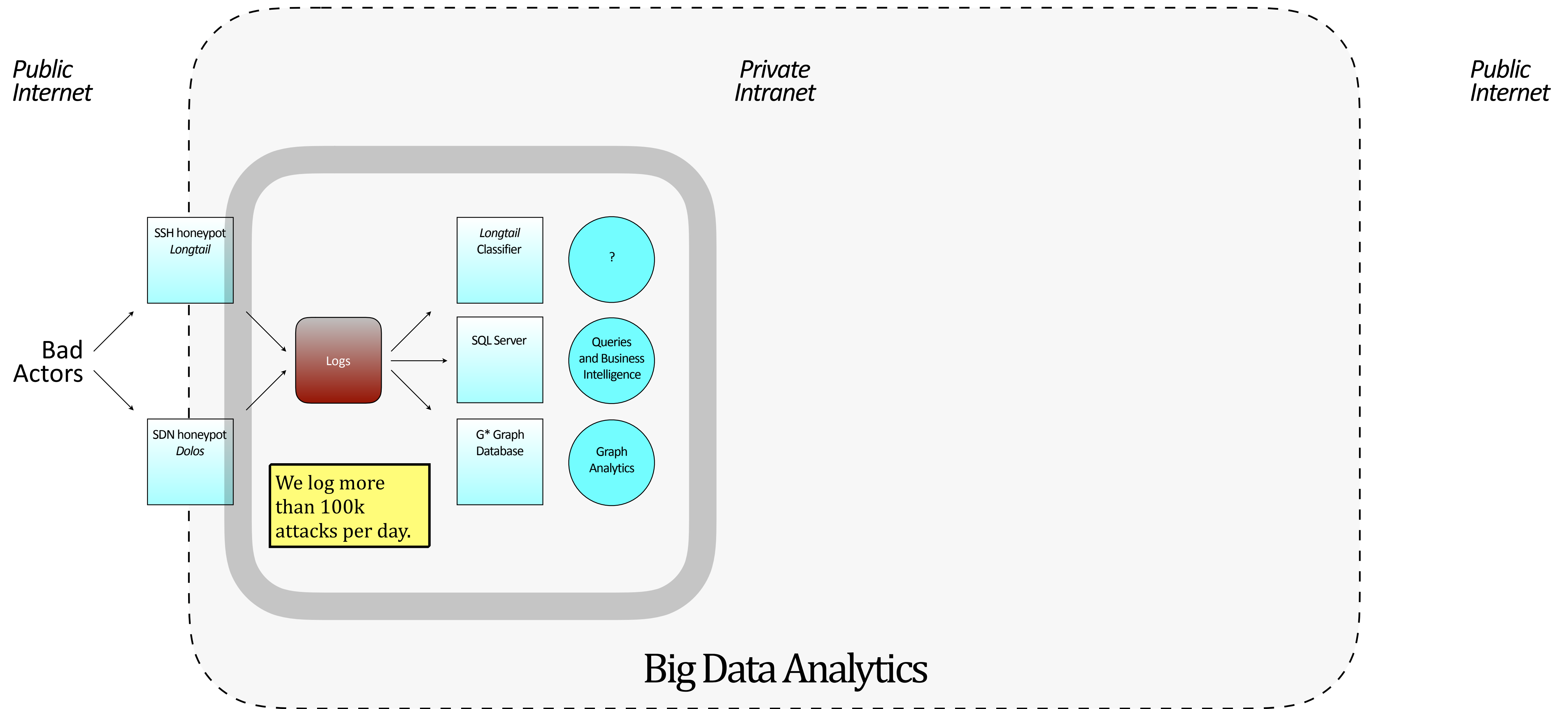
*Public
Internet*

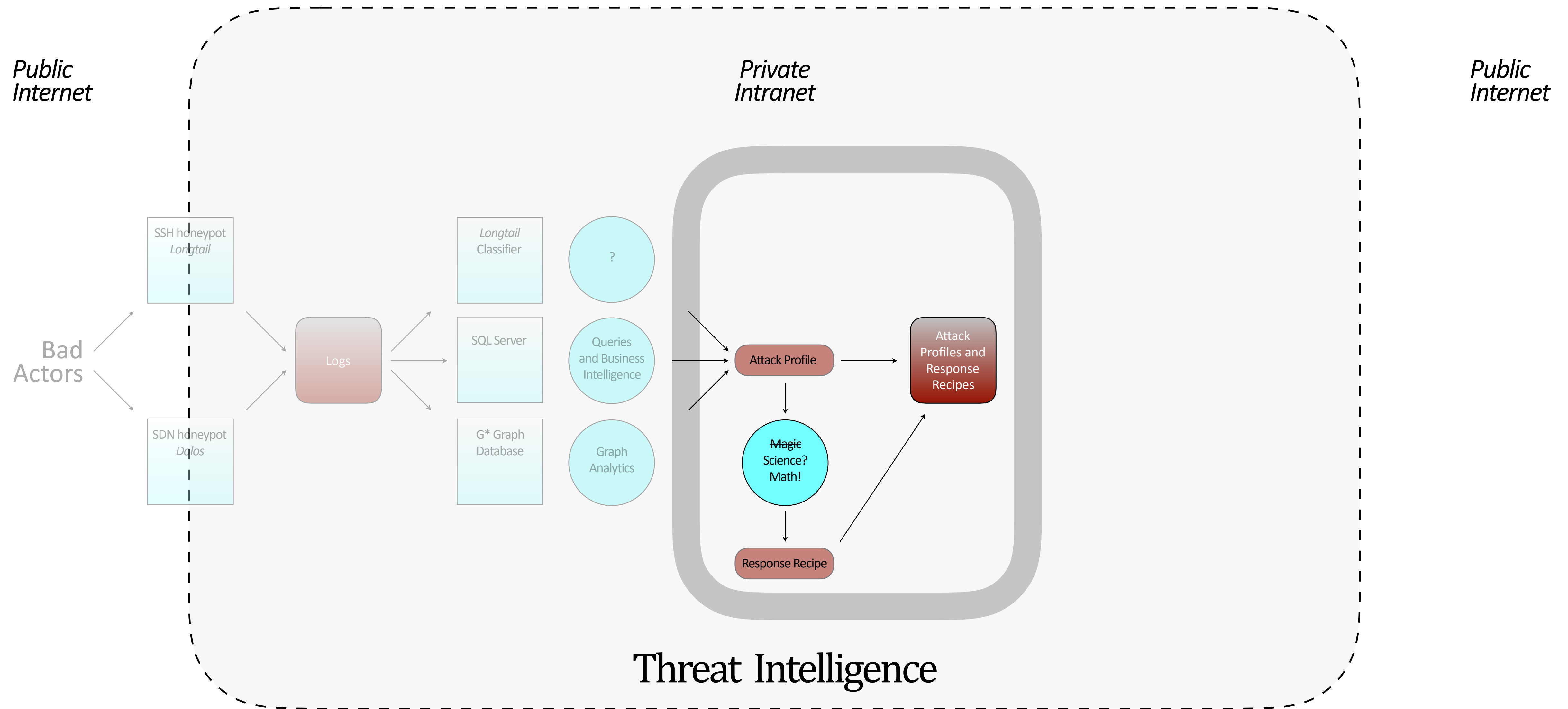
