Försvarbarhet i cyberdomänen

En litteraturstudie

Henrik Karlzén, Hannes Holm, Martin Karresand

FOI-R--5850--SE

December 2025

FOI

Henrik Karlzén, Hannes Holm, Martin Karresand

Försvarbarhet i cyberdomänen

En litteraturstudie

Titel	Försvarbarhet i cyberdomänen – En litteraturstudie
Title	Defensibility in the Cyber Domain – A Literature Study
Rapportnr/Report no	FOI-R--5850--SE
Månad/Month	December
Utgivningsår/Year	2025
Antal sidor/Pages	43
ISSN	1650-1942
Uppdragsgivare/Client	Försvarsmakten
Forskningsområde	Cyberförsvar och cybersäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E38559
Godkänd av/Approved by	Linda Sjödin
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Bild/Cover: Shutterstock: Volker Rauch

Sammanfattning

Den här rapporten sammanställer forskningslitteratur om skydds- och försvarslösningar som kan påverka förutsättningarna för försvar (försvarbarheten) i cyberdomänen. Rapporten ger en första inblick i det relativt nya begreppet försvarbarhet, genom att bedöma hur forskarnas lösningar förhåller sig till försvarbarhet.

Eftersom det finns extremt stora mängder skydds- och försvarslösningar görs här en begränsning till lösningar som använder terminologin i Mitres D3fend-ramverk. Den allra mesta inkluderade forskningslitteraturen fokuserar på ramverkets taktik benämnd detektion. Den forskningen rör främst nätverkstrafikanalys (77 % av artiklarna), men också användarbeteendeanalys (7 %), filanalys (6 %) med flera.

De allra flesta artiklarna (85 %) presenterar lösningar som bedömds underlätta försvarbarheten. Även de flesta av dessa är fokuserade på detektion. De lösningar som tvärtom försvårar försvarbarheten rör mestadels isolering men också härdning, kompletterat med detektion och vilseledning. Försvarbarhet verkar alltså underlättas av främst detektion, men försvåras av flera olika taktiker. Det talar också för att detektion i huvudsak ökar försvarbarheten, medan arkitektoniska förändringar som härdning och isolering mer troligt minskar försvarbarheten. Artiklarna själva diskuterar inte lösningarnas påverkan på försvarbarheten. Anledningen till de uteblivna diskussionerna tyder på att de som föreslår tekniska lösningar inte brukar beakta försvararens roll. En del av artiklarna nämner dock människan och främst då hur lösningarna kan ge visualisering av loggar.

För att bedöma hur applicerbara forskarnas lösningar är i praktiken gör rapporten också bedömningar av lösningarnas mognad och kvalitet samt vilken typ av indata de använder för utvärdering och framförallt om det är data från verkligheten. De allra flesta lösningar som forskningen producerat är på sin höjd prototyper i labbmiljö (TRL 3–4). Enbart 16 % av alla artiklar bedömdes vara av hög kvalitet. Av de studerade 198 artiklarna bedriver 192 någon typ av datainsamling. Det finns bara 29 artiklar (15 %) som använder publika dataset med data från riktiga system.

Nyckelord: försvarbarhet, cyber, cyberförsvar

Summary

This report compiles research literature on protection and defence solutions that can affect the conditions for defence (defensibility) in the cyber domain. The report provides a first introduction to the relatively new topic of defensibility, by assessing how the researchers' solutions relate to defensibility.

Since there are extremely many solutions, the report restricts its studies to solutions that use the terminology of the MITRE D3FEND framework. The vast majority of included research literature focuses on the framework's tactic of detection. This research mainly concerns network traffic analysis (77% of the papers), but also user behaviour analysis (7%), file analysis (6%) and others.

The vast majority of the papers (85%) present solutions that are assessed to facilitate defensibility. Most of these are also focused on detection. The solutions that instead make defensibility more difficult, mostly concern isolation but also hardening, supplemented by detection and deception. Thus, defensibility seems to be facilitated primarily by detection, but is made more difficult by several different tactics. This also suggests that detection mainly increases defensibility, while architectural changes such as hardening and isolation are more likely to reduce defensibility. The papers themselves do not discuss the solutions' impact on defensibility. The reason for the lack of discussions suggests that those who propose technical solutions do not usually consider the role of the defender. However, some of the papers mention the human, and mainly how the solutions can provide visualisation of logs.

To assess how applicable the researchers' solutions are in practice, the report also makes assessments of the solutions' maturity and quality. Assessments are also made of what type of input data the solutions use, primarily in terms of whether the data is from real systems. The vast majority of solutions produced by the research are at most prototypes in a lab environment (TRL 3–4). Only 16% of all papers were assessed to be of high quality. Of the 198 papers studied, 172 conduct some type of data collection. There are only 29 papers (15%) that use public datasets with data from real systems.

Keywords: defensibility, cyber, cyber defence

Innehållsförteckning

1 Inledning

Inget system har perfekt skydd. Även när mycket tid, pengar och möda har lagts på att skapa starka skydd kommer attraktiva system trots allt behöva utstå intrång från avancerade och ihärdiga angripare.

Avsaknaden av perfekta skydd medför behov av en förmåga att försvara systemet under pågående angrepp. Försvarsförmågan behöver upptäcka, analysera och åtgärda problem som kan åstadkommas av angripare. Försvaret är dock svårt och kräver rätt förutsättningar. Dessa förutsättningar utgörs av systemets försvarbarhet.

Försvarbarheten möjliggör försvar som kompletterar skyddet. Detta kan kontrasteras mot skydd som mer utgör hinder för angripare. I vissa fall kan skydd även bli begränsande för försvarares agerande.

Begreppsligt är försvarbarhet nytt och sällan använt i litteratur från forskare och andra experter. Det är också rimligt att den begränsade begreppsliga användningen speglas av att försvarbarhet även är begränsat använt som tankesätt. Den här rapporten försöker trots allt ge en första inblick i försvarbarhet som begrepp och tankesätt.

För att ge en första inblick i försvarbarhet utgår rapporten från tidigare forskningslitteratur som presenterar tekniska skydds- och försvarslösningar avsedda att öka säkerheten i ett system och därmed påverka försvarbarheten i cyberdomänen. Rapporten bedömer dessa lösningar och hur de förhåller sig till försvarbarhet. För att bedöma om lösningarna är applicerbara i praktiken görs också bedömningar av lösningarnas mognad och kvalitet samt vilken typ av indata de använder och framförallt om det är data från verkligheten.

Eftersom det finns extremt stora mängder skydds- och försvarslösningar görs här en begränsning till lösningar som använder terminologin i Mitres D3fend-ramverk. Liksom försvarbarhet är ramverket ganska nytt men lovande. Det utgör en sorts parallell till Mitres mer kända Att&ck-ramverk.

Att det är just lösningar presenterade i forskningslitteratur som studeras beror på att det ökar möjligheten att få information om lösningarna samt är en rimlig utgångspunkt för ett så omoget område som försvarbarhet. Ett alternativ hade annars varit att studera kommersiella lösningar.

1.1 Syfte

Rapporten är framtagen i ett projekt som syftar till att bistå Försvarsmakten med kunskap på området för att underlätta deras arbete med att försvara system och plattformar mot cyberangrepp. Projektet heter *Försvarbara system och plattformar i cyberdomänen*, och är en del av Försvarsmaktens FoT-beställning 2025–2027.

Rapporten utgör en första omvärldsanalys om försvarbarhet och kommer att vägleda de kommande årens fortsatta arbete i projektet.

