CLOUD STRIKE INTERN MAP

**1. Falcon Complete (Managed Detection and Response)**

**Tools:**

* **SIEM Platforms:**
  + Splunk
  + QRadar
* **EDR Tools:**
  + CrowdStrike Falcon (Core Platform)
  + Microsoft Defender for Endpoint
* **Incident Response Tools:**
  + Wireshark (network analysis)
  + FTK Imager (disk imaging)
  + Autopsy (digital forensics)
* **Forensics Tools:**
  + Volatility (memory forensics)
  + X-Ways Forensics (advanced digital forensics)

**Skills:**

* Threat detection and triage
* Incident response and malware forensics
* Knowledge of attack lifecycle (e.g., MITRE ATT&CK)
* Strong scripting (e.g., Python, PowerShell) for automation and reporting
* Familiarity with threat hunting methodologies
* Data correlation and analysis

**2. Falcon Insight (Endpoint Detection & Response)**

**Tools:**

* **EDR Platforms:**
  + CrowdStrike Falcon Insight
  + SentinelOne
  + Carbon Black
* **Log Analysis Tools:**
  + Kibana
  + LogRhythm
  + Graylog
* **Debugging Tools:**
  + GDB (GNU Debugger)
  + OllyDbg (Windows debugger)
* **Endpoint Monitoring:**
  + Sysinternals Suite (e.g., Process Explorer, ProcMon)
  + OSQuery (endpoint visibility)

**Skills:**

* Endpoint data analysis (Windows, Linux, MacOS)
* Malware behavior analysis (static/dynamic analysis)
* Incident handling and response
* Familiarity with cyberattack techniques (e.g., MITRE ATT&CK)
* Advanced debugging and reverse engineering
* Root cause analysis and remediation

**3. Falcon Cloud Workload Protection (Cloud Security)**

**Tools:**

* **Cloud Platforms:**
  + AWS (Amazon Web Services)
  + Microsoft Azure
  + Google Cloud Platform (GCP)
* **Cloud Security Tools:**
  + Prisma Cloud (formerly RedLock)
  + AWS Security Hub
  + Azure Security Center
* **Configuration Management Tools:**
  + Terraform
  + Ansible
* **Container Security Tools:**
  + Aqua Security
  + Docker Bench for Security
  + Kube-bench (Kubernetes security checks)

**Skills:**

* Cloud infrastructure and security (IaaS, PaaS, SaaS)
* Kubernetes and Docker container security
* Cloud workload protection and risk management
* Familiarity with cloud compliance standards (e.g., CIS, NIST)
* Automated security monitoring and configuration management
* Vulnerability management in cloud environments

**Final Notes**

1. **Hands-on Experience:** Try to get hands-on practice with the tools above (especially the CrowdStrike Falcon platform and the others for endpoint or cloud security).
2. **Lab Environments:** Set up test environments using free-tier cloud services or create sandbox setups to simulate attacks and defense strategies.
3. **Keep Practicing Scripting:** Learning Python, PowerShell, and Bash for automation and analysis will set you apart.
4. **Focus on Cloud Security:** Given the growth of cloud technologies, securing cloud workloads and understanding containerization tools will be increasingly valuable.