Big Data Analytics

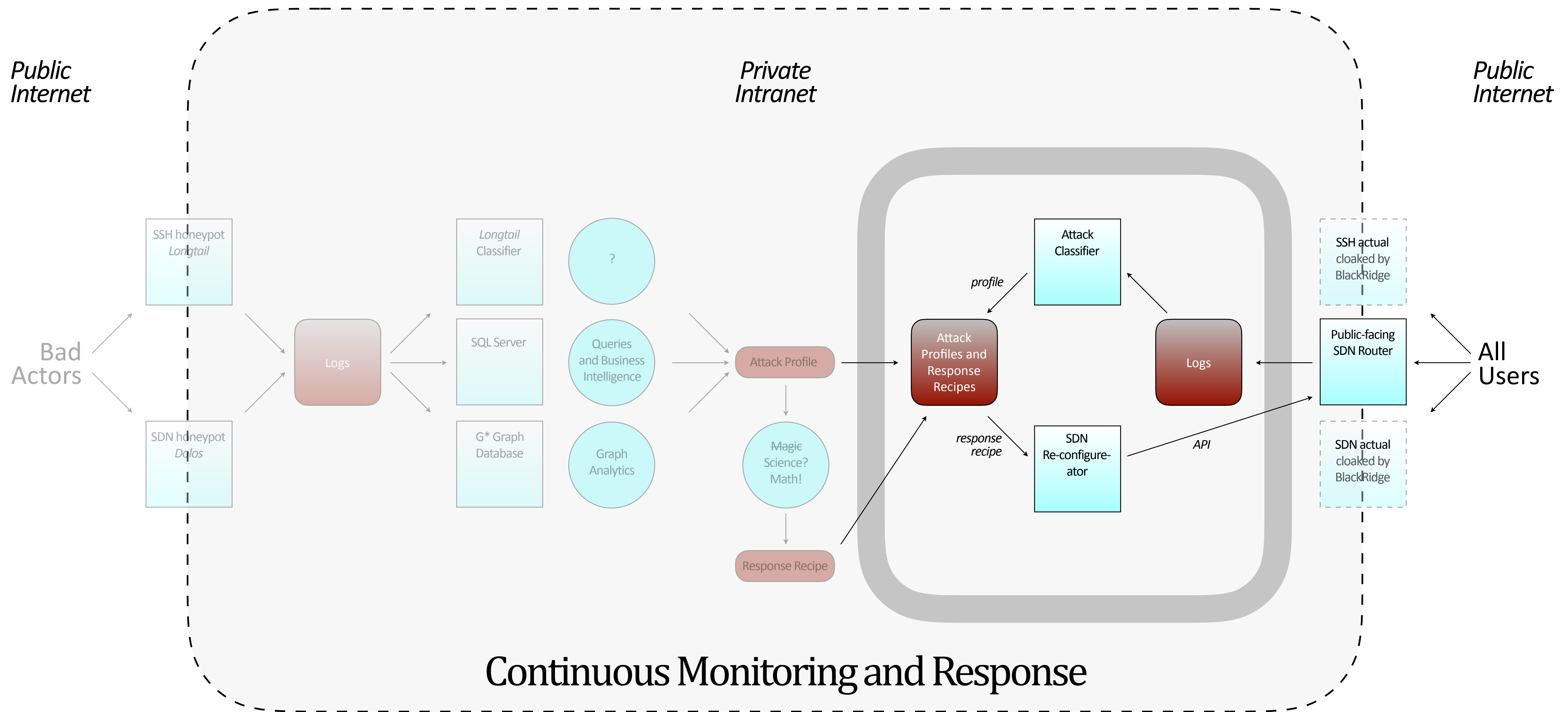
Threat