1.2 Mål

Rapportens mål är att genom en litteraturstudie av tidigare forskning besvara ett följande forskningsfrågor:

1. Vilka taktiker och tekniker använder forskarnas skydds- och försvarslösningar?
2. Hur påverkas försvarbarheten av forskarnas lösningar?
3. Hur hög mognad och kvalitet är det på forskarnas lösningar?
4. Vilka indata använder forskarnas lösningar?

1.3 Läsanvisning

Rapportförfattarna antar att läsaren är någorlunda bekant med grundläggande begrepp inom cyberdomänen. Det ovanligare begreppet försvarbarhet tas upp i nästa kapitel (2). Metodkapitlet (3) är förmodligen mer intressant för forskare än övriga läsare. Därpå följer ett kapitel (4) som beskriver den kategoriseringsmodell som används för att kategorisera forskningslitteraturen. Där nämns bland annat D3fend-ramverkets ingående taktiker och tekniker. I det följande kapitlet (5) beskrivs resultaten utifrån text och tabeller. Detta kan framstå som stort och svårgenomträngligt. Förhoppningen är dock att varje läsare själv kan välja att fokusera på det som är mest intressant. Dessutom diskuterar det följande kapitlet (6) resultaten, utan tabeller. Rapporten avslutas med ett slutsatskapitel (7) samt referenser (8).

2 Begreppet försvarbarhet

Det finns ingen entydig definition av begreppet försvarbarhet, åtminstone inte för cyberdomänen. En tidigare FOI-rapport (Ljung m.fl., 2010) hade ordet försvarbarhet i titeln men sammanhanget var inte cyberdomänen och någon definition gavs ej. Från den rapportens text framgår att försvarbarhet avsåg möjlighet att försvara, vilket också är en rimlig tolkning av ”försvar” + ”barhet”, språkligt sett. I nuvarande rapport innebär försvarbarhet förutsättningarna att försvara system. Ett mer försvarbart system är därmed enklare att försvara.

I de följande avsnitten beskrivs hur Försvarsmakten använt begreppet försvarbarhet i cyberdomänen. Därtill beskrivs andra källor som tar upp försvarbarhet (eng. defensibility) med koppling till utländskt cyberförsvar. Denna rapports användning av försvarbarhet är avsedd att fungera väl tillsammans med Försvarsmaktens användning av samma begrepp. Andra definitioner har i viss mån mer fokus på möjligheten eller förmågan att försvara, snarare än förutsättningarna för försvaret.

2.1 Försvarsmaktens doktrinansats

Försvarsmaktens (2024b) doktrinansats för cyberförsvar tar kortfattat upp försvarbarhet. Som framgår där är doktrinansatser en sorts vägledningar som fastställs av Försvarsstabens strategienhet. I doktrinansatsen definieras försvarbarhet som ”förutsättningar att genomföra cyberoperationer i ett system”. Därtill beskrivs att försvarbarhet både kan ses som ”en egenskap och ett mått på i vilken utsträckning ett system är utformat för eller på annat sätt möjliggör cyberförsvar”. Dessutom beskrivs att försvarbarhet, tillsammans med cyberlägesbild, är förutsättningsskapande verksamheter för ett effektivt försvar.

2.2 DCO-konceptet

Försvarsmakten (2024a) beskriver ett koncept för defensiva cyberoperationer (DCO). DCO-konceptet är framtaget av första it-försvarsförbandet och gäller där. Dokumentet beskriver bland annat möjligheten att anpassa system i cyberdomänen genom att med skydd ”försvåra för en aktör att utföra oönskade handlingar i systemet” eller genom att med försvarbarhet ”förenkla försvarsåtgärder i och kring systemet”. Dokumentet definierar försvarbarhet som ”förmågan hos ett sociotekniskt system att främja en försvarares aktiviteter under genomförandet av defensiva cyberoperationer”. Dokumentet beskriver också att begreppet innefattar ”egenskaper som påverkar försvararens förmåga att genomföra passiv och aktiv insamling, att filtrera och korrelera data, att modifiera systemet samt att fatta och exekvera beslut.” Som egenskaper exemplifieras det med bland annat synlighet för nätverk och maskiner, aktuella

och riktiga nätverkskartor samt dokumentation om förväntade gränsytor, enheter, konfigurationer, trafikflöden, användarbeteenden och exekverbara filer. Därtill ingår detektion av avvikelser från normalbild och förväntade beteenden, EDR-lösningar, riskbedömningar, mandat, anslutningspunkter för försvararen samt kanaliserande terräng dit angriparen tvingas in.

2.3 Internationella källor

DCO-konceptets definition av försvarbarhet baseras på en masteruppsats av en av DCO-konceptets medförfattare. Masteruppsatsen av Ekstorm (2022) beskriver bland annat att försvarbarhet kan hindras av skydd. Ett exempel på detta är trafikkryptering, vilket försvårar för angripare men också för försvarare. Därtill går Ekstorm igenom engelskspråkiga referenser om försvarbarhet (eng. defensibility) och säger att den mest utförliga definitionen och användningen ges av Ziring (2015). Den referensen säger att ett nätverk som är försvarbart är ”designat och byggt för att underlätta operationer i dess försvar, inklusive övervakning och respons” (dessa källor översätts i denna rapport). Ekstorms (2022) genomgång av litteratur tar även upp bland annat en forskningsartikel om riskanalys (Bier och Gutfraind, 2019), vilken såg försvarbarhet som ”försvararens förmåga att reducera skadan hos systemet”. Därtill nämns några rapporter från Mitre, med referenser i de parenteser som följer här. Bland dessa nämns att försvarbarhet ”gör att cybermotståndare rör sig långsammare, spenderar mer och tar mer risker” (Bodeau m.fl., 2013) och utgör ”förmågan att adressera pågående motståndaraktiviteter” (Bodeau och Graubart, 2013). Ekstorm nämner också hur dåvarande chefen för NSA och US Cybercom beskrev försvarbarhet, vilket bland annat var i termer av försvarbar arkitektur.

En rapport om cyberavskräckning och försvarbarhet skrevs av forskaren Healey (2024), som bland annat var med och grundade det första amerikanska cyberkommandot. Healey beskriver (fritt översatt) försvarbarhet som ett tillstånd där det är ”svårt för typiska hotaktörer att nå sina mål och relativt enkelt för försvarare att nå sina”. Definitionen baseras på en rapport framtagen åt New York stad (Healey m.fl., 2017). Som exempel på vad som ökar försvarbarheten nämner Healey (2024) säkrare programmeringsspråk som nästan helt eliminerar minnessårbarheter, automatisk uppdatering för säkerhetsrelaterade buggrättningar samt arkitektoniska förbättringar. I en presentation beskrev Healey m.fl. (2024) bland annat tänkbara sätt att mäta huruvida försvarbarheten ökat. Några exempel är att mindre hotaktörsgrupperingar inte kan fortsätta verka, att angreppskedjor blir längre och består av svårare och mer tillfälliga angreppstekniker samt att angripare upptäcks, identifieras och tvingas ut ur system snabbare. Dessutom nämns en reducerad ”svans av övergiven, kritisk kod”, vilket förmodligen ska tolkas som en sorts teknisk skuld. Dessa mått kan sättas i perspektiv utifrån mer kapabla hotaktörer. I sin rapport skriver Healey

(2024) att statsaktörers persistens och förmåga gör att förbättringar i försvarbarhet förmodligen inte har någon större påverkan på deras operationer.

