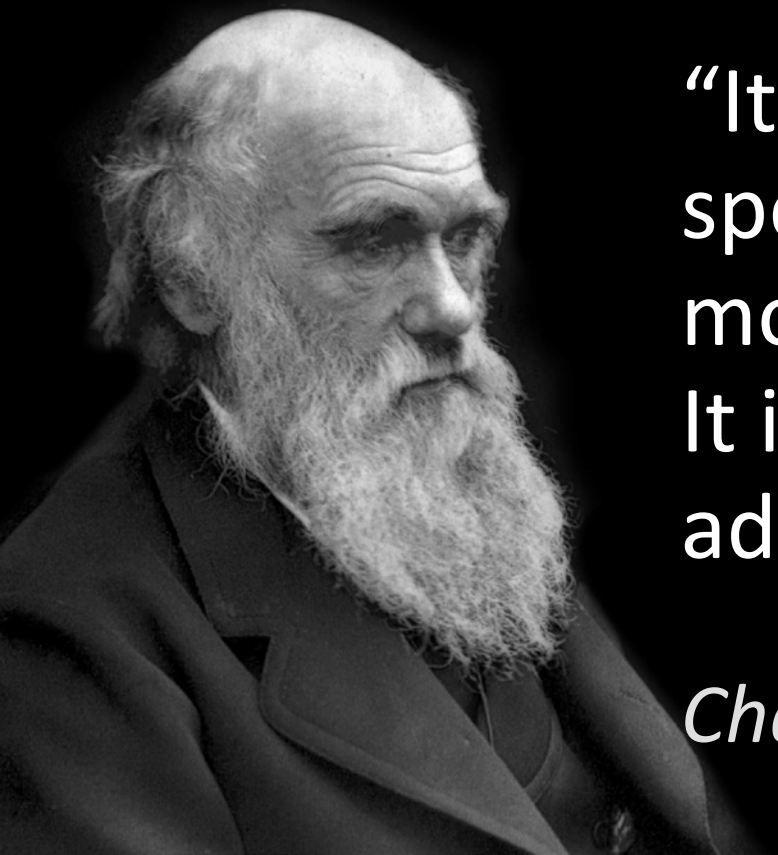
RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: SPO1-W12

CHARLES DARWIN, CYBERSECURITY VISIONARY

Dan Schiappa

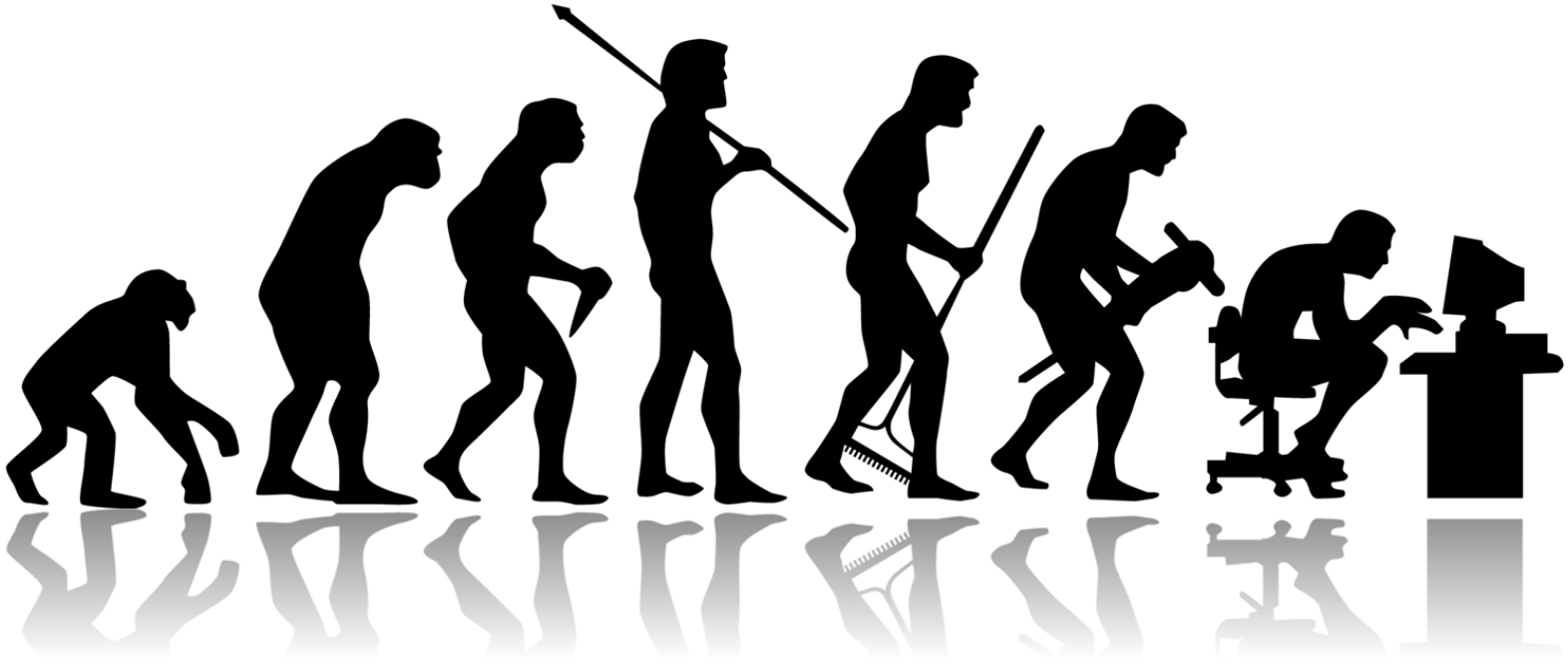
SVP and GM, Products
Sophos
@dan_schiappa



"It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change."

