

Falcon Complete Onboarding

1. Pre-Onboarding Preparation

- **Product Familiarization and FAQ:** Review the products provided by the SLCGP program and review the FAQ for specific information on the program.
- **Assessment of Current Infrastructure:** Evaluate your current IT environment to understand how Falcon Complete will integrate.
- **Identifying Key Stakeholders:** Determine who in your organization will be involved in the onboarding process (e.g., IT staff, security team, management).
- **Download Appendix B:** Categorize your identified assets for management by the Falcon Complete team and establish escalation chains and responsibilities.
- **CrowdStrike University:** Contact the Indiana IOT Local Government Outreach team to get a training seat and learn about product administration, reporting, and benefits.

2. Initial Consultation

- **Kick-off Meeting:** Participate in one of the standing, weekly technical meetings with the CrowdStrike onboarding team.
- **Requirements Gathering:** Discuss your specific security needs, expectations, and any compliance requirements.

3. Account Setup

- **Registration:** Sign up for a CrowdStrike account.
- **License Acquisition:** Licenses will be allocated according to the numbers given via the Consent Letter to the SLCGP committee.

4. Deployment Planning

- **Deployment Strategy:** Develop a plan for deploying the Falcon agent across your network, considering factors like endpoint types, network architecture, and potential disruptions.
- **Timeline Establishment:** Set a realistic timeline for deployment, including milestones and checkpoints.

5. Falcon Agent Installation

- **Download and Install Agent:** Obtain the Falcon agent from the CrowdStrike portal and begin installation on endpoints.
- **Configuration:** Configure the agent settings according to your security policies and requirements.

6. Integration with Existing Systems

- **Firewall Configuration:** Prepare required firewall rules to enable the CrowdStrike Falcon Complete team to support your local entity.
- **API Integrations:** Integrate Falcon Complete with other tools and systems (e.g., SIEM, ticketing systems) using APIs.
- **Data Import:** If necessary, import historical data or logs into the Falcon platform.

7. Training and Knowledge Transfer

- **Staff Training:** Ensure your IT and security teams are trained on use of the Falcon platform.
- **Documentation Review:** Go through the provided documentation to understand the full capabilities of the service.

8. Testing and Validation

- **Pilot Testing:** Conduct a pilot test on a limited number of endpoints to validate the setup.
- **Adjustments:** Make any necessary adjustments based on the pilot test results.

9. Full Deployment

- **Rollout:** Begin the full deployment of the Falcon agent across all endpoints.
- **Monitoring:** Monitor the deployment process for any issues or challenges.

10. Ongoing Management and Review

- **Regular Check-ins:** Schedule regular meetings with the CrowdStrike team for updates and reviews.
- **Performance Monitoring:** Continuously monitor the performance and effectiveness of Falcon Complete.

11. Support and Incident Response

- **Establish Support Protocols:** Understand how to contact CrowdStrike support and the process for incident response.
- **Incident Management:** Collaborate with the Falcon Complete team for any security incidents or alerts.

12. Documentation and Compliance

- **Policies and Procedures:** Modify policies and procedures to support the platform.
- **Compliance Reporting:** Ensure that the deployment aligns with any relevant compliance requirements.
- **Record-Keeping:** Keep detailed records of the deployment process, configurations, and any incidents.