SC2RAM: A **Deployable Cognitive** Model of a Cyber-Attacker

Van Parunak, Randy Jones
Soar Technology, Inc.
{van.parunak, rjones}@soartech.com

SOARTECH

Modeling human reasoning.
Enhancing human performance.

SOARTECH

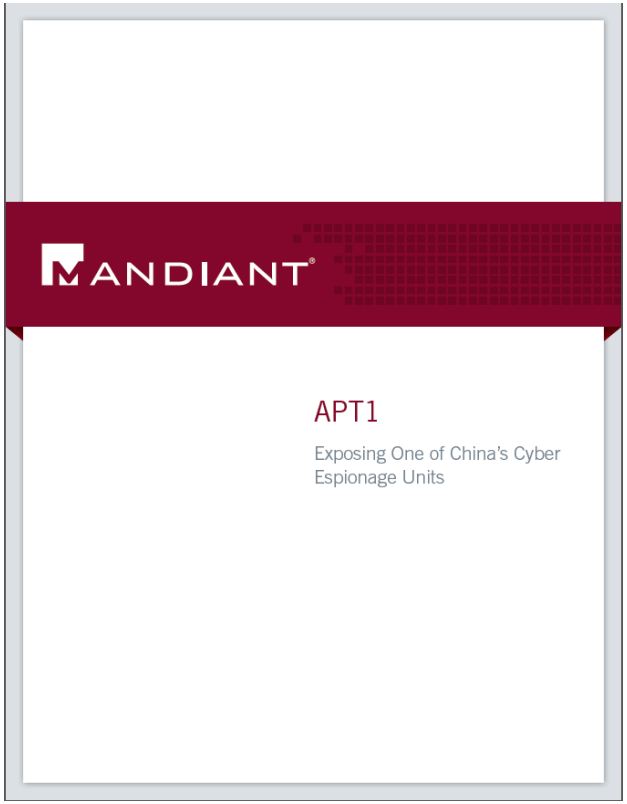
Advanced Persistent Threats

Persistent: Carried out over an extended period of time

Advanced: Multiple different steps, strategically related (e.g., initial compromise, establish foothold, escalate privileges, internal reconnaissance, move laterally, maintain presence, complete mission)

Adaptive: Human cognitive behavior

- *Sense* defensive actions and respond
- *Learn* from experience
- *Innovate* new actions
- *Interact* with (human and computer) colleagues



www.mandiant.com/apt1

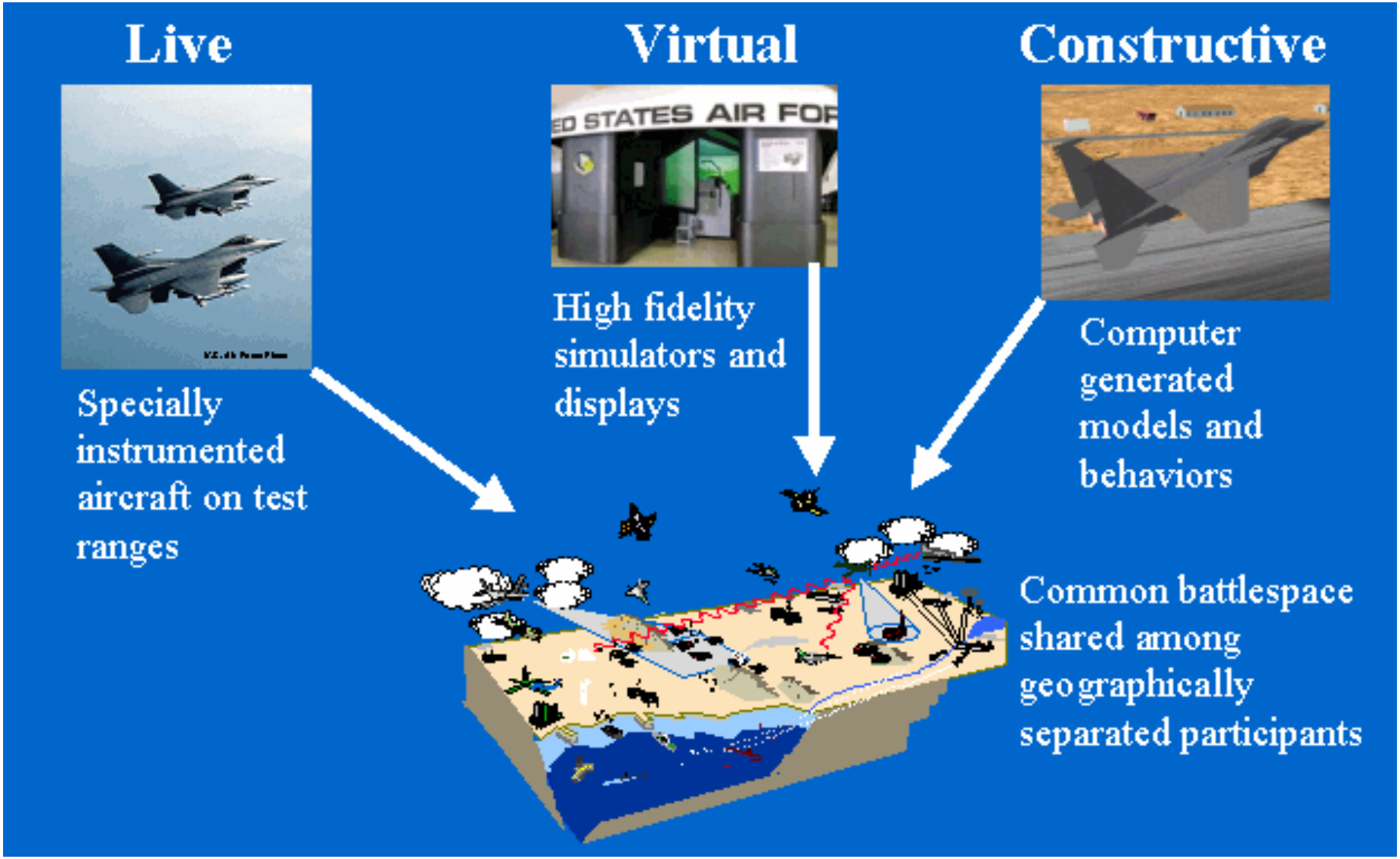
Highly-skilled **human Red Teams** are needed to

