Cautionary Statement Regarding Forward-Looking Statements

This presentation includes express and implied “forward-looking statements”, including forward-looking statement within the meaning of the Private Securities Litigation Reform Act of 1995. Forward-looking statements include all statements that are not historical facts, and in some cases, can be identified by terms such as “anticipate,” “believe,” “estimate,” “expect,” “intend,” “may,” “might,” “plan,” “project,” “will,” “would,” “should,” “could,” “can,” “predict,” “potential,” “continue,” or the negative of these terms, and similar expressions that concern our expectations, strategy, plans or intentions. Forward-looking statements contained in this presentation include, but are not limited to, statements concerning the performance and benefits of our platform, products and services; our strategic plans or objectives; our growth prospects; and our future financial and operational performance. By their nature, these statements are subject to numerous risks and uncertainties, including factors beyond our control, that could cause actual results, performance or achievement to differ materially and adversely from those anticipated or implied in the statements. These and other risk factors are described in the “Risk Factors” section of our most recent Form 10-Q and/or Form 10-K filed with the Securities and Exchange Commission. You should not rely upon forward-looking statements as predictions of future events. Although our management believes that the expectations reflected in our statements are reasonable, we cannot guarantee that the future results, levels of activity, performance or events and circumstances described in the forward-looking statements will be achieved or occur. Recipients are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date such statements are made and should not be construed as statements of fact. Except to the extent required by federal securities laws, we undertake no obligation to update these forward-looking statements to reflect events or circumstances after the date hereof, or to reflect the occurrence of unanticipated events.
Accelerate From Zero to Sixty in No Time: A Fast Path to Becoming a CrowdStrike API Expert

Devin Cargill, DevOps Engineer, CrowdStrike Falcon Complete
Agenda

- API Overview
- Deep Dive: OAuth 2
- Deep Dive: Devices
- Deep Dive: Detections
- Takeaways
Devin Cargill
DevOps Engineer – Falcon Complete

- Located in St. Louis, MO
- Started career as System Administrator
- Came to CrowdStrike May 2018 – Intern
- Automation is the way
Example Value

```json
{
  "errors": [
    {
      "code": 0,
      "id": "string",
      "message": "string"
    }
  ],
  "meta": {
    "pagination": {
      "limit": 0,
      "offset": 0,
      "total": 0
    },
    "powered_by": "string",
    "query_time": 0,
    "tenant_id": "string",
    "version": {
      "resources_affected": 0
    }
  },
  "resources": {
    "buckets": {
      "count": 0,
      "from": 0,
      "key_as_string": "string",
      "string_from": "string",
      "string_to": "string",
      "sub_aggregates": [
        {
          "sum": 0,
          "value": 0,
          "value_as_string": "string"
        }
      ],
      "name": "string",
      "sum_other_func_count": 0
    }
  }
}
```

Headers:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-RateLimit-Limit</td>
<td>Request limit per minute.</td>
<td>integer</td>
</tr>
<tr>
<td>X-RateLimit-Remaining</td>
<td>The number of requests remaining for the sliding one minute window.</td>
<td>integer</td>
</tr>
</tbody>
</table>
Deep Dive: OAuth 2
Deep Dive: OAuth 2

Client ID
Client Secret

Access Token

Headers = {
    "Authorization": "Bearer" + Access_Token
}
Deep Dive: OAuth 2

```json
{
    "access_token": "eyJhbGciOiJSUzIiLjEiLiJmYspjM0d4SCs5LWxzY2x5MiNzLz0iTGRpNiNvbWV0dG1lciI6Ml0iLCJzdW1iZXJzIjoiZXNlc3RyYW5kdXN0eWxlIiwiZGV2aWNlIjoiMjM5NzQzN2UzZmQ2NWY5LWQ3OTUtMzFkOC0wN2M0LWFjZjMtOTM1Yi00ZjQ2LTc0Y2ItNWNhZTVlMzNjZjMiIiwiaWF0YWRhdGVFIiwiMjQ3YmU5MGYxZjFlODJhYmZlZjE3ZjU1OTA0ZSIsInV1Y2U6b3JpZGVkeS1jb2R1bmsiOiIyZjIyMDI3ZDViZjM1ZTc5ZmQyMDg5ZjE5ZjE0YjM5YzEiLCJzdW1iZXJzIjoiYW1vdW50b2JvdGlvbklkIiwiY2hpb25zZG9jaWZpYyI6IjJiNDQwMDUxOTZkMzA0MzNiMTFiYzRjZDAiLCJoYXZwaWQ6ZGV2aWNlIjoiMmY0NzU2MTUxNjU3ZmU0ZmY4MmFhMjFjZjViNzE5ZjUiLCJzc3VzZGVkcyI6Ijg3ZmMyM2IyZWYzZDIwZTExMGIzZjZkZTk0Mjg2ODZiIiwiaGFzd本次2019年holderIjoiZjVlMWFlNDQxZjYyMzZlYzEwZmY2NDAyZjMzZGUyZjIyZjAiLCJpdGVtZ2VyX2NvbSIsIjoiMjQ3YmU5MGYxZjFlODJhYmZlZjE3ZjU1OTA0ZSIsImF1ZGxpbmVzX2FwaWQiOiIyZjIyMDI3ZDViZjM1ZTc5ZmQyMDg5ZjE5ZjE0YjM5YzEiLCJteWJsZ2V0X2FwaWQiOiIyZjIyMDI3ZDViZjM1ZTc5ZmQyMDg5ZjE5ZjE0YjM5YzEiLCJpZGl0eXBlIn0=
    
    "token_type": "bearer",
    "expires_in": 1799
}
```
Deep Dive: Device API
Deep Dive: Device API

- Query for Device IDs
- Get Device Details for Device IDs
- Perform Automation
"groups": [
  "5d32484152884e5d995e6cb7cee5d0f9"
],
"group_hash": "1bcacf6f886cb615c5164ad9a6ab38f5bce2025f39ff299a5e527d0c809248",
"product_type": "1",
"product_type_desc": "Workstation",
"provision_status": "Provisioned",
"service_pack_major": "1",
"service_pack_minor": "0",
"pointer_size": "8",
"status": "contained",
"system_manufacturer": "VMware, Inc.",
"system_product_name": "VMware Virtual Platform",
"tags": [],
"modified_timestamp": "2020-07-13T20:33:01Z",
"slow_changing_modified_timestamp": "2020-07-13T20:33:01Z",
"meta": {
  "version": "30"
}
Deep Dive: Detection API
Deep Dive: Detection API

Query for Detection IDs

Get Detection Details from Detection IDs

Perform Automation
Deep Dive: Detection API

- Detection example video. Get new detection, mark in progress, examine the details available, mark True Positive in postman. Plug how you could use Real Time Response API while in progress to do things.

- Video recorded demo coming when nice mic arrives in kit
Takeaways

- Python classes with sample scripts in public repo (I’m still working on getting this put on the public CrowdStrike github page)
Thank You

We look forward to your input to help us continue to make Fal.Con better year after year.

Please fill out the survey at the link below and provide your feedback – you will be entered to win $300 on items from the CrowdStrike Swag Store!