Intelligence

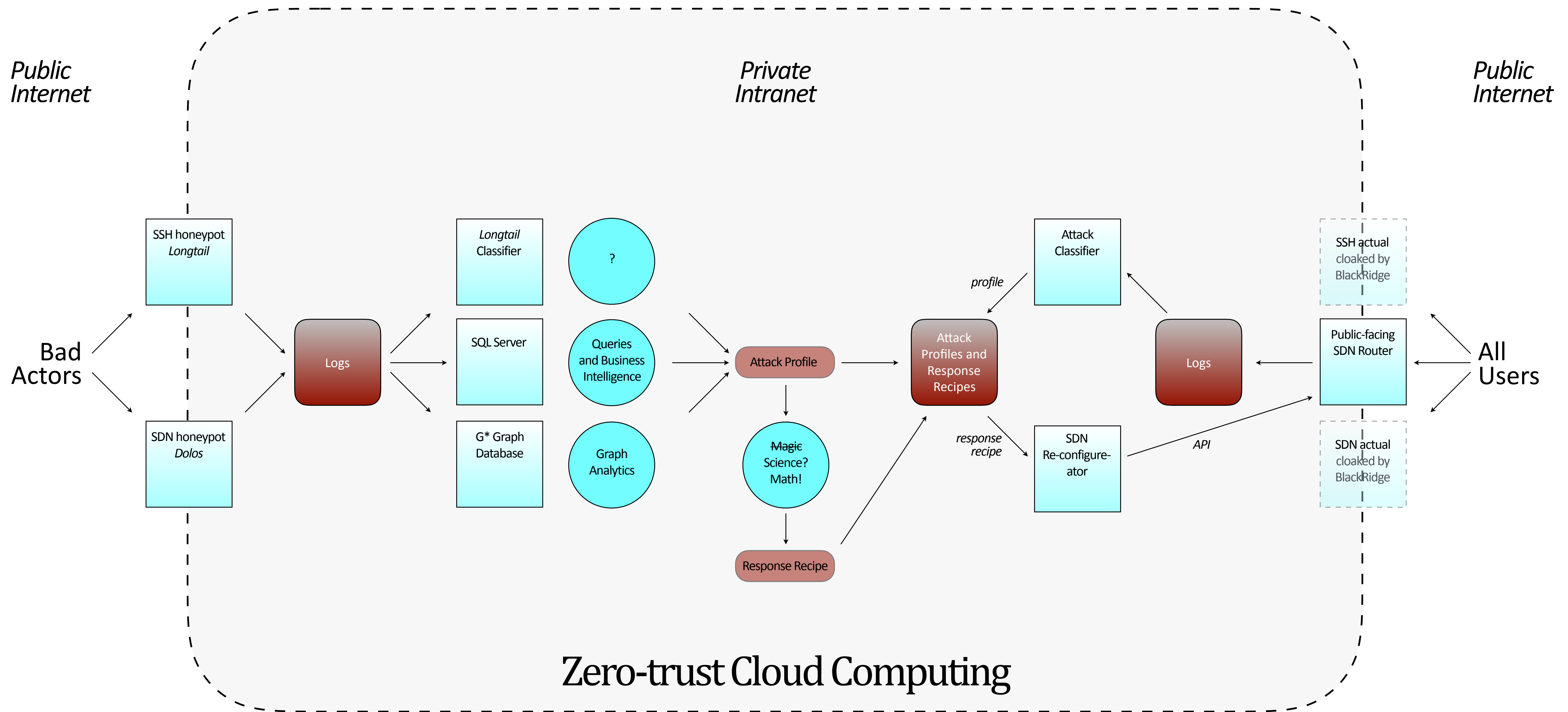
Continuous
Monitoring and
Response

