Förteckning över beviljade projekt – FSTP utlysning 2025

Organisation	Projektnamn	Sökt belopp (kr)	Beskrivning
Actalos AB	Plattform för Risk- och sårbarhetshantering	795000	Projektet vidareutvecklar en plattform för identifiering, prioritering och hantering av IT-säkerhetsrisker i digitala leveranskedjor. Genom automatiserad riskidentifiering, datainsamling och verksamhetsbaserad prioritering får organisationer ett tydligare underlag för beslut om skyddsåtgärder. Lösningen kombinerar hotintelligens, affärskritikalitet och trendanalys för att stärka små och medelstora företags förmåga att planera, prioritera och minska sin digitala sårbarhet.
Bitfront AB	Operationell transparens i digitala leveranskedjor	265000	Projektet utvecklar ett praktiskt ramverk som underlättar för organisationer att arbeta systematiskt med cybersäkerhet i digitala leveranskedjor. Genom att definiera roller, ansvar och informationsflöden för standarderna SBOM, VEX och VDR skapas förutsättningar för enhetlig kravställning, uppföljning och incidenthantering. Ramverket innehåller riktlinjer, innehållskrav och ett mognadsverktyg som hjälper organisationer att analysera sitt nuläge, införa förbättringar och stärka sin motståndskraft.
Capture Energy AB	Säker & Robust Energilagring	1000000	Projektet stärker cybersäkerheten i företagets egna system för energilagring genom att utveckla och införa strukturer för riskhantering, kontinuitetsplanering och ändringsstyrning. Arbetet omfattar kartläggning av sårbarheter, utveckling av rutiner för drifts- och säkerhetskritiska miljöer samt utbildning av nyckelpersonal. Genom att öka den interna förmågan att förebygga, hantera och återställa vid störningar bidrar projektet till en säkrare drift och högre motståndskraft inom energiförsörjningen.
CivSec Nordic AB	CivSec Säker utvecklingsmiljö	559000	Projektet vidareutvecklar en befintlig utvecklingsmiljö baserad på öppen källkod för att stärka säkerhet och resiliens i mjukvaruutveckling. Arbetet omfattar förbättrad funktionalitet för containerteknik, virtualisering och automatiserad hantering av säkerhetsrelaterad information. Genom att möjliggöra en helt lokal och isolerad driftmiljö med stöd för regelverk som CRA och NIS2, bidrar projektet till säkrare utvecklingsprocesser och stärkt leveranskedjesäkerhet.
Clever Collaboration Group	Kontinuitetskompassen för SMF & Kommuner	800000	Projektet utvecklar en digital verktygslåda som stärker organisationers kontinuitetshantering och förmåga att upprätthålla verksamheten vid störningar. Genom att kombinera etablerade standarder som ISO 22301 med praktiska metoder skapas ett tillgängligt stöd för små och medelstora företag samt kommuner. Lösningen omfattar verktyg för självskattning, planering och förbättringsarbete, vilket gör det enklare att införa och upprätthålla systematiskt kontinuitetsarbete utan omfattande externa resurser.
Controla AB	Controla	992500	Projektet utvecklar ett verktyg som identifierar och visualiserar verksamhetskritiska system och beroenden i organisationers digitala miljöer. Genom att kombinera AI-baserad riskklassning med automatiserad kartläggning av integrationer och leverantörstjänster skapas en tydlig överblick över digitala beroendekedjor. Lösningen ger verksamheter ett praktiskt underlag för att prioritera åtgärder och stärka kontinuiteten i sina system och leveranskedjor.
Digitalist Open Cloud AB	Plattform för spårbar & säker molnleverans av OSS	1000000	Projektet syftar till att utveckla en AI-förstärkt plattform för säker och spårbar förvaltning av molnapplikationer baserade på open source. Lösningen automatiserar hela kedjan från kodändring till driftsättning genom härdning, signering och verifiering, med stöd av AI-agenter som ger löpande återkoppling. Plattformen ska möjliggöra en policy-styrd och spårbar process som stärker både ändrings- och kontinuitetshantering genom minskad felrisk och ökad kontroll i leveranskedjan.
