

Tjänstebenenämning Säkerhetsspecialist		Avdelning Nätsäkerhetsavdelningen	
Stationeringsort Stockholm	Yrkesområde IT-incidenthantering	BESTA kod	Verksamhetskod

### Arbetsuppgifter

Utveckling, användning och analys av programvara, systemkomponenter och nätverk för enhetens interna/externa behov. Bevaka teknikutvecklingen inom IT-säkerhetsområdet och söka information om säkerhetsproblem i produkter och system. Utredda och publicera rapporter om IT-incidenter och sårbarheter, åt Sitics intressenter och enheten självt. Författa rapporter av teknisk karaktär beträffande incidenter samt IT-säkerhets- och teknikområdet. Medverka i seminarier och konferenser inom teknikområdet. Nätverka med intressenter i syfte att upprätthålla kompetens och delta i spridandet av information och kunskap. Delta i schemalagd 24/7/365 IT-incidenthanteringsfunktion, dvs relevant typ av schemalagd 24-timmars jour. Aktiv kompetensöverföring till medarbetare. Övriga gängse arbetsuppgifter inom linjeorganisationen.

### Arbetskrav

<p><b>A1a. Kunskaper (ange inriktning och nivå)</b>  <b>Grundkrav</b>                  Högskoleutbildning inom IT / telekom / Internet / säkerhet                  - eller motsvarande kunskap inhämtad på relevant sätt                  Bred kompetens inom flera IT-tekniska områden                  Specialistkompetens inom området IT-säkerhet                  Goda kunskaper i Windows, UNIX och BSD-operativ                  Goda kunskaper om TCP/IP och routing                  Programmeringsfärdigheter inom flera moderna och spridda språk                  - t.ex Python, Java, ECMAScript, C, C#, SQL, assembler                  Kunskap kring aktuella sårbarheter och hur de utnyttjas; populära verktyg för analys.                  Svenska och engelska i tal och skrift, flytande; speciellt data-/säkerhetsteknisk nomenklatur                  Svenskt medborgarskap och säkerhetsklassning.</p>	<p><b>A2. Anställningsform</b>                   Tillsvidareanställd <input type="checkbox"/>                   Tidsbegränsad <input type="checkbox"/></p>
<p><b>B1a. Erfarenheter (ange inriktning och omfattning)</b>  <b>Grundkrav</b>                  Arbete med incidenthantering och analys.                  Programmering och/eller Datanätverksarbete på publikt publicerad eller kommersiell basis.                  Deltagande i/vid internationellt erkända intressegrupper/forum, säkerhetskonferenser och/eller utbildningar.</p>	
<p><b>B1b. Meriterande</b>                  Arbete med incidenthantering och analys inom större organisation.                  Arbete med analys av skadlig kod och IT-forensiska undersökningar.                  Ryska och/eller kinesiska i skrift; speciellt slang och data-/säkerhetsteknisk nomenklatur.                  Certifieringar inom IT-säkerhetsområdet (som t.ex, men inte begränsat till, GCIH, CISSP, CISM, CISA osv)                  Djupare kunskaper runt: Programmeringsspråk, systemarkitektur, systemintegration, utvecklingsverktyg, utvecklingsmiljöer, utvecklingsprocess, testmetodik, kodgranskning, felsökning samt verktyg för kodanalys och verifiering</p>	
<p><b>C1. För befattningen viktiga personliga egenskaper</b>                  Förmåga att kommunicera tekniskt komplicerade skeenden på ett enkelt sätt.                  Gott omdöme i säkerhetsfrågor.                  Samarbetsförmåga.                  Analytisk förmåga.                  Stresstålighet.</p>	

### Förhandling med personalorganisationerna

Datum	Personalorg.	Underskrift	Namnförtydligande
	SACO		
	ST		
	(SEKO)		

Arbetskravsbeskrivningen fastställd	
Datum	Underskrift