- *Train* system operators to deflect such threats
- *Configure and test* defensive systems
- *Wargame* the cyber-ecology to develop TTPs

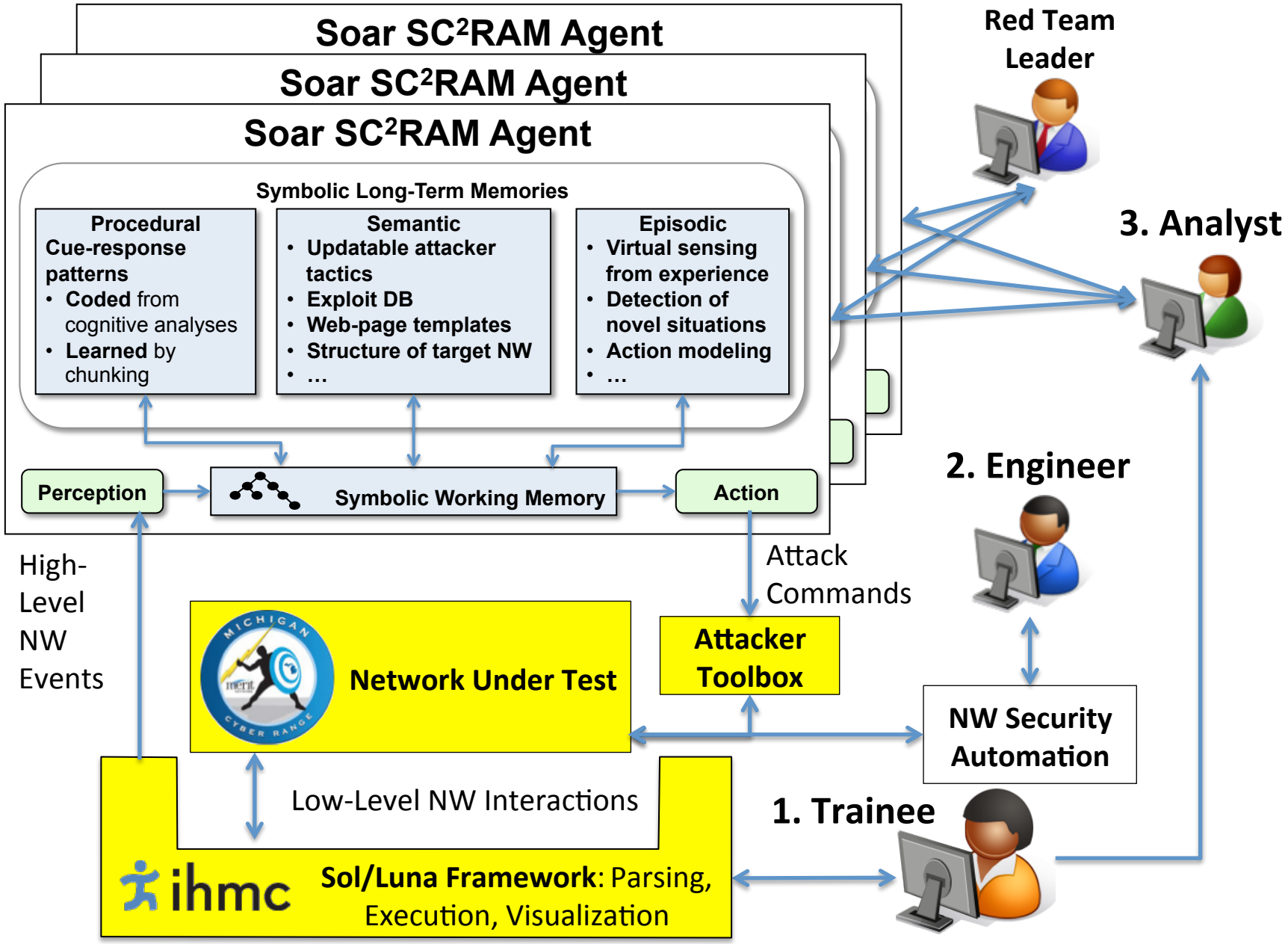
→ **SC2RAM**: Simulated Cognitive Cyber Red-team Attacker Model