3 Metod

Litteratursökningen utgick från den söksträng som beskrivs i det följande avsnittet. I avsnittet därefter beskrivs på vilka grunder vissa sökträffar exkluderades samt hur extraheringen från kvarvarande träffar utfördes. Metoden vägleddes av Kitchenham och Charters (2007).

3.1 Söksträng

Preliminära söksträngar byggdes först upp av termer skapade från rapportens syfte och titel samt konkretiserades i diskussioner i projektgruppen. De preliminära söksträngarna testades i pilotsökningar i Google Scholar och Scopus. Söksträngar som enbart byggdes upp av varianter av ordet försvarbarhet gav inte tillräckligt relevanta träffar. Detta insågs bland annat på grund av att söksträngen inte hittade artiklar som var känt relevanta av rapportförfattarna sedan tidigare. Eftersom försvarbarhet som forskningsområde är i sin linda är det inte heller förvånande att söksträngarna inte hittade tillräckligt med forskning som uttryckligen handlade om försvarbarhet. Det finns dock omfattande forskning kring de flesta aspekter som försvarbarhet innefattar, såsom skydd och hotjakt.

På grund av den bristande relevansen gjordes upprepade försök att hitta en bättre söksträng som visserligen inte använde ordet försvarbarhet men som matchade rapportens syfte. I samband med detta anpassades rapportens forskningsfrågor. Denna typ av anpassning är vanlig, vilket framgår av de lärdomar som rapporteras i en vägledning för litteraturstudier (Kitchenham och Charters, 2007; fritt översatt): ”Räkna med att anpassa frågor under protokollutvecklingen, allt eftersom förståelsen för problemet ökar.” Från och med utförandet av den slutgiltiga sökningen gjordes inga ändringar av forskningsfrågorna. Metoden för sökströngen var alltså satt innan resultaten inhämtades. Som framgår senare gjordes det på motsvarande sätt preliminära analyser med en preliminär extraheringsmall (kategoriseringsmodell) innan en slutgiltig mall sattes.

Som alternativ till en söksträng fokuserad på ordet försvarbarhet användes termer från Mitres ramverk D3fend.[1] D3fend är relativt nytt men har redan hunnit bli inflytelserikt bland både praktiker och forskare. Exempelvis har D3fend använts för att studera nolltillit (Menard m.fl., 2025), modellering av angreppsträd (Husseis m.fl., 2023) samt intrångsdetektion (Kaiser m.fl., 2022; Yousaf och Zhou, 2024). Pilotsökningar med söksträngar baserade på D3fend visade sig vara lovande. Den slutgiltiga söksträngen baserades därför på de övergripande taktikerna i D3fend tillsammans med respektive närmast underliggande tekniker, men gick inte ner på lägre nivå av undertekniker. Varje artikel behövde ta upp en

[1] https://d3fend.mitre.org/

viss taktik och minst en av dess underliggande tekniker. Därtill begränsades sökningen till språket engelska, ämnesområdet datavetenskap samt dokumenttyperna tidskriftsartikel eller konferensbidrag. Dessa typer av begränsningar är vanliga vid litteraturstudier inom cyberdomänen, se exempelvis Kitchenham och Charters (2007). Söksträngen blev som följer, där måsvingetecken används för att få exakta träffar:

TITLE-ABS-KEY (

({Model} AND ({Asset Inventory} OR {Network Mapping} OR {Operational Activity Mapping} OR {System Mapping}))

OR ({Harden} AND ({Agent Authentication} OR {Application Hardening} OR {Credential Hardening} OR {Message Hardening} OR {Platform Hardening} OR {Source Code Hardening}))

OR ({Detect} AND ({File Analysis} OR {Identifier Analysis} OR {Message Analysis} OR {Network Traffic Analysis} OR {Platform Monitoring} OR {Process Analysis} OR {User Behavior Analysis}))

OR ({Isolate} AND ({Access Mediation} OR {Access Policy Administration} OR {Content Filtering} OR {Execution Isolation} OR {Network Isolation}))

OR ({Deceive} AND ({Decoy Environment} OR {Decoy Object}))

OR ({Evict} AND ({Credential Eviction} OR {Object Eviction} OR {Process Eviction}))

OR ({Restore} AND ({Restore Access} OR {Restore Object})))

AND

(LIMIT-TO (SUBJAREA , "COMP")) AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cp")) AND (LIMIT-TO (LANGUAGE , "English")

)

Söksträngen användes 5 september 2025 och gav 738 träffar i Scopus. Begränsningar i tillgänglig projekttid medförde att det inte fanns utrymme att söka i flera databaser. Rapportförfattarnas erfarenhet är att andra databaser visserligen hittar fler, kompletterande, resultat men också att det är mycket överlapp. Metadata för sökträffarna laddades ner från Scopus. Mindre formateringsfel vid exporten justerades. Därefter inleddes den manuella inkluderingen och exkluderingen.

3.2 Exkludering och extrahering

För den manuella filtreringen av sökträffarna utfördes följande exkludering och extrahering. I första hand gjordes exkludering genom bedömning av sammanfattningar (eng. abstract). I andra hand gjordes bedömning av fulltexter (hela artiklar). För båda typerna av bedömningar valdes först en mindre mängd artiklar där flera projektmedlemmar bedömde samma artiklar och diskuterade sina bedömningar. På så vis kalibrerades bedömningsmetoden projektmedlemmarna sinsemellan och samstämmighet nåddes. Totalt innebär detta fyra steg:

1. inledande bedömning av sammanfattning
2. komplett bedömning av sammanfattning
3. inledande bedömning av fulltext
4. komplett bedömning av fulltext.

Dessa fyra steg beskrivs mer nedan. Därefter beskrivs ett femte steg om extrahering av data från inkluderade artiklar.

Första steget var att slumpa fram 30 artiklar. Två av rapportförfattarna läste dessa artiklars sammanfattningar och bedömde huruvida artiklarna borde inkluderas eller exkluderas. Detta följdes av diskussion för att förstå skiljaktigheter och nå enighet i bedömningarna. I 18 av 30 fall exkluderade båda bedömarna, i 10 av 30 fall inkluderade båda bedömarna. I två av de trettio fallen fanns mindre meningsskiljaktigheter, vilka diskuterades. I ena fallet hade den ena bedömaren gjort en aning för exkluderande bedömning och i det andra fallet hade den andra bedömaren gjort en aning för exkluderande bedömning. Tillsammans bestämdes att de fortsatta bedömningarna skulle vara mer inkluderande. Att använda denna typ av slumpade pilottester för bedömningar är normalt för att kunna dela upp arbetet. Kitchenham och Charters (2007) föreslår att samstämmigheten i bedömningarna bedöms med Cohens Kappa och att skiljaktigheter diskuteras fram till enighet. Med siffrorna som angetts i detta stycke blir Kappa 0,86. Cohen ansåg själv att värden över 0,80 är att se som nästan perfekt samstämmighet (McHugh, 2012).

Andra steget var att de två rapportförfattarna bedömde relevansen för de resterande sammanfattningarna. Kvar blev 258 artiklar.

Tredje steget var att inleda extraheringen genom att slumpa fram 13 artiklar vars fulltexter laddades ner och som alla tre rapportförfattare extraherade från enligt en preliminär kategoriseringsmodell. Utifrån detta diskuterades extraheringsmallen och den förfinades. En projektmedlem gjorde senare en kompletterande extrahering för dessa 13 gemensamma artiklar. Övriga 245 artiklar delades upp på de tre projektmedlemmarna, vilket gav 81–82 träffar var. Det slumpade pilottestet för extrahering följer vägledningen i Kitchenham och Charters (2007) (fritt översatt): ”Om flera forskare bedömer olika primärstudier på grund av tids- eller resursbegränsningar som förhindrar att alla primära

artiklar granskas av minst två forskare, är det viktigt att använda någon metod för att kontrollera att forskare extraherar data på ett konsekvent sätt. Till exempel bör vissa artiklar bedömas av alla forskare (t.ex. ett slumpmässigt urval av primärstudier), så att konsistens mellan forskare kan bedömas."