Charles Darwin (1809 – 1882)

Evolution



State of the Art

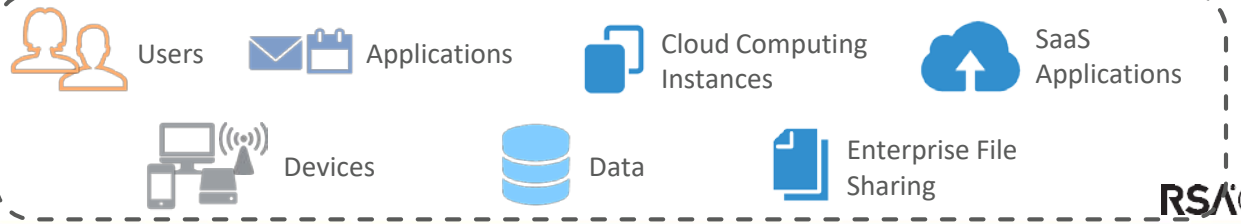
Security Operations Center

- Significant step up
- Requires Analyst
- Resource intensive
- Manual analysis and response

- Install
- Configure
- Set and Forget

Security Controls

Resources and Assets



So Why Don't I Feel safer?

You can't secure
what you don't know is there

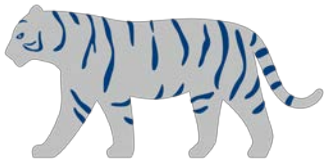
You can't manage
what you don't measure

You can't fix
what you don't know is broken

Evolution by Natural Selection

Discovery
Something is moving

Identification
Is this a predator, food, or a friend



Response
Fight or Flight

Analyze
It could be predator or food depending on the situation

Evolution of Security

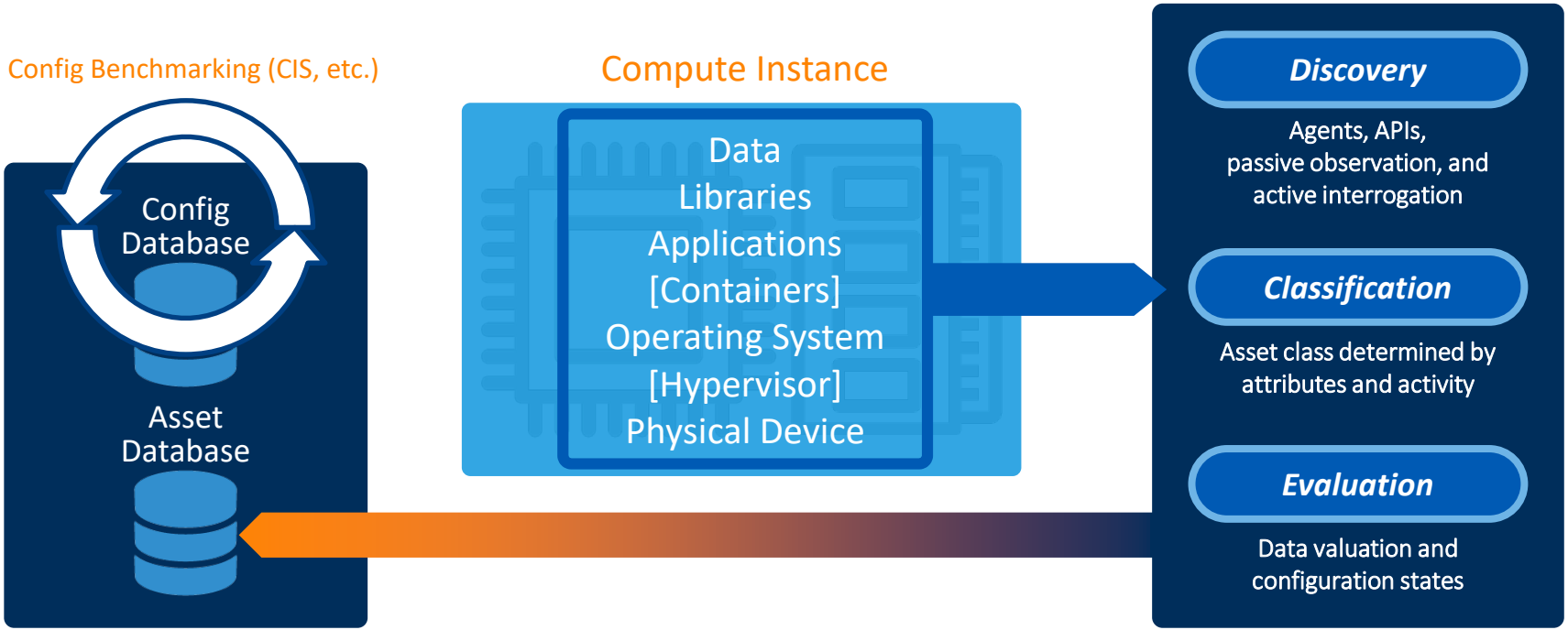
Discovery
Continuous discovery of devices, networks, apps, data, and workloads

Identification
Definition, collection, and organization

Response
Automated creation and enforcement

Analyze
Correlation and analysis of events, behaviors to the norm

Asset Discovery



Class-based, Programmable Event Models

ASSET CLASS → **EVENT MODEL**

Notebooks
Servers
Mobile Devices
Domain Controllers
IoT Devices
EC2 instances
Docker Containers
Etc...