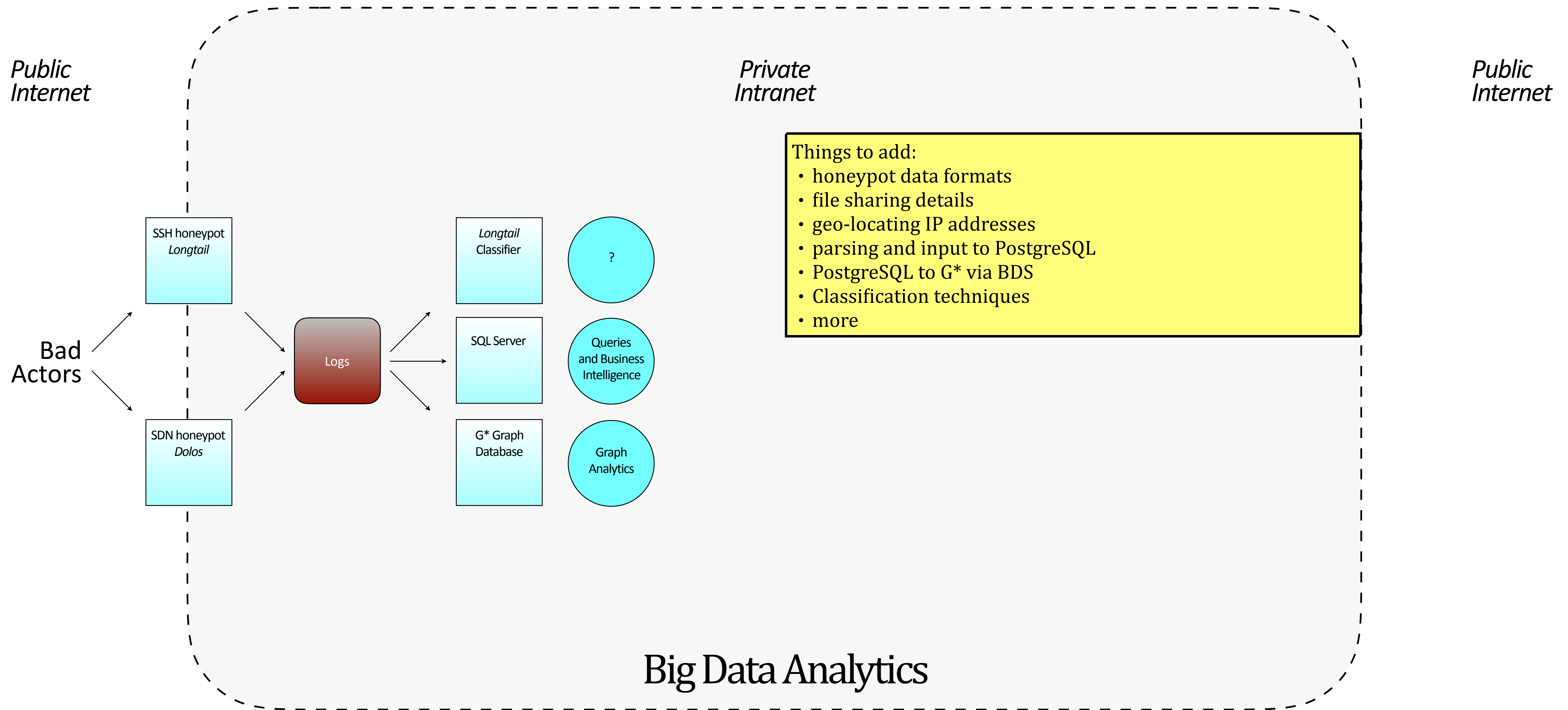
Components







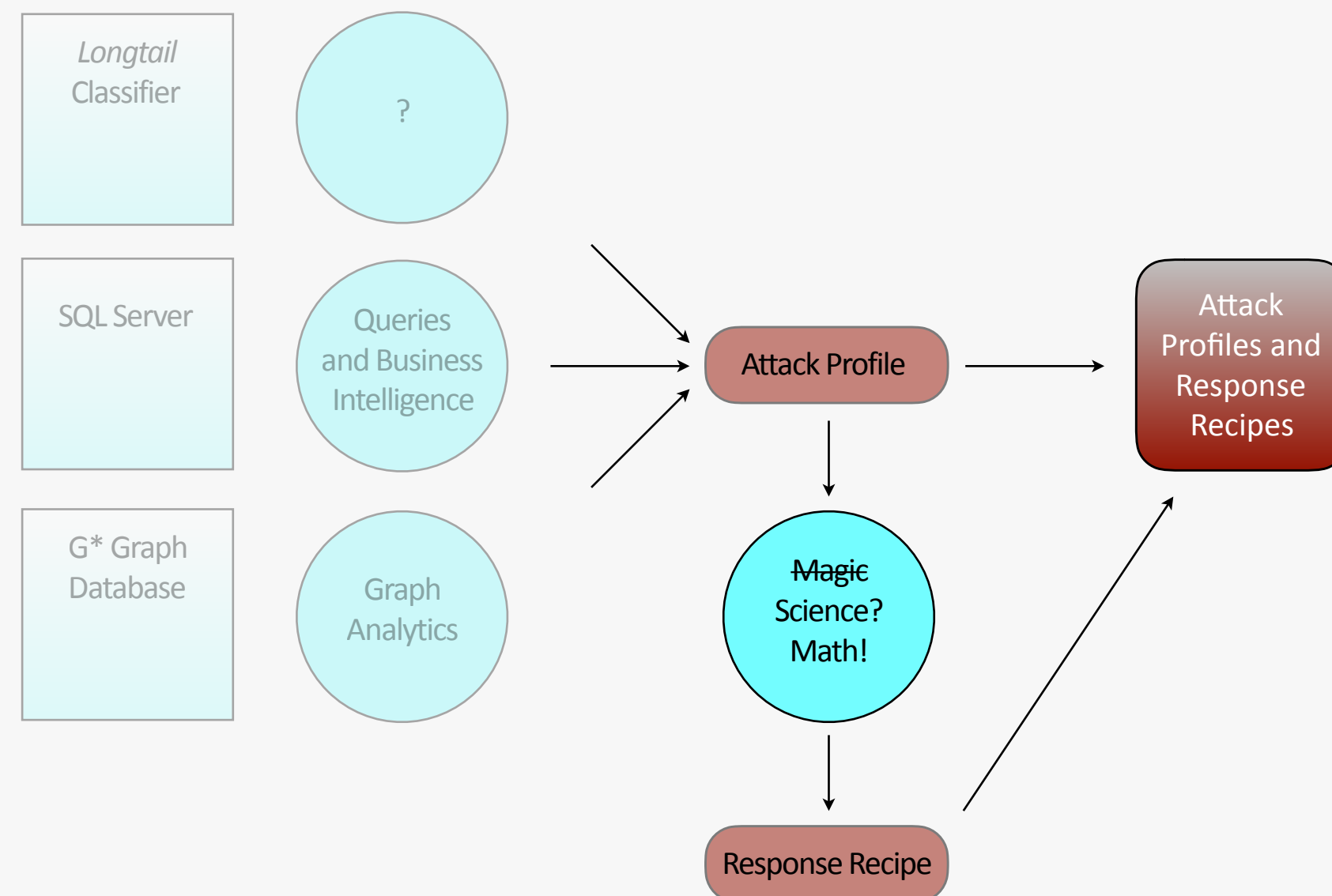




Public
Internet

Private
Intranet

Public
Internet



Things to add:

- Math!
- APIs for Attack Profiles and Response Recipes CRUD
- lots more

Threat Intelligence

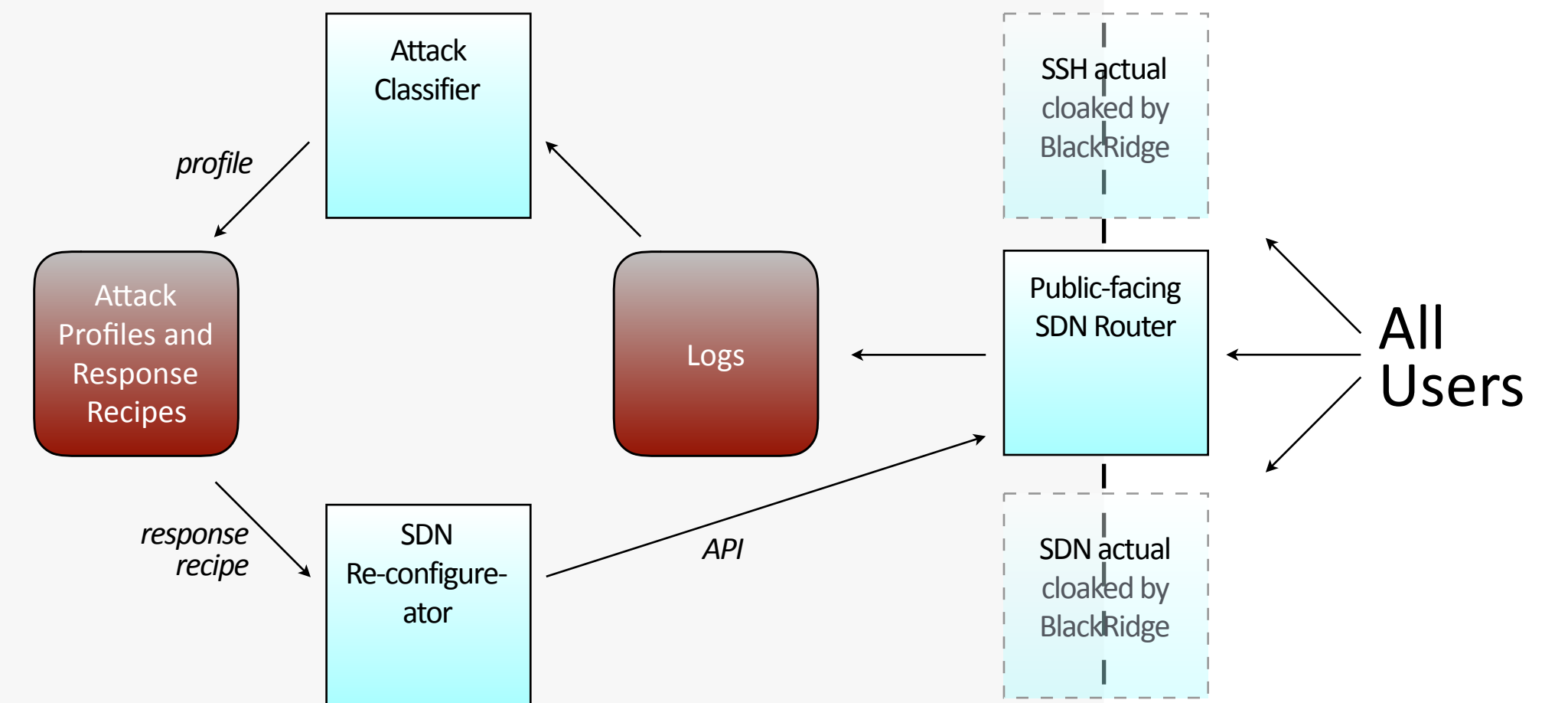
Public Internet

Private Intranet

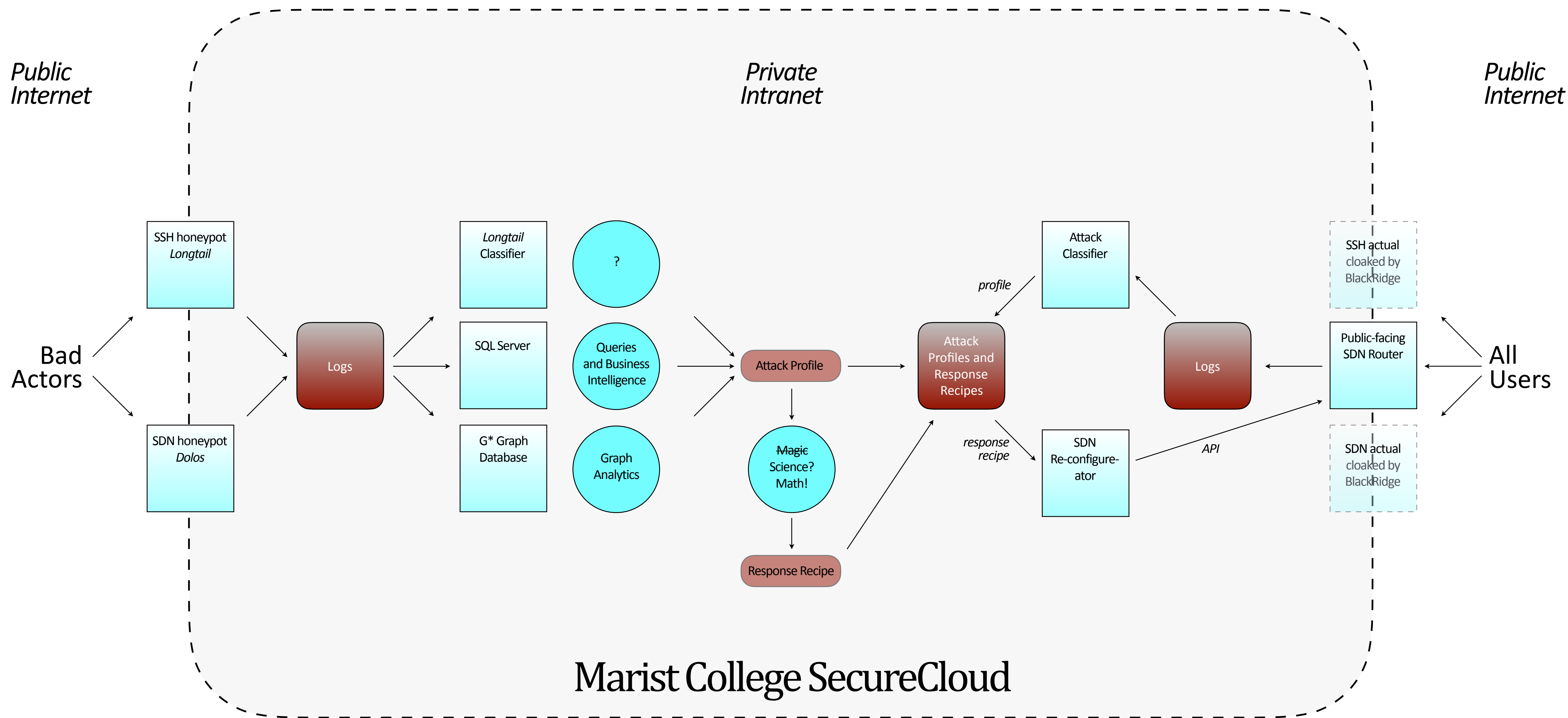
Public Internet

Things to add:

- attack classifier
- software orchestration magic (OpenStack/VMWare ESXi, SDN controller APIs)
- firewall and access control lists re-provisioning
- WAN bandwidth re-provisioning
- lots more



Continuous Monitoring and Response



- ?