Fjärde steget var att ladda ner de övriga 245 fulltexterna. Exkludering gjordes av 42 artiklar vars fulltexter inte kunde hittas utan särskild betalning. Dessutom exkluderades de artiklar som vid fulltextläsning bedömdes som irrelevanta. Detta gällde 15 artiklar, varefter det återstod 188 artiklar plus de 13 som bedömts gemensamt för en total på 201. Därtill exkluderades två artiklar som haft felaktiga metadata och inte borde träffats av sökströngen samt en artikel som publicerats men sedan dragits tillbaka av förlaget. Efter detta återstod 198 artiklar.

Femte steget var att extrahera data från de 198 artiklarna, enligt den fastställda kategoriseringsmodellen. Denna modell framgår av nästa kapitel. Det mesta av extraheringen berodde i viss mån på rapportförfattarnas subjektiva bedömningar.

4 Kategoriseringsmodell

För att extrahera data användes en kategoriseringsmodell som utgick från forskningsfrågorna och sammanfattas av Tabell 1. Vid extraheringen fanns också en kommentarskolumn där rapportförfattarna kunde notera övrigt av intresse.

Tabell 1. Kategoriseringsmodellen för extrahering av data från artiklarna.

Forskningsfråga	**Kategori**	**Möjliga värden**
Taktiker och tekniker	D3fend-taktik	Enligt D3fend-ramverket. Flera kunde väljas för en artikel.
	D3fend-teknik	Enligt D3fend-ramverket. Flera kunde väljas för en artikel.
Påverkan på försvarbarheten	Påverkan på försvarbarhet (bedömd)	Underlättar, hindrar, eller ingen påverkan.
	Påverkan på försvarbarhet (diskuteras)	Ja, Nej. Samt fritext.
Mognad och kvalitet	Technology Readiness Level (TRL)	Skala 1–9, där 9 är mest mogen.
	Kvalitet	Låg, ok eller hög.
Indata	Indatas öppenhet	Publik eller privat.
	Indatas realism	Syntetisk eller riktig.
	Indatas detaljrikedom	Protokoll eller abstraktion.

För rapportförfattarnas bedömningar av de två första kategorierna användes Mitres ramverk D3fend. En översikt av D3fend återges i Tabell 2. Översättning ges också från originalets engelska till rapportens (egna) svenska termer. Dessa svenska termer används med tanke på att resten av rapporten är på svenska. Det finns inte utrymme att i rapporten definiera alla dessa begrepp och läsaren förväntas vara ytligt bekant med begreppen. Närmare kunskap om begreppen eller D3fend ger inte nödvändigtvis bättre förståelse för litteraturstudien eftersom resonemangen är på en ganska övergripande nivå.

Tabell 2. Taktiker och tekniker i Mitres D3fend-ramverk på originalets engelska och rapportens översättning till svenska.

Tactic	**Taktik**	**Technique**	**Teknik**
Model	Modellera	Asset Inventory	Tillgångsinventering
		Network Mapping	Nätverkskartläggning
		Operational Activity Mapping	Operationell aktivitetskartläggning
		System Mapping	Systemkartläggning
Harden	Härda	Agent Authentication	Agentautentisering
		Application Hardening	Applikationshärdning
		Credential Hardening	Inloggningsuppgiftshärdning
		Message Hardening	Meddelandehärdning
		Platform Hardening	Plattformshärdning
		Source Code Hardening	Källkodshärdning
Detect	Detektera	File Analysis	Filanalys
		Identifier Analysis	Känneteckensanalys
		Message Analysis	Meddelandeanalys
		Network Traffic Analysis	Nätverkstrafikanalys
		Platform Monitoring	Plattformsövervakning
		Process Analysis	Processanalys
		User Behavior Analysis	Användarbeteendeanalys
Isolate	Isolera	Access Mediation	Behörighetskontroll
		Access Policy Administration	Administration av behörighetspolicy
		Content Filtering	Innehållsfiltrering
		Execution Isolation	Exekveringsisolering
		Network Isolation	Nätverksisolering
Deceive	Vilseleda	Decoy Environment	Lockbetesmiljö
		Decoy Object	Lockbetesobjekt
Evict	Avlägsna	Credential Eviction	Avlägsna inloggningsuppgifter
		Object Eviction	Avlägsna objekt
		Process Eviction	Avlägsna process
Restore	Återställa	Restore Access	Åtkomståterställning
		Restore Object	Objektåterställning

Övriga kategorier förklaras enligt följande.

Kategorin *påverkan på försvarbarheten (bedömd)* rör huruvida en förespråkad lösning påverkar möjligheten att försvara systemet, enligt rapportförfattarnas bedömning. Det rör sig om sådant som möjligheten till insyn och att kunna utföra nödvändiga åtgärder.

Kategorin *påverkan på försvarbarheten (diskuteras)* rör huruvida en artikel nämner människans roll i försvaret. Exempelvis kan D3fend täcka in analys av nätverkstrafik men inte vilka delar av analysen som ska utföras av en människa. I praktiken är det få intrångsdetektionssystem som inte kräver återkoppling från en operatör innan det inför en motåtgärd. Detta beror på att falsklarm är vanliga samt att felaktiga beslut kan få stora konsekvenser.

Kategorin *Technology Readiness Level (TRL)* är en bedömning av den tekniska mognadsnivån för de tekniska lösningar som presenteras av artiklarna. Den lägsta nivån är nivå 1 och där finns grundläggande formulerade principer. På nivå 2 når detta upp till koncept. På nivå 3 finns någon form av utvärdering i proof-of-concept. På nivå 4 har tekniken validerats i labbmiljö, medan nivå 5 innebär validering i relevant miljö. På högre nivåer är tekniken inte bara validerad utan även demonstrerad eller faktiskt införd. Den högsta nivån är 9. Ofta saknas uppenbar tydlighet mellan de olika nivåerna och bedömningar av nivån utifrån en forskningsartikel är inte heller alltid enkel. Läsaren bör se enstaka på varandra följande steg som nära ekvivalenta.

Kategorin *kvalitet* är en bedömning av lösningars kvalitet via artiklarnas vetenskapliga höjd. Som låg kvalitet klassificeras artiklar som innehåller stora mängder svårtydda resonemang, klart bristande mängd referenser till relaterat arbete, väldigt enkla lösningar som inte för forskningsfronten framåt, grov språkförbistring och andra allvarliga fel. Nivån däröver är ok och motsvarar den nivå som borde kunna förväntas av forskningsartiklar. Den högsta nivån är hög och innebär särskilt goda resonemang, klart och tydligt presenterat, med ett gediget forskningsbidrag.

De tre övriga kategorierna rör vilken typ av indata som nyttjats för att analysera effekten av en förespråkad teknisk lösning. *Indatas öppenhet* rör huruvida data är publikt tillgängliga som dataset eller privata. *Indatas realism* rör huruvida data från operativa (riktiga) system används eller om data är syntetiska i form av artificiellt genererad data, såsom fiktiva angrepp mot en simulerad miljö. *Indatas detaljrikedom* rör huruvida data är från ett verkligt protokoll (såsom IP-trafik sparad som PCAP) eller om data är en abstraktion (såsom IP-trafik sparad som en kommaseparerad fil med metadata). En samling indata kan även kallas dataset och rapporten benämner då även dess indata med det kortare data.