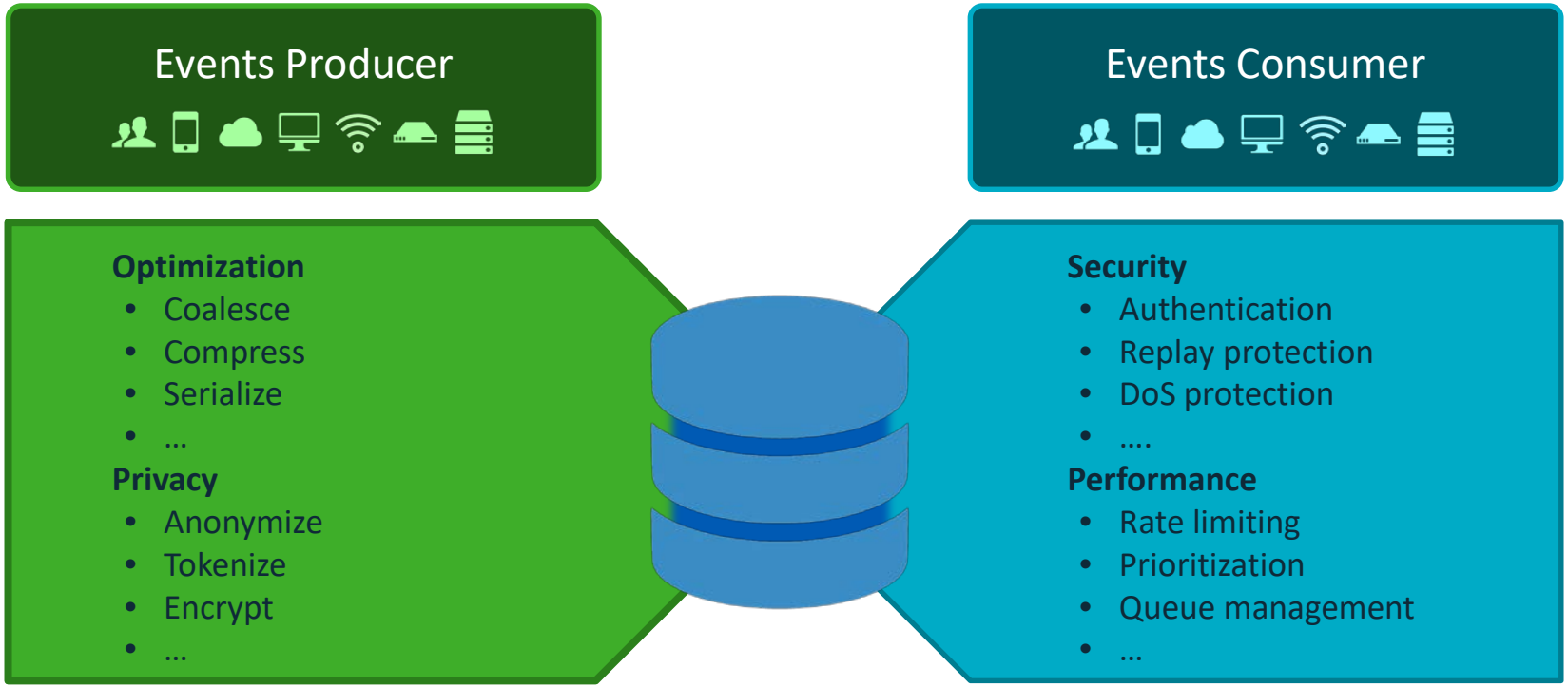
Mobile

{
”device”: ”iPhone X",
"name": "William Brown",
”device_id": S3817216BA
”chip”: ”A11 Bionic",
”storage": ”128MB",
“osbuild”: “15E218”
},
{
”accelerometer": ”37,23,…",
”gps": "51.6725448,-1.2645493}
}