SOARTECH

The TAC-AIR Soar Heritage in LVC Simulations

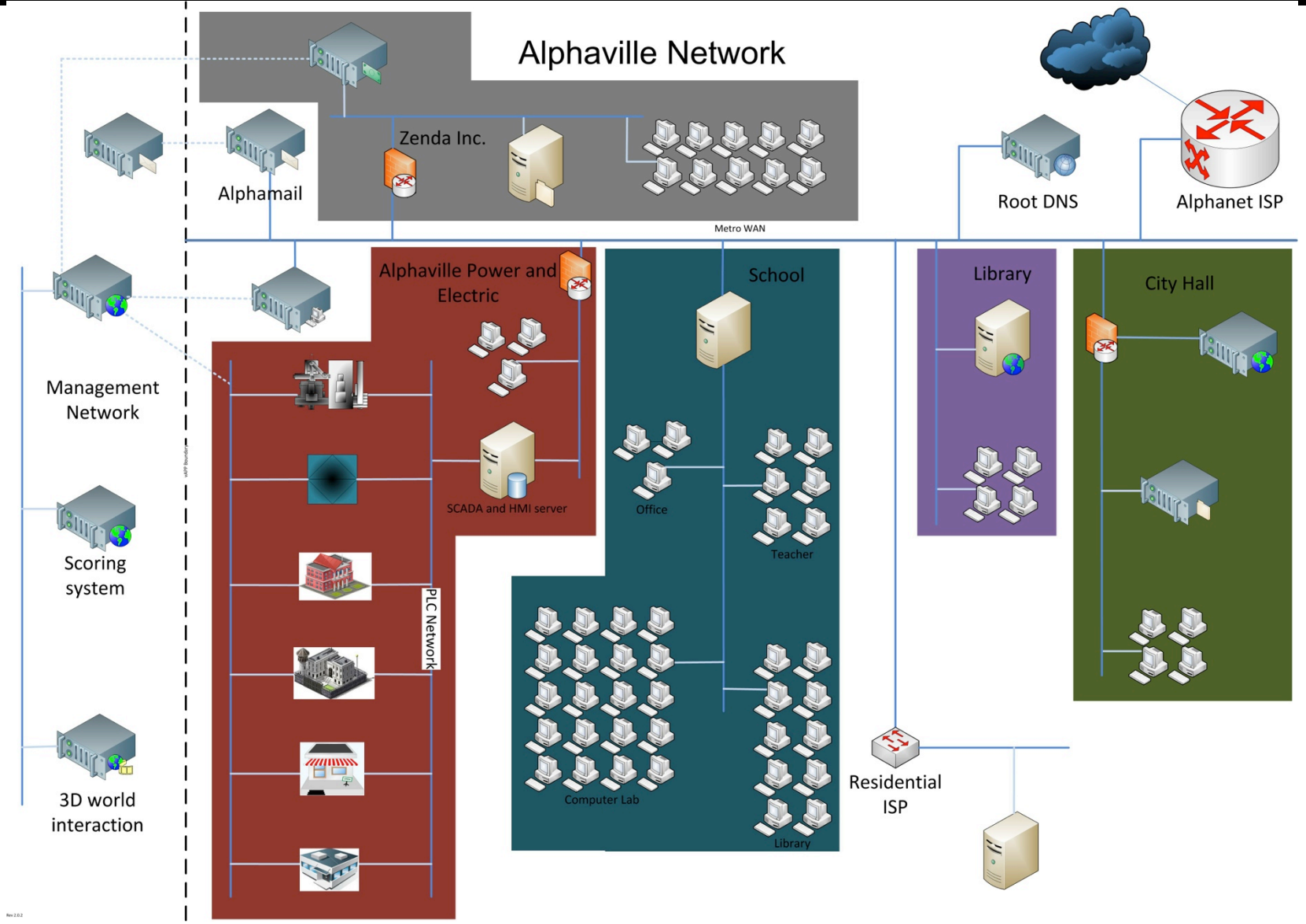


A Deployable Architecture



Alphaville