5 Resultat

Detta kapitel presenterar studiens resultat, indelat efter forskningsfrågorna:

- Avsnitt 5.1 presenterar resultaten för fråga 1: *Vilka taktiker och tekniker använder forskarnas skydds- och försvarslösningar?*
- Avsnitt 5.2 presenterar resultaten för fråga 2: *Hur påverkas försvarbarheten av forskarnas lösningar?*
- Avsnitt 5.3 presenterar resultaten för fråga 3: *Hur hög mognad och kvalitet är det på forskarnas lösningar?*
- Avsnitt 5.4 presenterar resultaten för fråga 4: *Vilka indata använder forskarnas lösningar?*

Resultatet baseras på 198 artiklar. Läsaren bör notera att de mätetal som presenteras i kapitlet ibland är lägre än 198 eftersom en artikel kan sakna information om ett mätetal. Läsaren bör också notera att mätetalen kan vara högre när de rör taktiker eller tekniker i D3fend eftersom samma artikel kan ta upp flera taktiker eller tekniker. Exempelvis tar artikeln Li m.fl. (2024) upp tre D3fend-taktiker (detektera, härda och isolera).

5.1 Taktiker och tekniker

Som framgår av Tabell 3 fokuserar den allra mesta forskningen på D3fend-taktiken detektion. Ingen av artiklarna rör att avlägsna hot. För två artiklar var skydds- och försvarslösningarna ovanliga på ett sätt som gjorde att bedömning av taktik och teknik inte kunde göras. Notera att en artikel kan ta upp flera olika taktiker, varför summan i tabellen är högre än antalet artiklar (198). Taktikernas förekomster i artiklarna räknat i andelar summerar därmed också till mer än 100 % (summan anges ej i tabellen). För de allra flesta artiklar användes en enda taktik och teknik. Tre artiklar använde exakt två taktiker (alltid detektera och isolera), två artiklar hade tre taktiker (detektera, isolera och härda; respektive detektera, isolera och vilseleda). Varje taktik räknas dock max en gång per artikel i denna tabell.

Tabell 3. Observerade taktiker i D3fend.

Taktik	Antal	Andel av artiklarna
Modellera	4	2 %
Härda	3	2 %
Detektera	189	95 %
Isolera	6	3 %
Vilseleda	2	1 %
Avlägsna	0	0 %
Återställa	1	1 %
Summa	*205*	–

Tabell 4 redogör för vilka D3fend-tekniker som artiklarna rör. Som framgår av antalet rader i tabellen bedömdes artiklarna forska om bara 18 av de 248 tekniker som ingår i D3fend. Ingen av dessa 18 tekniker rörde taktiken avlägsna. Som i föregående tabell kunde en artikel använda flera taktiker. I vissa fall innehöll dessutom en artikel flera varianter (tekniker) av samma taktik. Tre artiklar använde två olika tekniker av taktiken detektera. Därtill hade en artikel tre olika tekniker av taktiken detektera.

Tabell 4. Artiklarnas D3fend-tekniker. Vissa artiklar rörde flera tekniker.

Taktik	Teknik	Antal	Andel av artiklarna
Modellera	Tillgångsinventering	1	1 %
	Nätverkskartläggning	3	2 %
Härda	Agentautentisering	1	1 %
	Applikationshärdning	1	1 %
	Plattformshärdning	1	1 %
Detektera	Filanalys	11	6 %
	Känneteckensanalys	1	1 %
	Meddelandeanalys	1	1 %
	Nätverkstrafikanalys	153	77 %
	Plattformsövervakning	6	3 %
	Processanalys	8	4 %
	Användarbeteendeanalys	14	7 %
Isolera	Behörighetskontroll	1	1 %
	Exekveringsisolering	1	1 %
	Nätverksisolering	4	2 %
Vilseleda	Lockbetesmiljö	1	1 %
	Lockbetesobjekt	1	1 %
Återställa	Objektåterställning	1	1 %
Summa		*210*	–

Artiklarna som forskar om att modellera studerar tillgångsinventering (Tripathi m.fl., 2024) samt kartläggning av nätverksanslutna resurser (Vigna m.fl., 2002; Marksteiner m.fl., 2016; Zhang m.fl., 2019).

Artiklarna som forskar om att härda rör agentautentisering i form av biometrisk autentisering (Jawed m.fl., 2018); applikationshärdning (Miao m.fl., 2017) samt plattformshärdning i form av mjukvaruuppdatering (Li m.fl., 2024).

Artiklarna som forskar om att detektera rör främst nätverkstrafikanalys (77 % av artiklarna, exempelvis Lashkari m.fl., 2017; Hu m.fl., 2018; Priyadarshini och Barik, 2022). De artiklar som forskar om annan typ av detektion rör främst filanalys (6 %, exempelvis Cabau m.fl., 2016) eller användarbeteendeanalys (7 %, exempelvis Landauer m.fl., 2018; Fei m.fl., 2025).

Artiklarna som forskar om att isolera handlar om behörighetskontroll (Abdelhay och Refaey, 2024), att blockera mjukvaror från exekvering (Li m.fl., 2024) samt om nätverksisolering (Moraes m.fl., 2016; Rivera m.fl., 2022; Zhang m.fl., 2024; Abhinav m.fl., 2025).

Artiklarna som forskar om att vilseleda hotaktören presenterar en honungsfälla i form av ett helt nätverkssegment (Rivera m.fl., 2022) samt en honungsfälla implementerad som en virtuell maskin (AlQahtan m.fl., 2025).

Artikeln som rör att återställa miljön presenterar ett backupsystem (Ali m.fl., 2025).

5.2 Påverkan på försvarbarheten

I detta avsnitt redovisas rapportens bedömningar av huruvida försvarsmöjligheterna (försvarbarheten) påverkas av lösningarna. Därtill beskrivs huruvida artiklarna själva beskriver påverkan på försvarbarheten.

Tabell 5 presenterar rapportens bedömningar av hur artiklarnas lösningar påverkar försvarbarheten. De allra flesta artiklar (85 %) presenterade lösningar som enbart bedömdes underlätta (öka) försvarbarheten. Tre av artiklarna var antingen litteraturstudier eller teoretiska på ett vis som medförde att bedömningar av försvarbarhet inte var relevant. Detta gällde artiklarna Bishop m.fl., 2014; Vivek och Veeravalli, 2024; Tundis och Cauteruccio, 2025.

Tabell 5. Artiklarnas lösningars påverkan på försvarbarhet.

Påverkan på försvarbarhet	Antal	Andel
Ingen	20	10 %
Försvårar	5	3 %
Underlättar	169	85 %
Båda	1	1 %
Ej tillämpbart	3	2 %
Summa	*198*	*100 %*

Fem artiklar hade lösningar som av rapportförfattarna bedömdes försvåra försvarbarheten. En artikel hade en lösning som bedömdes både underlätta och försvåra. De sex artiklar som hade delvis eller helt försvårande lösningar beskrivs som följer (med artiklarnas taktiker kursiverade):

- Miao m.fl. (2017) föreslår att automatiskt fördela olika operativsystem till olika användare för att *härda*. Tekniskt löses detta genom ett fördelningssystem samt virtuella datorer som finns samlade på en centraliserad plats.
- Moraes m.fl. (2016) presenterar ett system för att *isolera* genom att blockera nätverkstrafik mellan olika virtuella maskiner.
- Abdelhay och Refaey (2024) föreslår en åtkomstmetod mellan olika resurser i ett nätverk för att motverka exempelvis nätverkskartläggning och man-in-the-middle-angrepp. I lösningen ingår förutom att *isolera* behörigheter även att *detektera* nätverkstrafik.
- Zhang m.fl. (2024) presenterar en DDoS-detektor som kan användas för att automatiskt *detektera* och blockera (*isolera*) trafik.
- Rivera m.fl. (2022) beskriver ett verktyg som bedömer om maskiner nyttjas för angrepp. För att *detektera* används funktioner i mjukvarudefinierade nätverk och för att *isolera* så placeras maskinen på ett särskilt nätverkssegment med honungsfällor (för att även *vilseleda*).
- Abhinav m.fl. (2025) presenterar ett system för att *detektera* nätverksintrång och automatiskt blockera angrepp för att *isolera*. Denna lösning var den som även bedömdes underlätta försvarbarheten.