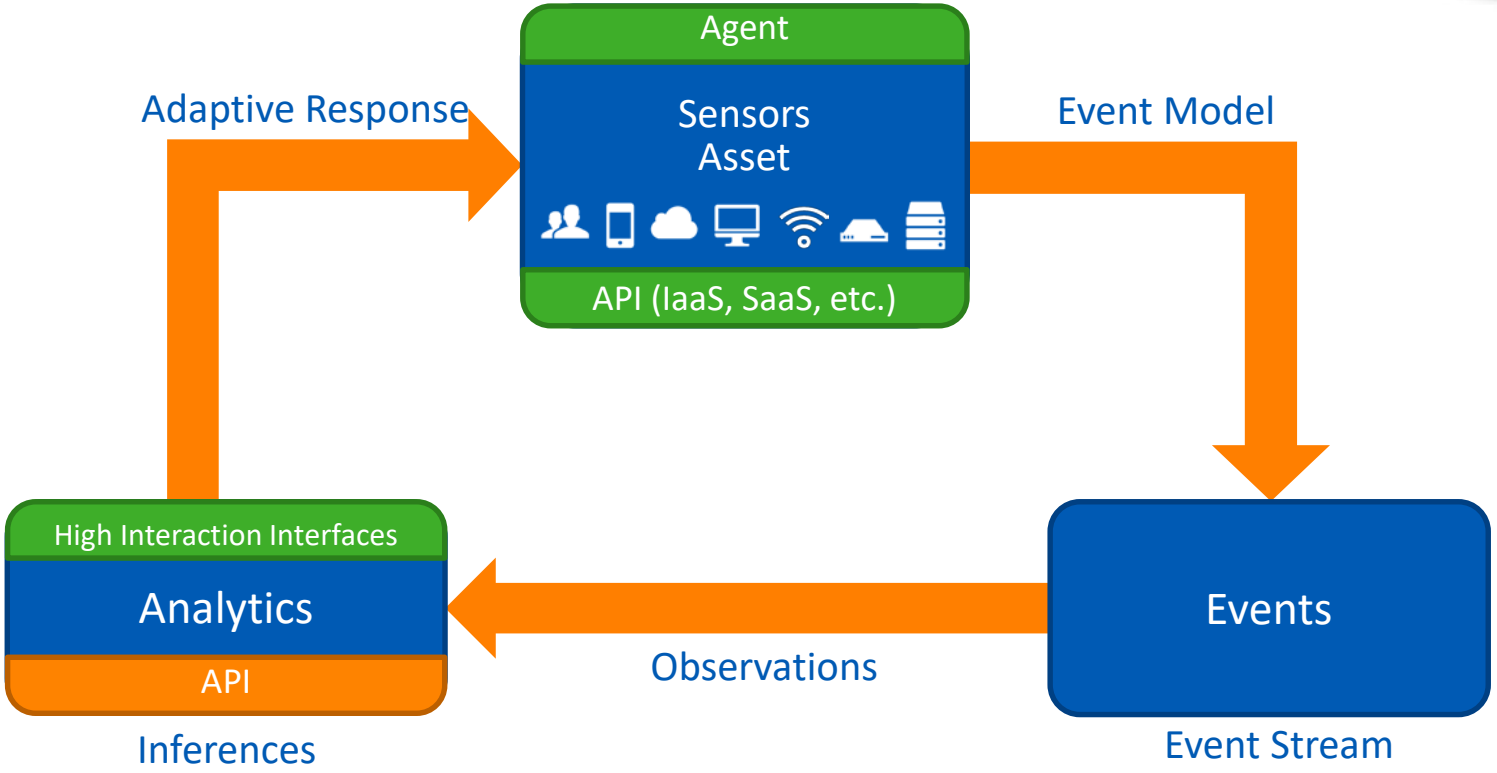
Domain Controller

{
”eventID": ”4688",
“desc": ”New Process Created",
“account”: “administrator”,
“cmdline”:
“C:\temp\moosifer.bat”
},
{
”eventID": ”4768",
”desc": ”Kerberos TGT requested",
”account": ”alexs",
”result": ”0x12”
},