DuNovo AB	Substation Eye	168562	Projektet utvecklar ett portabelt, leverantörsoberoende test- och verifieringsverktyg för transformator- och distributionsstationer i elnätets digitala leveranskedjor. Genom att dokumentera kommunikationsflöden, övervaka bussar under arbete och verifiera signaler efter ändringar minskar risken för fel vid idrifttagning och underhåll. Lösningen stödjer de vanligaste kommunikationsprotokollen för nätstationer och möjliggör både simulering och automatiserad detektion av oavsiktliga konfigurationsförändringar. Genom fälttester och vidareutveckling av funktioner för riskbedömning och prestandamätning skapas en robust metod för säker ändringshantering i takt med att Sveriges elnät byggs ut och moderniseras.
EICS AB	Trygg Leverantör – utvecklingsprojekt	600000	Projektet utvecklar en metod för att bedöma cybersäkerhetsförmåga och kontinuitet hos leverantörer i digitala leveranskedjor. Genom att kombinera riskbaserad leverantörsstyrning med nya krav i regelverk som NIS2 och DORA ska projektet ge organisationer verktyg för strukturerad och jämförbar leverantörsutvärdering. Arbetet omfattar framtagning av frågebatteri, processmodell och en konceptuell digital lösning som testas i samarbete med pilotorganisationer. Resultatet förväntas underlätta systematiskt riskarbete och bidra till stärkt motståndskraft i leverantörskedjor.
H5 Förnyelsebyrå AB	Continuum - Säker och robust	1000000	Projektet utvecklar en AI-baserad lösning som hjälper små och medelstora företag att hantera kontinuitet och förändringar i sina digitala leveranskedjor. Genom att kombinera externa datakällor, såsom hotdatabaser, incidentrapporter och leverantörsinformation, med maskininlärningsmodeller kan systemet automatiskt identifiera risker, föreslå åtgärdsstrategier och simulera scenarier för kontinuitetshantering. Lösningen ska vara användarvänlig, molnbaserad och integrera pedagogiska övningar genom lärplattformen plugga.tech, vilket gör det möjligt för företag att förstå, träna och tillämpa kontinuitetsarbete i praktiken.
Healthy WP Sweden	Den mänskliga faktorn i resiliens och säkerhet	500000	Förstudien kartlägger sambandet mellan arbetsmiljö och organisationers förmåga att stärka cyberresiliens, hantera förändringar och upprätthålla kontinuitet i digitala leveranskedjor. Genom att identifiera mänskliga faktorer som stress, bristande kompetens och negativ organisationskultur ska projektet bidra till en djupare förståelse av hur systemfel uppstår och hur dessa kan förebyggas. Arbetet kombinerar kompetens inom arbetsmiljö och cybersäkerhet för att ta fram ett evidensbaserat ramverk som stärker psykologisk trygghet, engagemang och motståndskraft i organisationer. Resultatet ska utgöra grunden för ett mer hållbart och mänskligt förankrat säkerhetsarbete.
Internetworking Stockholm AB	Interaktivt kontinuitetshanteringssystem	999722	Projektet utvecklar en prototyp av ett webbaserat system för kontinuitetshantering som integreras med befintliga verktyg för cybersäkerhetsutvärdering och riskhantering. Lösningen ger användare ett sammanhållet flöde för att identifiera verksamhetskritiska processer, beroenden och risker, samt skapa och förbättra kontinuitets- och redundansplaner. Systemet inkluderar AI-stöd för rådgivning, scenariobaserade övningar och automatiserad riskanalys, med ett intuitivt gränssnitt som gör det användbart för både små och stora aktörer. Projektet omfattar pilotverifiering, återkoppling och drift i svensk molnmiljö enligt gällande standarder, och bidrar till att stärka organisationers resiliens och efterlevnad av cybersäkerhetskrav.

Intil Group AB	Förstärkt leverantörsuppföljning	821000	Projektet utvecklar en modell för kontinuerlig leverantörsövervakning som stärker säkerheten i digitala leveranskedjor. Genom automatiserad scanning identifieras leverantörers exponerade sårbarheter, AI-användning och risker för social manipulation, vilket ligger till grund för anpassade riskbaserade enkäter. Arbetet genomförs i samverkan med kunder inom kritisk infrastruktur och syftar till att effektivisera uppföljning, minska sårbarheter och höja relevansen i leverantörsutvärderingar. Resultatet väntas bidra till förbättrad riskkultur, stärkt NIS2-efterlevnad och lägre kostnader för säkerhetsincidenter.