Alla utom en av artiklarna som presenterar försvårande lösningar använder sig alltså av taktiken isolera (och ibland samtidigt andra tekniker). Den återstående artikeln (Miao m.fl., 2017) använder taktiken härda. Detta tyder på att härda och framförallt isolera är tekniker som försvårar försvarbarheten. Detektera däremot verkar underlätta försvarbarheten. Vilka taktiker som påverkar försvarbarhet och hur framgår också av Tabell 6.

Tabell 6. Påverkan på försvarbarhet, per taktik.

	Påverkan på försvarbarhet				
Taktik	**Ingen**	**Försvårar**	**Underlättar**	**Båda**	***Summa***
Modellera	1	0	3	0	*4*
Härda	1	1	1	0	*3*
Detektera	18	3	164	1	*186*
Isolera	1	4	0	1	*6*
Vilseleda	0	1	1	0	*2*
Avlägsna	0	0	0	0	*0*
Återställa	1	0	0	0	*1*
Summa	*22*	*9*	*169*	*2*	*202*

Bland de artiklar som bedömdes underlätta försvarbarheten fanns några som själva också beskriver denna påverkan, och då i form av människans roll. Totalt utgör detta 18 artiklar (9 % av alla artiklar). I majoriteten av artiklarna rör det sig om att grafiskt visualisera larm och systemstatus för en mänsklig operatör. Även gränssnitt i form av kartor och text förekommer, till exempel i Marksteiner m.fl. (2016) och Gingade m.fl. (2023). Alla utom en av de 18 artiklarna rör detektion. En artikel som inriktar sig på en annan taktik är Marksteiner m.fl. (2016). Det rör sig om taktiken modellera med tekniken nätverkskartläggning och då skanning av nätverk för att underlätta till exempel säkerhetsgranskning.

5.3 Mognad och kvalitet

Detta avsnitt beskriver artiklarna utifrån lösningarnas mognadsnivå (bedömd med TRL-skalan) och kvalitet (bedömd utifrån artiklarnas vetenskaplig höjd). Därtill beskrivs dessa två varianter i kombination.

Bedömningen av TRL framgår av Tabell 7 och Tabell 8. Sådan bedömning var tillämplig för alla artiklar utom en (Canali m.fl., 2023), vilken är en studie av hur webbhotell upptäcker cyberangrepp.

Tabell 7. TRL för lösningarna i artiklarna.

Technology Readiness Level (TRL)	Antal	Andel
1	42	21 %
2	98	49 %
3	47	24 %
4	4	2 %
5	6	3 %
Ej tillämpbart	1	1 %
Summa	*198*	*100 %*

Tabell 8. TRL för lösningarna i artiklarna, per taktik.

	Technology Readiness Level (TRL)					
Taktik	**1**	**2**	**3**	**4**	**5**	***Summa***
Modellera	1	1	1	0	1	*4*
Härda	3	0	0	0	0	*3*
Detektera	38	97	44	4	5	*188*
Isolera	2	2	2	0	0	*6*
Vilseleda	0	1	1	0	0	*2*
Avlägsna	0	0	0	0	0	*0*
Återställa	1	0	0	0	0	*1*
Summa	*45*	*101*	*48*	*4*	*6*	*204*

De allra flesta lösningar som forskningsartiklarna beskriver är på sin höjd prototyper i labbmiljö (TRL 3–4). Det finns sex artiklar som utgjorde undantag och som bedömdes ha TRL 5 eftersom de hade testats i relevanta miljöer. Ingen artikel hade en TRL över 5.

Bland artiklarna med TRL 5 är det vanligaste att presentera ett nätverksintrångsdetektionssystem (Cejka m.fl., 2016; AsSadhan m.fl., 2017; Caprolu m.fl., 2021; Piet m.fl., 2023; Gao m.fl., 2024). Ett undantag är Vigna m.fl. (2002) som presenterar ett verktyg som kartlägger nätverksanslutna system.

Artiklarnas kvalitet beskrivs i Tabell 9 och Tabell 10. Denna bedömning kunde göras för alla artiklar, vilket inte var fallet för TRL-bedömningen där en artikel inte kunde bedömas. Därför är summan högre i taktik-tabellen för kvalitet än i den tidigare taktik-tabellen för TRL. Enbart 16 % av alla artiklar bedömdes vara av hög kvalitet. Hela 36 % bedömdes vara av låg kvalitet.

Tabell 9. Artiklarnas kvalitet.

Kvalitet	**Antal**	**Andel**
Låg	71	36 %
Ok	96	48 %
Hög	31	16 %
Summa	*198*	*100 %*

Tabell 10. Artiklarnas kvalitet, per taktik.

	Kvalitet			
Taktik	**Låg**	**Ok**	**Hög**	***Summa***
Modellera	1	2	1	*4*
Härda	1	2	0	*3*
Detektera	70	89	30	*189*
Isolera	3	3	0	*6*
Vilseleda	1	1	0	*2*
Avlägsna	0	0	0	*0*
Återställa	0	1	0	*1*
Summa	*76*	*98*	*31*	*205*

Artiklar med en högre TRL bedömdes i snitt ha en högre kvalitet (se Tabell 11). Som nämnts tidigare kunde TRL-bedömning inte göras för en artikel, varför summan är 197 här. Bland artiklarna med hög kvalitet hade 19 % en TRL över 3. Bland artiklarna som bedömdes vara av låg kvalitet var denna siffra endast 1 %. Detta är ganska naturligt då det i regel krävs högre kvalitet för att uppnå en högre TRL.

Tabell 11. TRL och kvalitet.

	Technology Readiness Level (TRL)					
Kvalitet	**1**	**2**	**3**	**4**	**5**	***Summa***
Låg	19	39	12	0	1	*71*
Ok	21	47	24	1	2	*95*
Hög	2	12	11	3	3	*31*
Summa	*42*	*98*	*47*	*4*	*6*	*197*

Enbart sex artiklar bedömdes ha både en hög kvalitet samt en TRL över 3. Hälften av dessa artiklar hade en TRL på 4 och beskrivs som följer. Caprolu m.fl. (2021) föreslår ett verktyg som kan används för att identifiera skadlig mjukvara för att skapa kryptovalutamynt. Piet m.fl. (2023) presenterar ett verktyg som kan användas för att klassificera nätverkstrafik, såsom FTP eller DNS-över-HTTPS. Gao m.fl. (2024) föreslår ett verktyg som kan detektera skadlig kod baserat på

anomalier i nätverkstrafik observerade genom nätverksteleskop[2]. Andra hälften av artiklarna med hög kvalitet hade en TRL på 5. Dessa artiklar beskrivs som följer. Alasmary m.fl. (2021) presenterar ett verktyg som detekterar skadliga kommandon på Linux-maskiner. Sharma och Swarnkar (2025) föreslår ett verktyg som kan detektera angreppsaktivitet över DNS, såsom exfiltrering av data över DNS. Song m.fl. (2020) föreslår ett intrångsdetektionssystem som detekterar anomalier i nätverkstrafik.