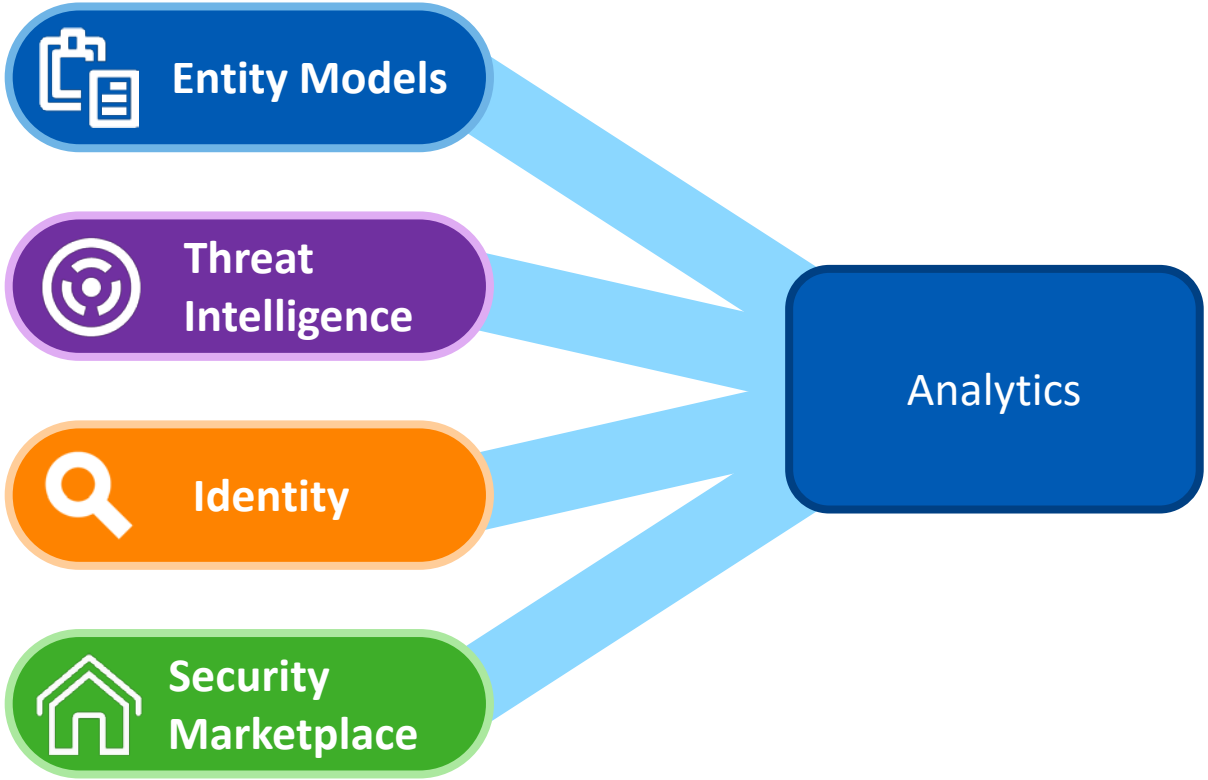
Event Exchange



SEAR: Sensors-Events-Analytics-Response

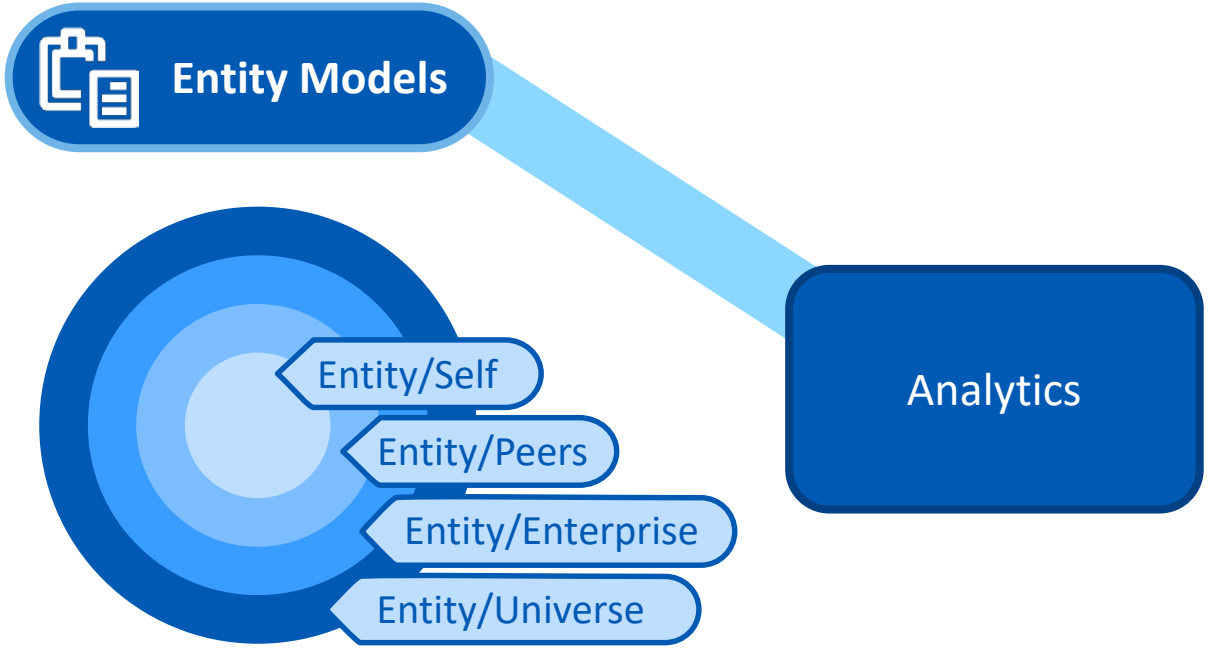


Analytics



- Create mathematical models from events
- Continuously analyze against baseline
- Discover anomalies
- High-Interaction Interfaces
- Adaptively respond

Entity Modeling



Model Construction

- Users, compute instances
- Continuously updated

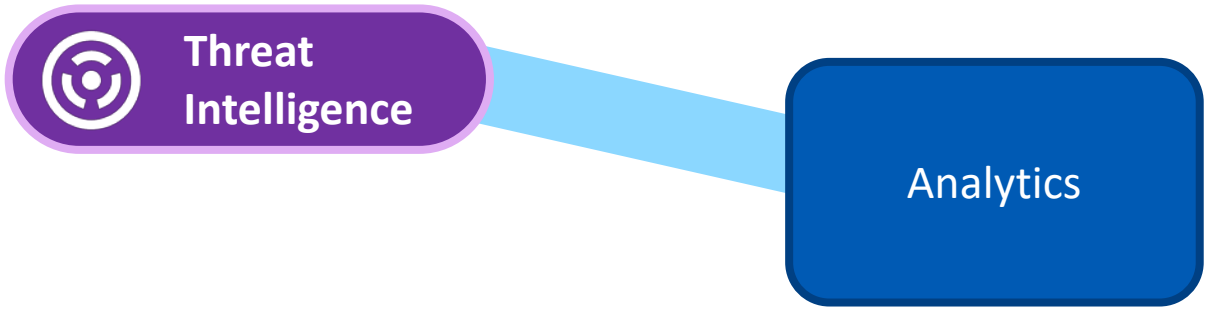
Modeled

- Data volumes
- URLs visited
- IP session partners
- File shares accessed
- Processes started
- Usage times and location
- …