MICHIGAN CYBER RANGE



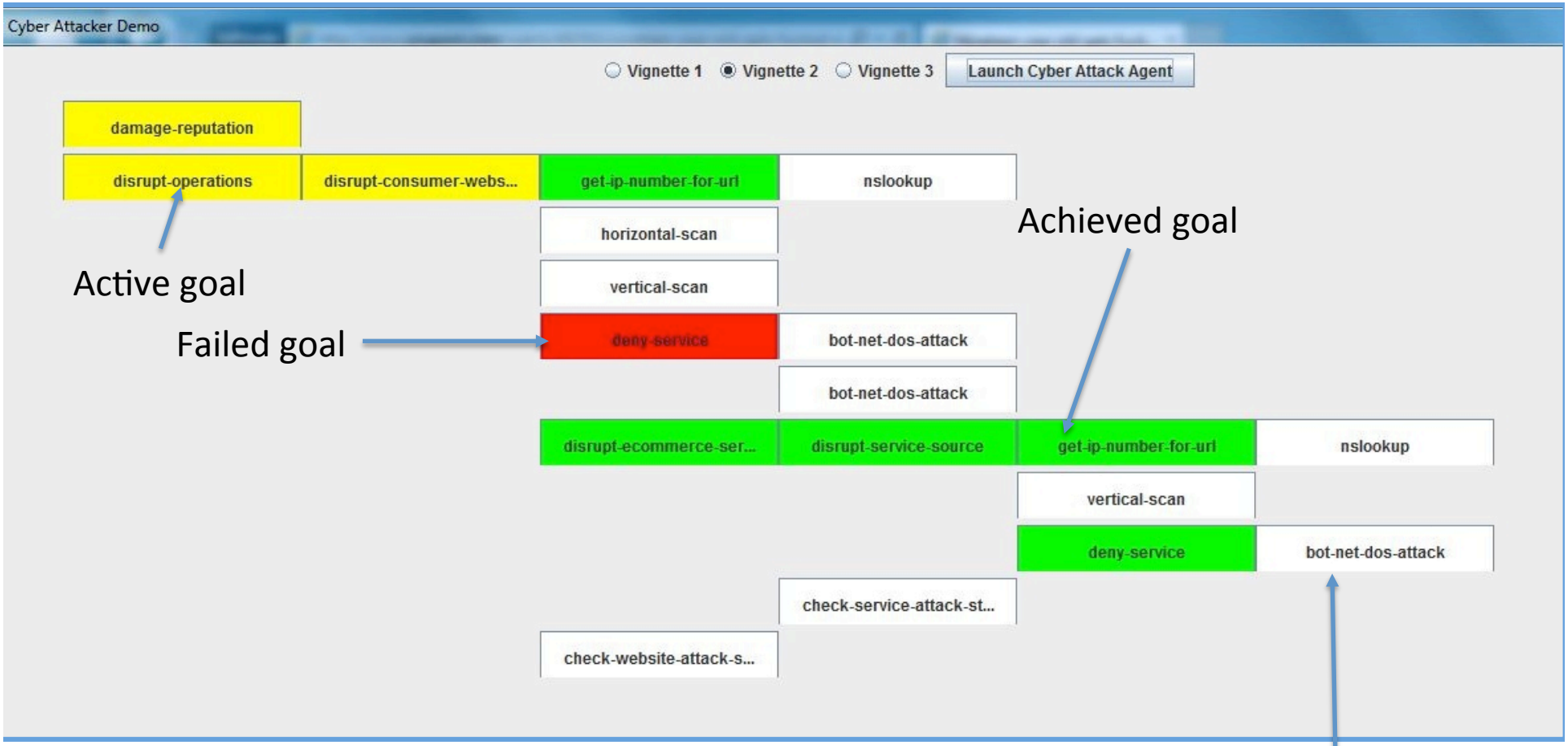
SOARTECH

Demo: Three Vignettes

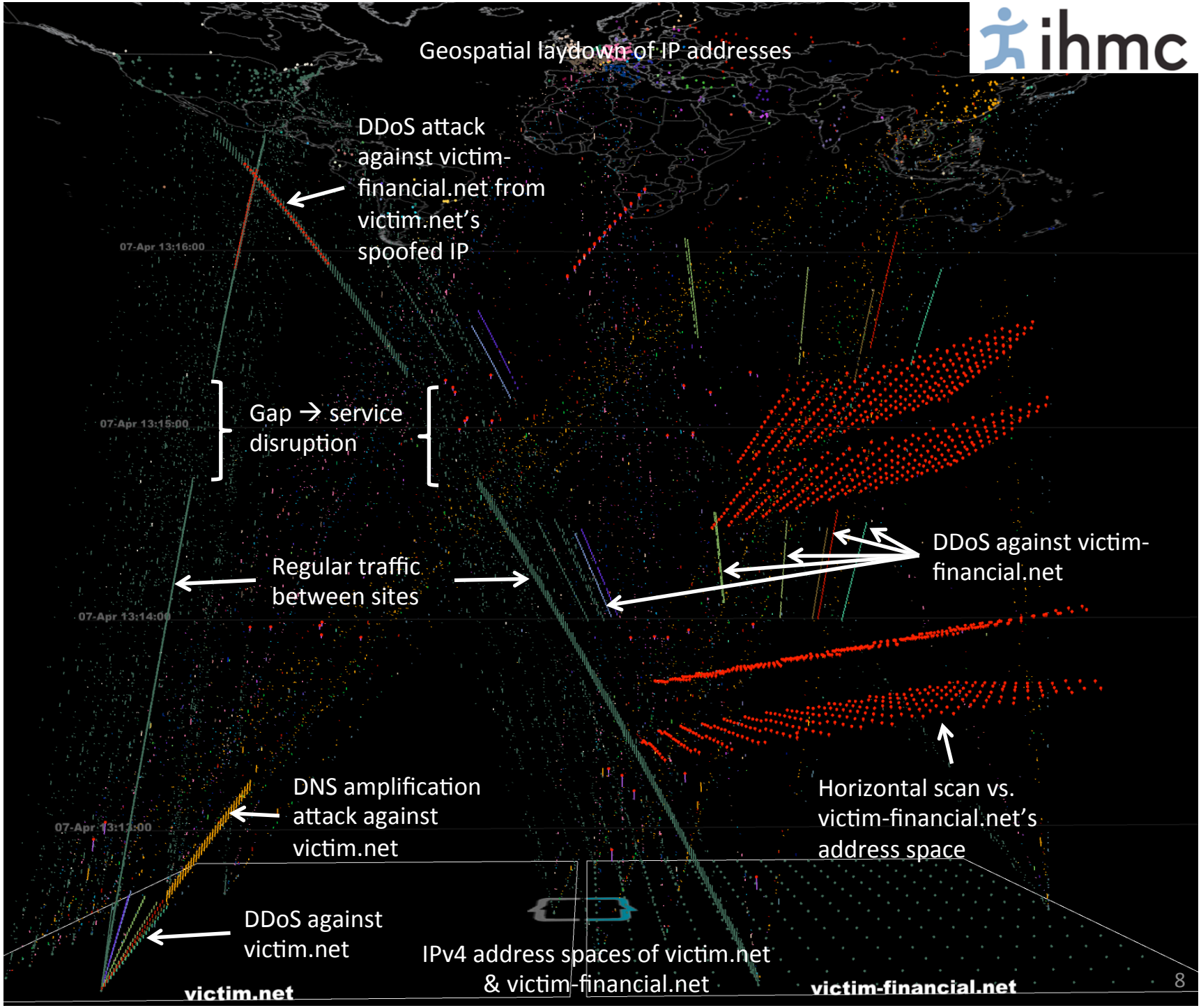
Attacker wants to disrupt the operations and damage the reputation of Company A, which uses Company B's DB service for financial transactions.