ITSL Solutions AB	Kapacitetsuppbyggnad för kontinuitet & Incident	610000	Projektet stärker organisationens förmåga inom incident- och kontinuitetshantering genom att införa ett strukturerat och långsiktigt arbetssätt för motståndskraft i digitala tjänster. Arbetet omfattar utveckling av kontinuitetsplaner, förbättrade backup- och redundanslösningar, etablering av tydliga incidentrutiner samt införande av en extern övervakningstjänst. Genom utbildningar, simulerade övningar och omfattande tester stärks verksamhetens beredskap och förmåga att upprätthålla kritiska tjänster vid IT-incidenter. Projektet bidrar därmed till ökad cybersäkerhet både inom organisationen och i den bredare digitala leveranskedjan.
Mirror Partner Utveckling AB	Stärkt cybersäkerhet genom digitalt ledningssystem	473200	Projektet stärker organisationers informationssäkerhet och kontinuitetshantering genom att utveckla en ny modul till ett digitalt ledningssystem integrerat med Microsoft 365. Lösningen förenklar hanteringen av styrande dokument och säkerställer att användare alltid har tillgång till aktuella och kvalitetssäkrade versioner. Funktioner som kvittenshantering, notifieringar och redundans skapar spårbarhet, minskar risken för felaktig tillämpning och möjliggör tillgång även vid driftstörningar. Projektet bidrar därmed till tydligare rutiner för ändringshantering och ett mer robust informationsflöde i digitala leveranskedjor.
NetSymphony AB	ChangeGuard - Säker hantering av Nätförändringar	698150	Projektet utvecklar en molnbaserad lösning för spårbar och säker ändringshantering över interna system och leverantörsgränser. Modulen omfattar riskbedömning, rollback-planer, automatiserad validering och schemaläggning av förändringar, med stöd för regelefterlevnad enligt DORA- och NIS2-direktiven. Lösningen integreras med befintliga verktyg för systemförvaltning och dokumentation, vilket ger förbättrad spårbarhet, snabbare återställning vid driftstörningar och minskad klimatpåverkan. Projektet bidrar till ökad resiliens i nätverksstyrning och en säkrare hantering av förändringar i digitala leveranskedjor.
Nordlo Syd AB	Projekt Robust	1000000	Projektet utvecklar ett ramverk för samordnad ändrings- och kontinuitetshantering inom digitala leveranskedjor. Arbetet genomförs inom ramen för Nordlo Security Governance och omfattar utveckling av verktyg, metodik, utbildning och pilotverksamhet. Syftet är att stärka organisationers förmåga att upprätthålla säker och kontinuerlig drift i enlighet med NIS2- och DORA-krav. Projektet förväntas bidra till mer systematiska arbetssätt för riskhantering och en ökad motståndskraft i digitala ekosystem, i linje med målen i den nationella strategin för cybersäkerhet.
OneMore Secure AB	AI-baserad analysmodul för digitala leveranskedjor	1000000	Projektet utvecklar en AI-baserad analysmodul för att identifiera och visualisera risker, sårbarheter och beroenden i digitala leveranskedjor. Syftet är att möjliggöra en mer systematisk och datadriven bedömning av kontinuitetsrisker hos både offentliga och privata aktörer. Genom att tillämpa statistisk modellering och befintliga data om säkerhetsnivåer kan organisationer få förbättrad överblick över riskmönster och beroenden.
PocketSafe Technology AB	Åtgärdsregister för säkerhetsåtgärder	341850	Projektet utvecklar ett digitalt åtgärdsregister som stödjer organisationer i arbetet med kontinuitetsplanering och riskanalys enligt NIS2 och GDPR. Genom att samla, strukturera och visualisera säkerhetsåtgärder möjliggörs snabbare beslutsfattande vid incidenter och bättre uppföljning över tid. Lösningen bidrar till mer effektiv prioritering av resurser, kortare reaktionstid vid driftstörningar och stärkt motståndskraft i samhällsviktiga leveranskedjor.
Storegate AB	Informationsklassificering av data	533500	Projektet syftar till att utveckla en funktion för informationsklassificering i en befintlig svensk molntjänst för säker lagring och fildelning. Funktionen ska möjliggöra klassificering av filer och mappar som delas med externa aktörer, i enlighet med MSB:s metodstöd och standarden SS-EN ISO/IEC 27000:202 för konfidentialitet, riktighet och tillgänglighet. Lösningen utvecklas i dialog med användare från både privat och offentlig sektor och utformas för att vara flexibel, användarvänlig och tillgänglig oavsett organisationens storlek. Genom projektet stärks förutsättningarna för säker informationshantering och delning i digitala leveranskedjor.