Detections

- Outliers
- Anomalies / Impossibilities

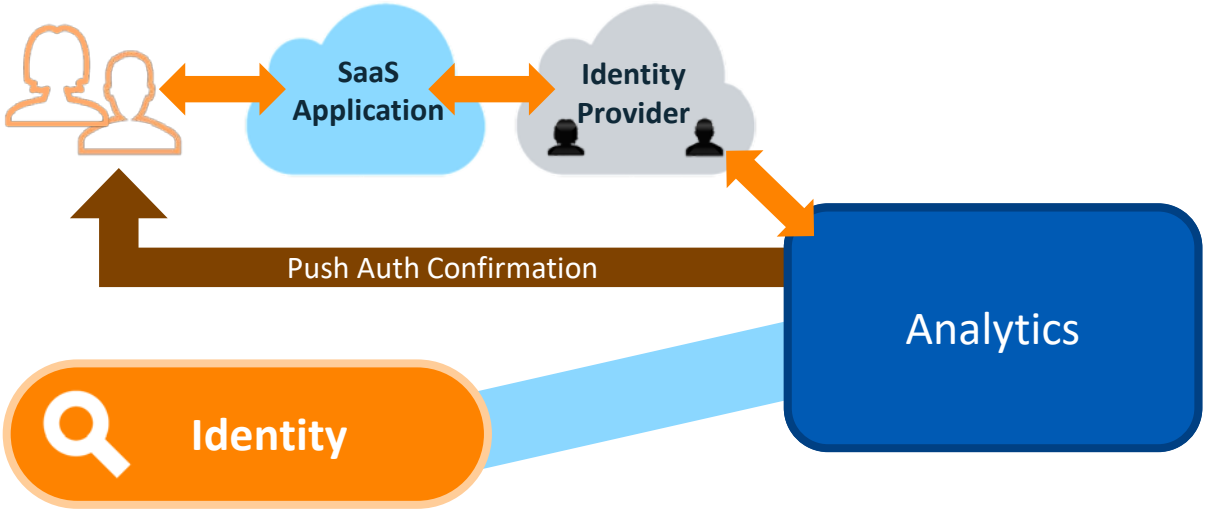
Threat Intelligence



Threat Intelligence

- Real-time and retrospective threat intelligence
  - Sophos Labs
  - 3rd Party, supporting STIX and TAXII
- Vulnerability data
- Patch information

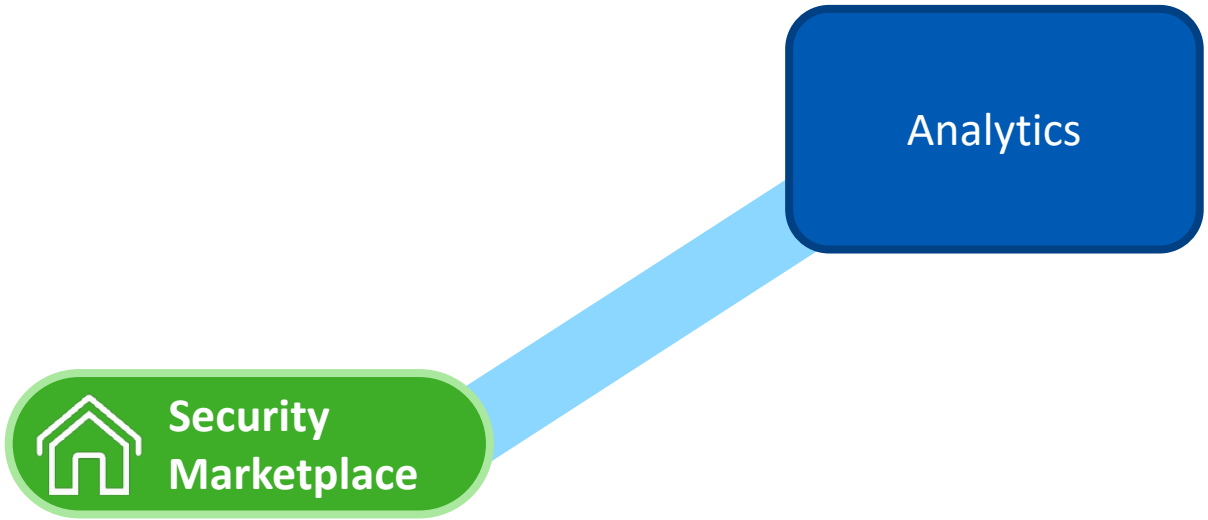
Identity and Continuous Authentication



Federation and MFA

- Security attestations based on user/device health states
- Support for SAML, OAuth, and OpenID standards
- Support for push-auth
- Conditional authentication (and de-authentication) based on representations in Central Analytics platform