5.4 Indata

I detta avsnitt bedöms vilka indata som forskarna använder för att utvärdera sina lösningar. Av de studerade 198 artiklarna bedriver 172 någon typ av datainsamling medan 26 saknar indata. Som i kategoriseringsmodellen delas indata in utifrån huruvida det finns publik åtkomst till dem, hur realistiska de är (exempelvis verkliga händelser på operativa system insamlad via nätverksövervakningssystem) samt hur stor detaljrikedom de har. För samtliga tre indelningar redovisas en enkel skärning (till exempel antal publik eller privat) och en skärning med D3fend-taktikerna. Det finns också en skärning som har med både åtkomsten och realismen. Denna skärning visar bland annat hur vanligt det är att riktiga data delas mellan forskare.

Tillgång till indata som används i artiklarna beskrivs av Tabell 12 och Tabell 13. I 6 % av artiklarna var det ej möjligt att avgöra om deras nyttjade indata var publikt tillgängligt eller inte.

Tabell 12. Åtkomst till nyttjade indata.

Indatas öppenhet	**Antal**	**Andel**
Okänd	12	6 %
Privat	68	34 %
Publikt	83	42 %
Blandning	9	5 %
Ingen data används	26	13 %
Summa	*198*	*100 %*

[2] System som passivt övervakar stora mängder routad nätverkstrafik, exempelvis https://www.caida.org/projects/network_telescope/

Tabell 13. Åtkomst till nyttjade indata, per taktik.

	Indatas öppenhet				
Taktik	**Okänd**	**Privat**	**Publikt**	**Blandning**	***Summa***
Modellera	0	3	1	0	*4*
Härda	0	2	0	0	*2*
Detektera	12	62	82	9	*165*
Isolera	2	4	0	0	*6*
Vilseleda	0	2	0	0	*2*
Avlägsna	0	0	0	0	*0*
Återställa	0	0	0	0	*0*
Summa	*14*	*73*	*83*	*9*	*179*

En översikt av huruvida artiklarna använder riktig indata (helt realistisk) eller syntetisk data presenteras i Tabell 14 och Tabell 15. Riktig data rör ofta verkliga händelser för operativa system insamlad via nätverksövervakningssystem (till exempel Cejka m.fl., 2016; Demertzis m.fl., 2018; Su m.fl., 2023), alternativt angrepp mot honungsfällor (till exempel Demertzis m.fl., 2018; Ji m.fl., 2020).

Tabell 14. Realism för indata, där riktig är fullt realistisk.

Indatas realism	**Antal**	**Andel**
Okänd	21	11 %
Riktig	44	22 %
Syntetisk	98	49 %
Blandning	9	5 %
Ingen data används	26	13 %
Summa	*198*	*100 %*

Tabell 15. Realism för indata, per taktik.

	Indatas realism				
Taktik	**Okänd**	**Riktig**	**Syntetisk**	**Blandning**	***Summa***
Modellera	0	2	2	0	*4*
Härda	0	1	1	0	*2*
Detektera	21	41	94	9	*165*
Isolera	1	0	4	1	*6*
Vilseleda	0	2	0	0	*2*
Avlägsna	0	0	0	0	*0*
Återställa	0	0	0	0	*0*
Summa	*22*	*46*	*101*	*10*	*179*

Förhållandet mellan syntetiska och riktiga indata är ungefär samma oavsett om indata är publikt tillgängliga eller privata (se Tabell 16). Notera att ingen indata används i 26 artiklar, varför summan är 172 istället för 198.

De vanligaste publika dataseten som används som indata är för nätverksintrångsdetektion. Några av dessa är NSL-KDD[3] (sex artiklar), UNSW-NB15[4] (fem artiklar) och KDD-CUP[5] (fem artiklar). De innehåller syntetiska angrepp och är dessutom föråldrade. NSL-KDD släpptes år 2018, UNSW-NB15 2015 samt KDD-CUP redan 1999.

Det finns 20 artiklar med publika dataset som också använder data från riktiga system samt nio artiklar som på olika sätt blandar sådana varianter av data (publik–blandning och riktig–blandat samt blandat–blandat). Anledningen till att det inte finns fler är förmodligen svårigheten för forskare att erhålla data gällande angrepp mot operativa (riktiga) system, eftersom data kan innefatta känslig information om de angripna målen. Av dataseten med publika och riktiga data finns bland annat nätverksövervakningssystem (till exempel Demertzis m.fl., 2018; Su m.fl., 2023) samt två artiklar som noterade angrepp mot honungsfällor (Demertzis m.fl., 2018; Ji m.fl., 2020).

[3] https://www.kaggle.com/datasets/hassan06/nslkdd

[4] https://research.unsw.edu.au/projects/unsw-nb15-dataset

[5] https://kdd.org/kdd-cup/view/kdd-cup-1999

Tabell 16. Öppenhet och realism för indata.

	Indatas realism				
Indatas öppenhet	**Okänd**	**Riktig**	**Syntetisk**	**Blandning**	***Summa***
Okänd	6	4	1	1	*12*
Privat	4	17	45	2	*68*
Publik	10	20	49	4	*83*
Blandat	1	3	3	2	*9*
Summa	*21*	*44*	*98*	*9*	*172*

Tabell 17 och Tabell 18 beskriver huruvida artiklarnas indata är i verkliga filformat. En vanlig abstraktion är att nyttja förbehandlade särdrag, exempelvis CICIDS2017[6] som innefattar kommaseparerade ark med särdrag.

I de allra flesta fall är indata i form av verkliga filformat. De klart vanligaste formaten är relaterade till avlyssning av nätverkstrafik. Av dessa tillämpar 71 artiklar indata med filformatet PCAP, vilket lagrar nätverkstrafik. Ytterligare 23 artiklar nämner PCAP, men med någon form av abstraktion (detaljrikedomen är inte protokoll). I flera andra fall handlar det förmodligen också ofta om PCAP, även om det inte nämns explicit. Förutom nätverkstrafik utgörs filformaten främst av binärfiler eller varianter av maskinloggar.

Tabell 17. Detaljrikedom för indata.

Indatas detaljrikedom	**Antal**	**Andel**
Okänd	17	9 %
Protokoll	115	58 %
Abstraktion	32	16 %
Blandning	8	4 %
Ingen data används	26	13 %
Summa	*198*	*100 %*

[6] https://www.unb.ca/cic/datasets/ids-2017.html

Tabell 18. Detaljrikedom för indata, per taktik.

	Indatas detaljrikedom				
Taktik	**Okänd**	**Protokoll**	**Abstraktion**	**Båda**	***Summa***
Modellera	0	4	0	0	*4*
Härda	0	1	1	0	*2*
Detektera	17	108	32	8	*165*
Isolera	1	2	3	0	*6*
Vilseleda	0	1	1	0	*2*
Avlägsna	0	0	0	0	*0*
Återställa	0	0	0	0	*0*
Summa	*18*	*116*	*35*	*8*	*179*

6 Diskussion

Detta kapitel diskuterar litteraturstudiens resultat, studiens begränsningar och möjlig framtida forskning.

