5 Conclusies

Fox-IT heeft onderzoek verricht op basis van de onderzoeksvragen zoals beschreven in hoofdstuk 1.3. Op basis van de bevindingen beantwoordt Fox-IT de onderzoeksvragen als volgt.

1 **Zijn (digitale) sporen aanwezig waaruit aannemelijk wordt dat door Betrokkene de DIVD Code of Conduct is geschonden?**
Fox-IT heeft geen sporen aangetroffen waaruit aannemelijk wordt dat de DIVD Code of Conduct door Betrokkene is geschonden. Wel merkt Fox-IT het volgende op:

Er zijn verdachte activiteiten uitgevoerd onder het gebruikersaccount van Betrokkene. Hieronder verstaat Fox-IT het volgende. Onder het gebruikersaccount van Betrokkene:
- zijn timestomping-acties uitgevoerd;
- wordt de commandogeschiedenis uitgezet;
- is een wachtwoordhash te zien in Metasploit-commandogeschiedenis.

Fox-IT is niet in staat om te beoordelen of deze acties legitiem van aard zijn. Fox-IT adviseert Opdrachtgever om deze bevindingen te bespreken met Betrokkene om meer duidelijkheid te krijgen.

A. **Is door Betrokkene naar kwetsbaarheden in externe systemen gezocht die afwijken van hoe DIVD deze werkzaamheden normaliter zou uitvoeren?**
Fox-IT heeft geen activiteiten geïdentificeerd waarbij onder het gebruikersaccount van Betrokkene naar kwetsbaarheden wordt gezocht op externe systemen die ongewoon zijn voor DIVD.

B. **Zijn door Betrokkene scanresultaten of andere data gekopieerd naar een locatie buiten de DIVD-omgeving en waar dit kan worden gezien als afwijkend van legitieme DIVD-werkzaamheden?**
Fox-IT heeft geen activiteiten geïdentificeerd waarbij onder het gebruikersaccount van Betrokkene data wordt gekopieerd naar een locatie buiten de DIVD-omgeving.

C. **Zijn door Betrokkene activiteiten uitgevoerd op het serversysteem die wijzen op oneigenlijke toegang tot gegevens van DIVD?**
Fox-IT heeft geen activiteiten geïdentificeerd onder het gebruikersaccount van Betrokkene die wijzen op oneigenlijke toegang tot gegevens van DIVD.