Security Marketplace



Security Ecosystem

- API Everywhere

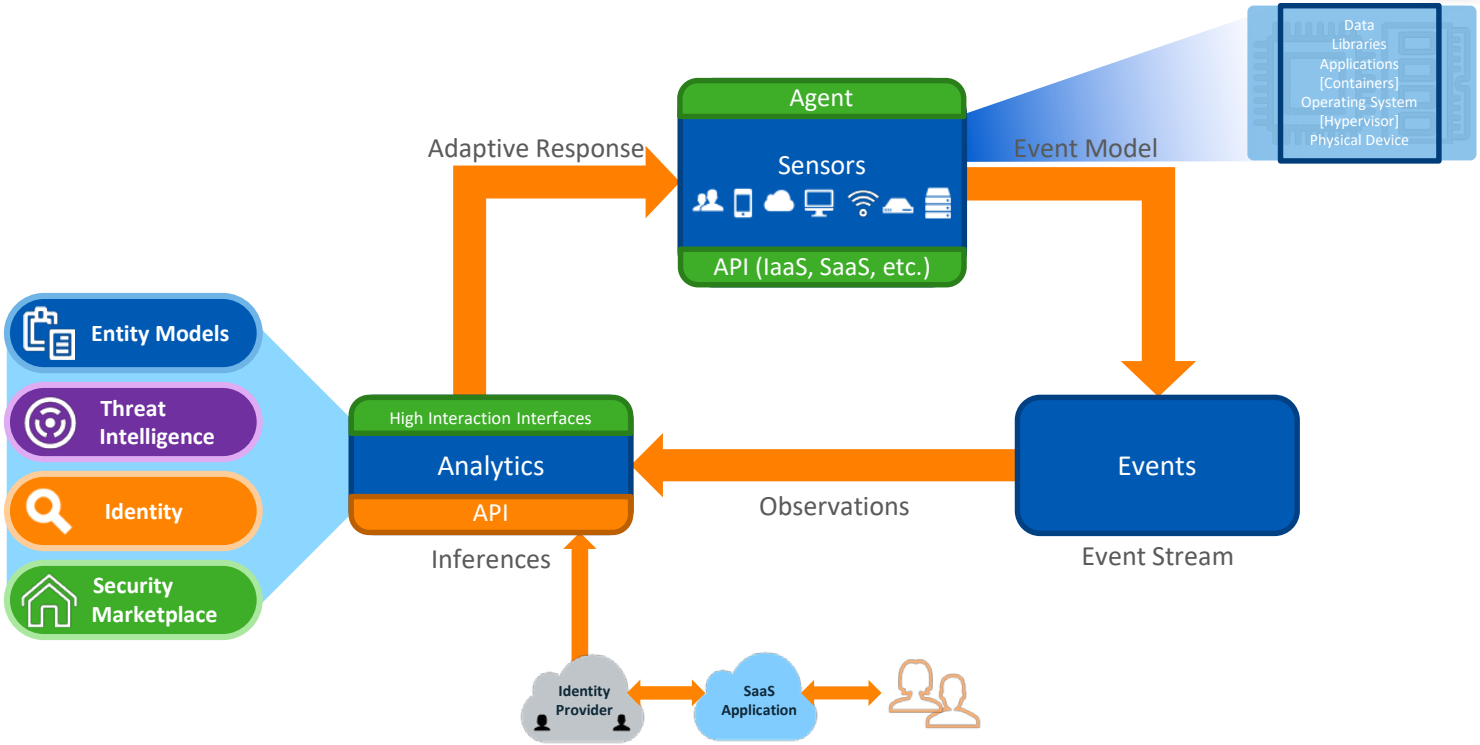
External Data Access

- 3rd parties can leverage data and events to develop complementary solutions (e.g. Dark Web analysis, training)

Data / Code Extensibility

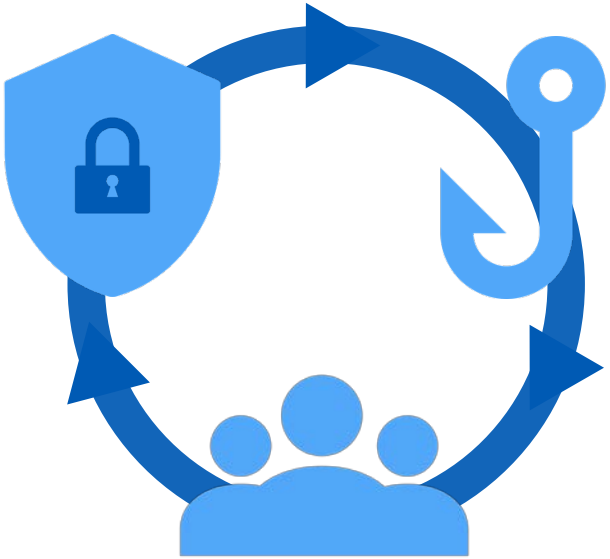
- Trusted vendors could extend asset classes and event models, deliver new agents (e.g. VA, patch)