- Vignette 1
  - Attacker attempts a Denial of Service attack against Company A.
  - The attack fails, because of Company A's load-balancing infrastructure.
- Vignette 2
  - Attack also knows Company A's web site uses Company B's database service for financial transactions
  - Attacker successfully launches a DoS attack against Company B's database server
- Vignette 3
  - Company B shuts down traffic from attacking DoS IPs
  - Attacker initially believes DoS attack against B is successful, but double checks and finds A's web site still functioning
  - Attacker learns a new potential response/effect to a DoS attack is a blocked IP
  - Attacker formulates a new DoS attack from B to A by spoofing B's IP address
  - B responds by blocking traffic from A
  - Attacker verifies that A's web site is non-functioning

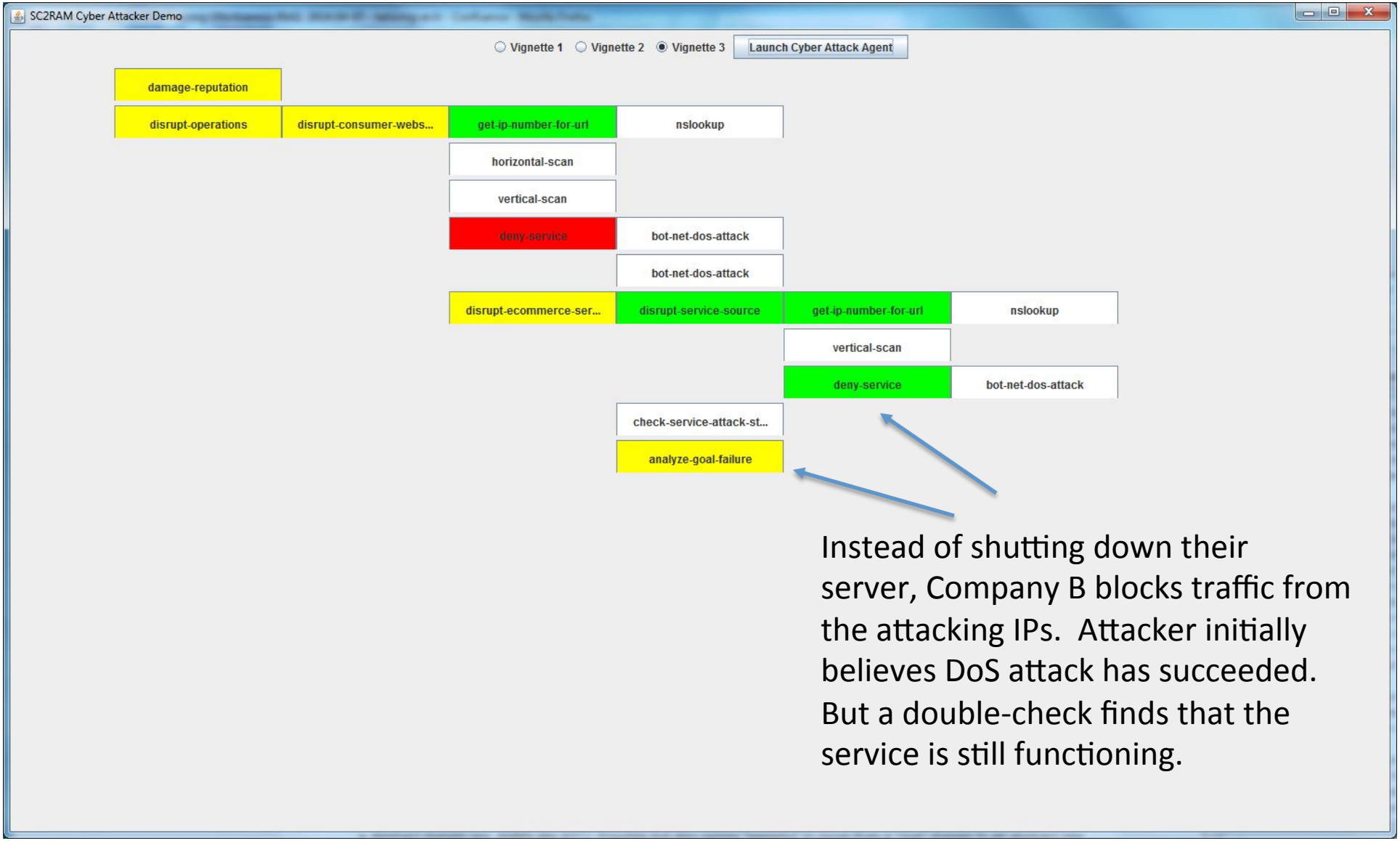
Agent Knowledge Example



Vignette 3 Example



Demo: Vignette 3

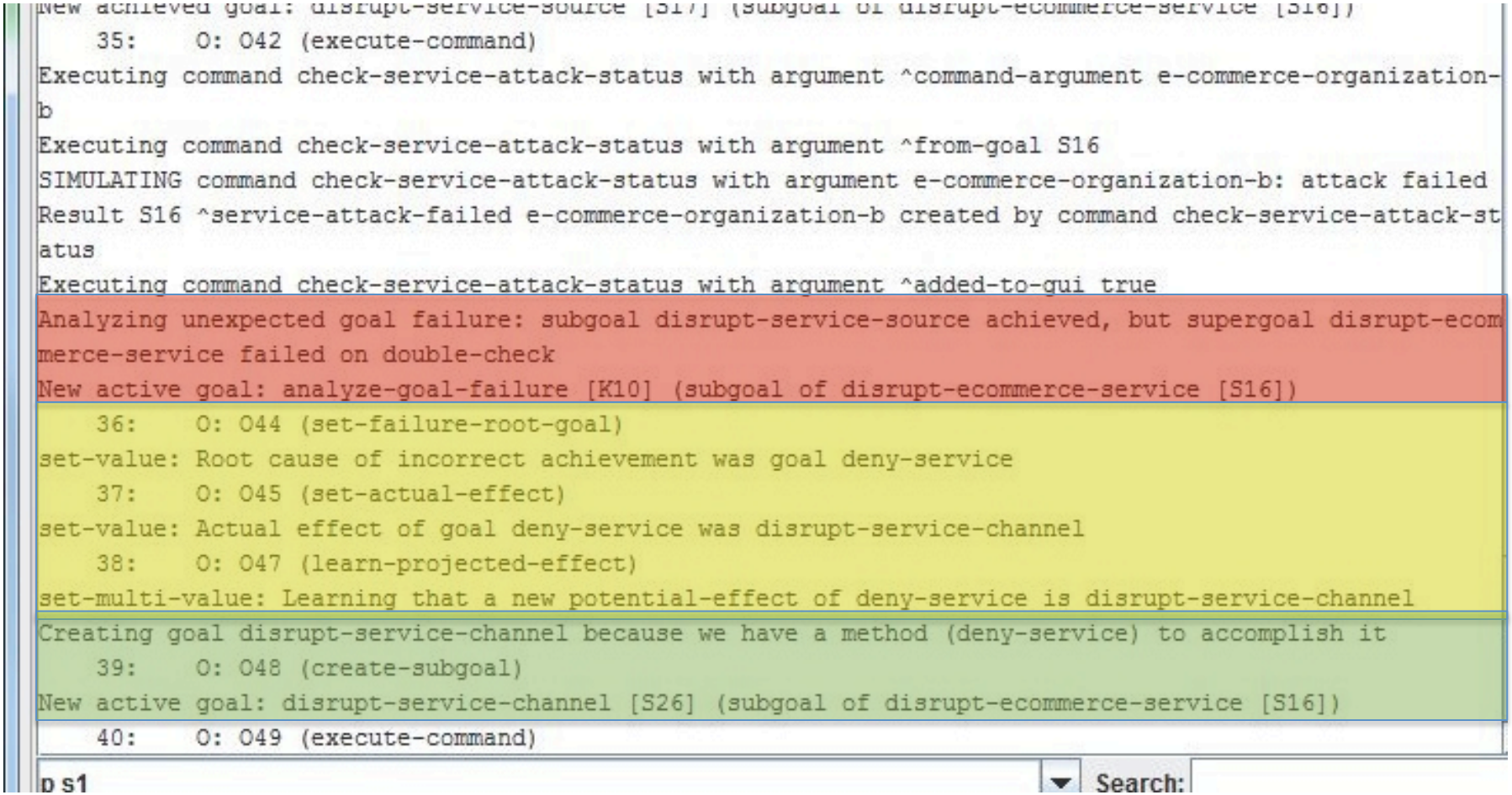


Instead of shutting down their server, Company B blocks traffic from the attacking IPs. Attacker initially believes DoS attack has succeeded. But a double-check finds that the service is still functioning.