Strado AB	ConflictControl Automatiserad Säkerhetsuppföljning	1000000	Projektet utvecklar funktionen Conflict Control, ett automatiserat verktyg för kontinuerlig säkerhetsuppföljning i digitala leveranskedjor. Funktionen adresserar behov som identifierats i nationella rapporter om cybersäkerhet, där bristande uppföljning av leverantörers säkerhetsnivåer lyfts som en särskilt kritisk sårbarhet. Verktyget bygger på en avancerad regelmotor som i realtid kan identifiera och flagga inkonsekvenser eller konflikter i leverantörsdata. Syftet är att minska risken för mänskliga fel och möjliggöra snabbare åtgärder vid nya hot. Projektet vidareutvecklar Strado AB:s befintliga tekniska plattform och bidrar till mer systematisk, datadriven och proaktiv uppföljning av leverantörers säkerhet. Resultatet förväntas stärka motståndskraften i både offentlig och privat sektor genom effektivare övervakning och uppföljning av säkerhetskrav i digitala leveranskedjor.
T2 Data AB	Bättre riskhantering för digitala leveranskedjor.	400000	Projektet utvecklar SBOM Central, en tjänst för att samla, övervaka och administrera SBOM:ar (Software Bill of Materials) i syfte att stärka cybersäkerheten i digitala leveranskedjor. Tjänsten erbjuder automatiserad övervakning, rapportering av sårbarheter och stöd för riskbedömning. Genom att införa modellen SSVC (Stakeholder-Specific Vulnerability Categorization) skapas mer verksamhetsanpassade prioriteringar och minskad risk för onödiga systemändringar. Genom automatisk datainsamling och en användarvänlig utformning blir riskhanteringen enklare och mer tillgänglig även för organisationer med begränsade resurser.
TECH BROWS AB	AI-assistent för ändrings- & kontinuitetshantering	278000	Projektet utvecklar en webbaserad AI-assistent för små och medelstora företag som stärker ändringshantering och kontinuitet i digitala leveranskedjor. Assistenten genererar rekommendationer, checklistor, riskbedömningar och valideringsplaner samt föreslår lämpliga change-fönster och följer upp påverkan på drift och verksamhet. Inom kontinuitet erbjuder den stöd för BIA, framtagning av planer och scenariobaserade övningar med automatiserad utvärdering. Leverantörsledet omfattas genom mallar, uppföljningsstöd och säker informationsdelning. Lösningen har låg införandetröskel, kan integreras med befintliga verktyg och avslutas med ett öppet kunskapspaket för breddinförande.
Technigo AB	Cybersäkerhet i praktiken	877556	Projektet utvecklar ett digitalt utbildningspaket som gör cybersäkerhet begriplig och praktiskt tillämpbar för utvecklare och ledare. Genom mikrokurser och scenariobaserade övningar tränas deltagarna i säker mjukvaruutveckling, riskbedömning, incidenthantering och NIS2-efterlevnad. Målet är att stärka organisationers säkerhetskultur och förmåga att agera vid cyberincidenter. Projektet bidrar till ökad kompetens i hela leveranskedjan och gör cybersäkerhet mer tillgänglig för icke-specialister.

Urban Hippo AB	Trygg leverantörskedja 360 - TL360	1000000	Projektet utvecklar en ny modul för systematisk säkerhetsuppföljning av leverantörer och ett verktyg för leverantörsutvärdering ur cybersäkerhetsperspektiv. Syftet är att ge organisationer ett skalbart sätt att mäta, jämföra och följa upp leverantörers säkerhetsnivåer. Lösningen omfattar automatiserad utvärdering, kravställning vid upphandling, dashboard för rapportering och stöd för NIS2-efterlevnad. Projektet testas i samarbete med pilotföretag från olika sektorer och ska bidra till att stärka motståndskraften i digitala leveranskedjor genom mer enhetliga och effektiva uppföljningsprocesser.
Whippy AB	Stärkt säkerhet och tillförlitlighet	360000	Projektet stärker säkerhet och driftsäkerhet genom förbättrad databasloggning, övervakning och automatisk backup-verifiering som säkerställer spårbarhet och återställningsförmåga. Dessutom införs säkerhetsmognadstest för kunder och underleverantörer, vilket höjer standarden i hela leveranskedjan. Målet är att skapa ökad trygghet och tillförlitlighet i hantering av personuppgifter samt att möta växande krav på kontinuitet och informationssäkerhet inom offentlig och privat sektor.