Darwinian View of Security



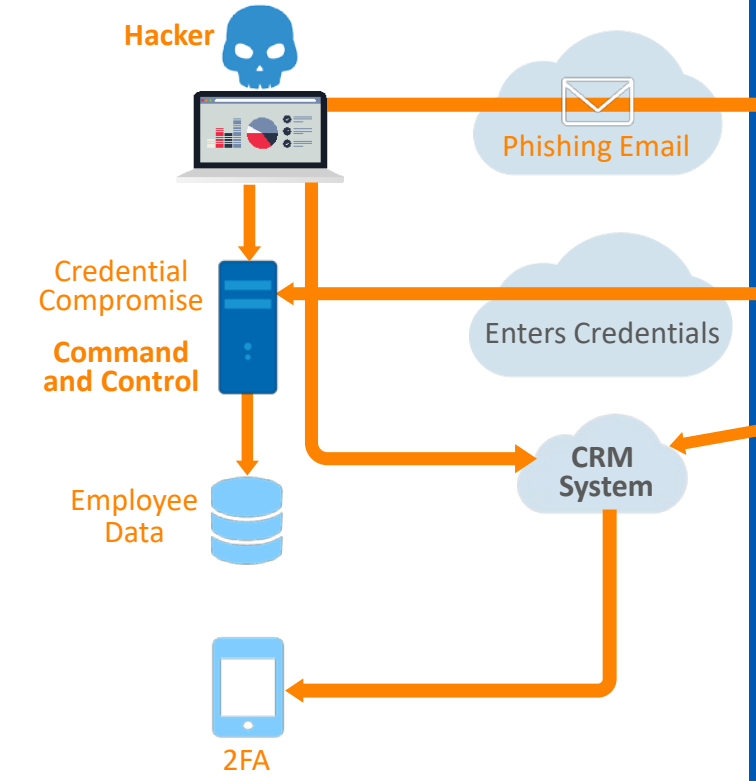
Dynamic Policy Based on User Experience

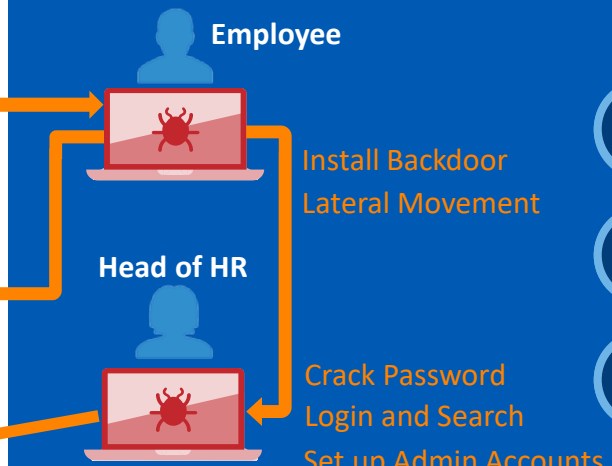
1. Protection policies assigned to User Groups based on awareness
2. User awareness assessed via phishing simulations and training



3. Users dynamically assigned to Groups based on behavior
4. Users get new policy based on Group membership

Synchronized Security Use Case





Applications

CRM System
Productivity Suite
Designer Tools
MFA
Note Taking
Collaboration
Etc…

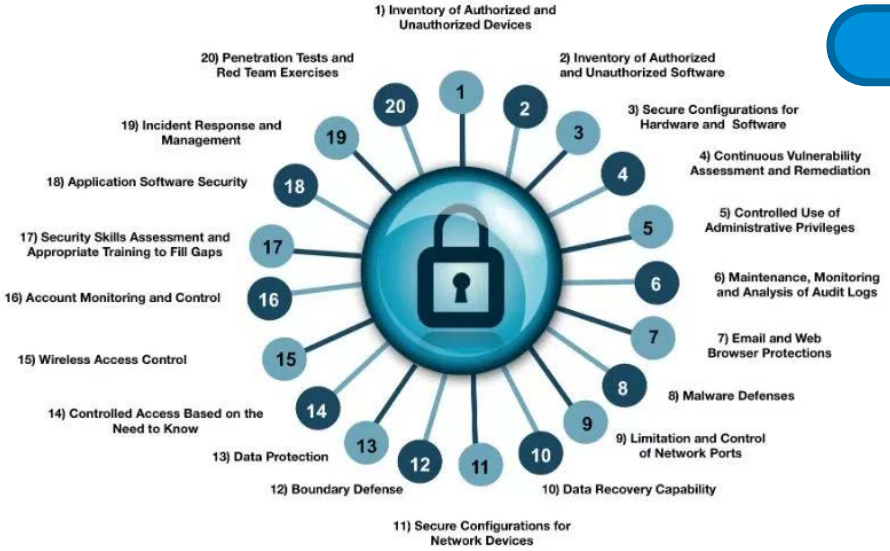
MFA Device

Authentication accepted twice

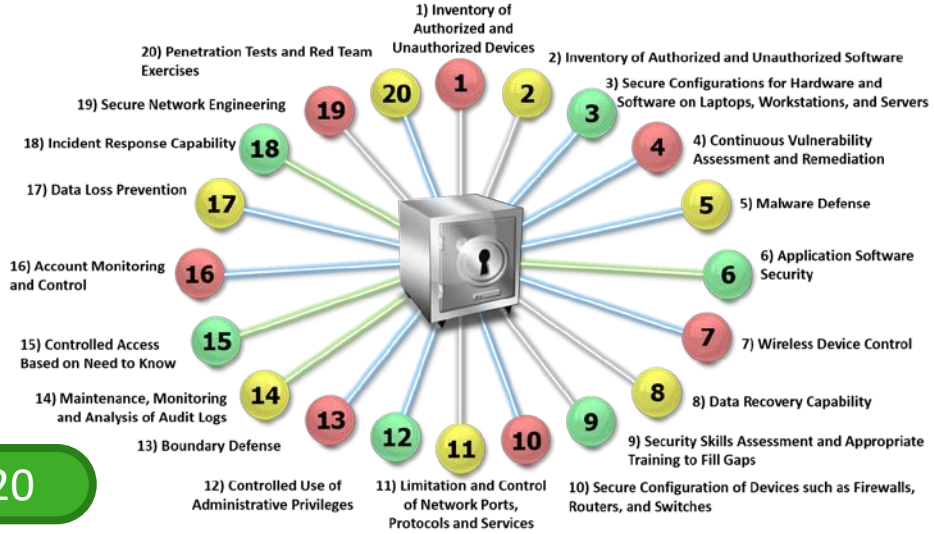
1. Employee entering credentials on a site with no reputation
2. Lateral movement to access Head of HR system
3. Privilege escalation on Head of HR system
4. Remote login to CRM system at same time as Head of HR
5. Accept second factor authentication twice
6. Multiple segmented downloads of employee database

SOPHOS

Darwinian Compliance Coverage



CIS TOP 20



SANS TOP 20

Apply What You Have Learned Today

Now

- Greatest survival benefit comes from adaptability

Next month

- Analyze your existing environment
  - Do you know how many managed/unmanaged devices you have?
  - Are you able to identify all the applications, users in your environment
  - How much of your environment is on-prem, hosted, or shadow IT?

Post Analysis

- Know thyself
- Define appropriate controls, changes for your environment
- Look for automation, not just information. You'll never be able to hire enough analysts and admins.

In 6 Months

- Invest in systems which enable continuous discovery, threat scoring and adaptive response

Thank You!