SOARTECH

Demo: Vignette 3

Learning from an unexpected goal failure



SOARTECH

Demo: Vignette 3

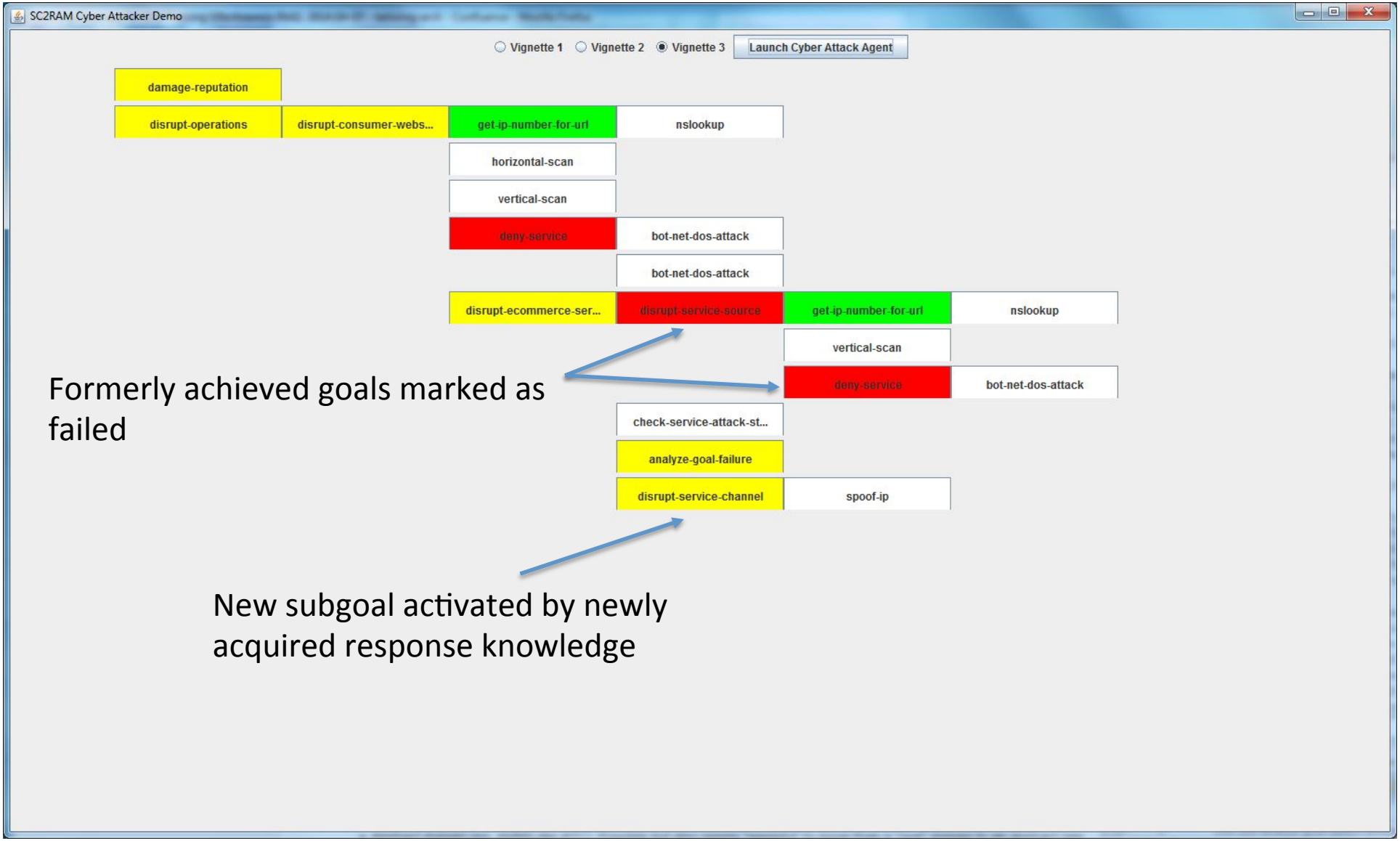
Goal-effect knowledge prior to learning:

(<k> ^goal <kg1>)
(<kg1> ^name deny-service
^potential-effect disrupt-service-source)

After learning:

(<k> ^goal <kg1>)
(<kg1> ^name deny-service
^potential-effect disrupt-service-source
^potential-effect disrupt-service-channel)

Demo: Vignette 3



Formerly achieved goals marked as failed

New subgoal activated by newly acquired response knowledge

SOARTECH

Conclusion

Nuggets

- Soar is well suited to the needs of modeling cyber operations
  - Adaptive
  - Innovative
  - Communicate with others
- Connection with real systems can be facilitated by hybrid architectures
  - IHMC's ontological reasoning for processing low-level NW events
- Strategic potential of collocation of Soar Lab, SoarTech, and Merit/MCR

Lumps

- Current knowledge is very simple, just a prototype
  - SMP
- Knowledge updating requires a Soar programmer
  - Opportunity for interactive task learning