Oracle Identity Security Operations Center
Next-Generation Security Cloud Services

OOW Identity SOC Explanation & Demo

April, 2018

gusztav.szuhai@oracle.com
Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Oracle Identity SOC Provides Next-Generation Security

1. Full Access to Data From Hybrid Cloud Without Penalty
2. Adaptive ML-based Analytics with Identity & Ops Context
3. Direct & API-based Collection, Detection & Automation
Security Cloud Services: Enabling customers to secure on-prem and heterogeneous cloud services

Identity Cloud Service

Security Monitoring & Analytics Cloud Service

Cloud Access Security Broker Cloud Service

API Platform Cloud Service

Compliance Cloud Service

Hybrid Data Security Protection: Database Security
Oracle’s Cloud Access Security Broker (ex-Palerra)

- **Visibility**
- **Compliance**
- **Data Security**
- **Threat Protection**

**Direct Cloud Service Access**

**CASB**

**Enterprise Security Integration**

**API Access**

**MOBILE USERS AND DEVICES**

**ENTERPRISE**

**INSIDE PERIMETER**

- SIEM
- IDaaS
- NGFW
- DLP
- MDM

**IaaS**

**PaaS**

**SaaS**

**Oracle Cloud Access Security Broker**

**Oracle’s Cloud Access Security Broker (ex-Palerra)**

**Visibility**

**Compliance**

**Data Security**

**Threat Protection**
Ongoing assessment of configurations for on-premises and cloud deployments

Analyze deviations from industry benchmarks and best practices

Protect applications from unwanted changes and known vulnerabilities
Shared Responsibility Model

- **IaaS**
  - Identity
  - Security Monitoring & Analytics
  - API Platform
  - Virtualization
  - Network
  - Infrastructure
  - Physical

- **PaaS**
  - CASB
  - Configuration & Compliance
  - Service configuration
  - Data
  - Apps
  - OS
  - Virtualization
  - Network
  - Infrastructure

- **SaaS**
  - Service configuration
  - Data
  - Apps
  - OS
  - Virtualization
  - Network
  - Infrastructure
Architecture for customer for On-prem and Cloud Security
Independent services that can be layered or independent

<table>
<thead>
<tr>
<th>On-premise</th>
<th>Non-Oracle Cloud</th>
<th>Oracle Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IaaS, PaaS, SaaS</td>
<td>IaaS, PaaS, SaaS</td>
</tr>
<tr>
<td>Security Monitoring and Analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration and IT compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>API Security and Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Access Security Broker – deep monitoring and threat detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relational and Big Data Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Future Security Cloud Services</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Identity SOC – Conceptual Architecture

- On-Premises Activity
- Identity Context
- Identity SOC
- Cloud Activity
- Asset Context
- Threat Intelligence
- Cloud
Mary Baker:

57

Threat 1 of 4: Suspicious Browsing from Anomalous Source

Sep 26, 2017 12:31:32

Suspicious URL
http://ecoheat22.ro:80
Reputation Score: Low (36)
Frequency: 2

Auto Remediated Actions
- User added to suspicious user watch list
- Risk score updated: 57

Optional Actions
Top recommended manual actions for this threat:

- Search: Search on anomalous attribute values.
- View: View raw events related to this threat.
- Record: Record your investigation for others to reference.
User = mary.baker@rideshare.com AND URL_Reputation IN (Suspicious, Malicious) AND sourceIP IN (Baseline, Anomaly)

<table>
<thead>
<tr>
<th>Time (UTC-7:00)</th>
<th>Original Log Content</th>
</tr>
</thead>
</table>
Mary Baker

Threat 2 of 4: Brute Force Attack
Sep 28, 2017 09:17:21

At tempted Logins
Target Asset: rs_app02

- Failed Login
- Successful Login

Auto Remediated Actions
- MFA Imposed
- Risk score updated: 59

Optional Actions
Top recommended manual actions for this threat:
- Identity: Impose MFA, change access or disable user account.
- View: View raw events related to this threat.
- Record: Record your investigation for others to reference.

View More...
Mary Baker: Mary.Baker

Risk Score: 85

Threat Details

Attempted Logins
Target Asset: rs_app02

- Sep 28, 09:13:52 Failed Login
- Sep 28, 09:17:21 Successful Login

Auto Remediated Actions
- MFA Imposed
- Risk score updated: 59

Optional Actions

Identity

- MFA Status: Enabled
- User Status: Suspended
- Password: Reset

Submit Cancel
Mary Baker

Threat 3 of 4: SQL Anomaly Against Watchlist Resource
Sep 30, 2017 11:40:08

Description: Rare sql activity from user mary.baker against watchlist resource

Anomalous SQL:
```
SELECT grantee, granted_role, admin_option, default_role FROM dba_role_privils WHERE granted_role IN ('GGSYS_ROLE', 'EXP_FULL_DATABASE', 'DATAPUMP_EXP_FULL_DATABASE') AND grantee NOT IN ('DBA', 'SYS');
```

Target Asset:
r_s_dbo

Watchlist Resource:
dba_role_privils

Baseline SQL Count:
1,436

Similarity Score:
10-30%

Top Nearest Neighbor Queries:

<table>
<thead>
<tr>
<th>Topmost 3 Nearest Neighbor Queries</th>
<th>Similarity Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>select * from dba_tab_privls where GRANTEE = :b1;</td>
<td>30%</td>
</tr>
<tr>
<td>select * from dba_tab_privls where GRANTEE = :b1 and privilege = :b2;</td>
<td>30%</td>
</tr>
</tbody>
</table>

Auto Remediated Actions:
- Target added to critical asset watchlist
- Risk score updated: 69

Optional Actions:
- Search: Search on anomalous attribute values.
- View: View raw events related to this threat.
- Record: Record your investigation for others to reference.

View More...
Threat 4 of 4: Exfiltration
Oct 2, 2017 03:21:36

“Staging” S3 Bucket Data Exposure

Access Permissions

<table>
<thead>
<tr>
<th></th>
<th>Restricted</th>
<th>Confidential</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td><img src="chart1.png" alt="Public Chart" /></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External</td>
<td><img src="chart2.png" alt="External Chart" /></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal</td>
<td><img src="chart3.png" alt="Internal Chart" /></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private</td>
<td><img src="chart4.png" alt="Private Chart" /></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Auto Remediated Actions

- Incident created
- CASB DLP workflow enabled
- Risk score incremented from 69 to 85

Optional Actions

Top recommended manual actions for this threat:

- **Explore**
  - Explore Data Risk in CASB Data Navigator
- **View**
  - View base events related to this threat.
- **Record**
  - Record your investigation for others to reference.

View More...