6.1 Taktiker och tekniker

Den allra mesta forskningen fokuserar på D3fend-ramverkets taktik detektion. Framförallt gäller det nätverkstrafikanalys (77 % av artiklarna). Detta stämmer bra med tidigare forskning (såsom Karlzén och Sommestad, 2023) som funnit att nätverkstrafikanalys är överlägset vanligast som indata för lösningar som hanterar intrång. De övriga sex icke-detektionsrelaterade taktikerna i D3fend, som till exempel modellering och härdning, har betydligt mindre fokus. Detta kan medföra praktiska problem vid tillämpning av de förespråkade lösningarna. Exempelvis kan falsklarmen bli många om det saknas modellering av de system som ska skyddas och de hot som ska undvikas. Därtill blir möjligheterna till reaktion små om forskningen inte sträcker sig längre än detektion. Möjligen ser många forskare det som ointressant att forska om reaktiva åtgärder. Det kan vara ett fåtal åtgärder som är relevanta och som dessutom är tekniskt enkla att utföra. Det bör dock noteras att resultaten i denna rapport är baserade på en sökstäng som använder specifika begrepp, utifrån D3fend. Det är mycket möjligt att andra artiklar studerar likartade lösningar men använder andra begrepp. Kanske är nätverkstrafikanalys ett mer vedertaget begrepp bland forskare än andra begrepp i D3fend.

6.2 Påverkan på försvarbarheten

Den allra mesta forskningen som identifierats bedöms underlätta försvarbarheten, vilket är naturligt med tanke på att artiklarna fokuserar på detektion. Det skulle dock kunna vara möjligt att även detektion försvårar försvarbarheten genom att producera alltför många loggar och larm. En erfaren analytiker vill förmodligen själv välja bland det som detekterats och samlats in, medan en mindre erfaren analytiker möjligen kan bli förvirrad av mängden information.

Bland forskning som presenterar lösningar som i rapporten har bedömts försvåra försvarbarheten är det lilla som förekommer uppdelat på flera taktiker och uppvisar inte alls samma fokus på detektion som forskningen i allmänhet. Artiklar som fokuserar på detektion verkar för det mesta öka försvarbarheten, medan arkitektoniska förändringar som härdning och isolering mer troligt minskar försvarbarheten. Detta stämmer väl med den idé som förekom i bakgrundskapitlet om att förebyggandet av intrång (och annan skada) också kan hindra försvarsmöjligheterna.

Artiklarna själva diskuterar inte lösningars påverkan på försvarbarheten. Men en mindre mängd av artiklarna sätter lösningarna i relation till människan. Att människan för det mesta inte är i loopen är ganska typiskt för forskning i cyberdomänen. Det är ju också naturligt att man bygger bort människan och förenklar försvararens arbete maximalt. Kanske tänker sig forskare dessutom att den mänskliga aspekten ska tas upp i senare, mer mogen, forskning. Det är också möjligt att människofokuserad forskning inte hittats med den valda sökströngen.

6.3 Mognad och kvalitet

De allra flesta lösningar som forskningen producerat är på sin höjd prototyper i labbmiljö (TRL 3–4). Detta är enligt förväntan för en litteraturstudie som sökt ganska brett. Samtidigt vore det intressant att göra motsvarande sökningar om fem år för att se om mer mogen forskning då kommit, exempelvis som fokuserar mer på mänskliga aspekter.

Kvaliteten på lösningarna bedömdes utifrån artiklarnas vetenskapliga höjd. Enbart 16 % av alla artiklar bedömdes vara av hög kvalitet. Hela 36 % bedöms vara av låg kvalitet. Artiklar av högre kvalitet bedöms i snitt även ha en högre TRL. Detta är ganska naturligt då det i regel krävs högre kvalitet för att uppnå en högre TRL. Överlag är dock kvaliteten betydligt lägre än man borde kunna förvänta sig av vetenskapliga artiklar som genomgått kollegial granskning.

6.4 Indata

Bara 29 artiklar (15 %) använder indata från publika dataset med data från riktiga system. Detta är ganska förväntat. Det är typiskt svårt för forskare att få tag i data med angrepp mot riktiga system. Sådana data kan ju innehålla konfidentiell systeminformation. Bland de vanligaste publika dataseten finns typiskt syntetiska angrepp. Dessutom är dessa data föråldrade, varav ett vanligt tillämpat dataset är över 25 år gammalt. Detta är en typisk, om än beklaglig, situation för forskning inom cyberdomänen. En annan aspekt är att indata ibland består av bearbetade abstraktioner snarare än verkliga filformat. Sådana abstraktioner kan visserligen vara bekväma att använda i labb. Men i riktiga system är en stor del av mödan att hantera rådata från olika källor och översätta dessa data till en enhetlig representation. Det är därmed olyckligt att forskare inte arbetar mer med datainsamlingen och speciellt med översättning mellan olika format, vilket enligt våra erfarenheter är en viktig aspekt i praktiken. Utöver bekvämligheten är kanske en anledning till det begränsade intresset av riktiga format att det är mer spännande att detektera angrepp än att översätta mellan format eller att simulera användare och system på ett realistiskt sätt.

6.5 Studiens begränsningar

Det finns flera begränsningar med denna studie. Dessa begränsningar är på en allmän nivå typiska för litteraturstudier. Begränsningarna rör sökströngen, databasvalet samt exkluderingen och extraheringen. Det bör först sägas att litteraturstudien inte varit systematisk på så vis att den heltäckande försökt identifiera all relevant litteratur eller i övrigt helt och hållet följt exempelvis den vägledning för systematiska litteraturstudier som tagits fram av Kitchenham och Charters (2007). I huvudsak är detta ett resultat av att på rimlig tid sammanställa publicerad forskning inom ämnet. Som rapportförfattare anser vi att ämnet försvarbarhet är nytt nog för att det är rimligare att göra denna litteraturstudie mer explorativ än fullt systematisk.

Vad gäller sökströngen var ett grundproblem att begreppet försvarbarhet är nytt. Att bara söka efter det skulle ge alltför få träffar. Alternativa sökströngar ger dock mer subjektivitet, i tolkningen av försvarbarhet, och kan som alltid vid litteraturstudier ge alltför många sökträffar istället. För att nå viss objektivitet och en rimlig mängd sökträffar valde rapportförfattarna till slut att utgå från D3fend-ramverket. Det är ett någorlunda populärt ramverk. Det är dock inte så etablerat att alla forskare använder dess termer. Därtill är dess indelningar förmodligen inte perfekta. Exempelvis kan en viss teknik i ramverket innehålla flera konkreta skydd och försvar medan andra tekniker kan implementeras på färre sätt, vilket gör upplösningen skev. Det är också uppenbart att ramverket inte fullt ut speglar begreppet försvarbarhet.

Vad gäller databasvalet Scopus är det en databas som är både flitigt använd och omfattande. Vissa artiklar kommer förmodligen ändå ha missats. Därtill laddades enbart artiklar ner när rapportförfattarna kunde få tag på artiklarna utan att avlägga särskilda avgifter. Detta kan ha missat viktiga artiklar. Resultaten här är dock på övergripande nivå ungefär de samma som i en liknande tidigare studie (Karlzén och Sommestad, 2023) där även mer praktikernära litteratur inkluderades.

Vad gäller exkluderingen och extraheringen omfattade den en del subjektiva bedömningar av rapportförfattarna. Relevansbedömningarna kan ha exkluderat vissa artiklar av intresse. Att många artiklar som inkluderades sedan bedömdes vara av låg kvalitet talar dock för att själva exkluderingen inte var särskilt hård. Även kvalitetsbedömningarna var i och för sig subjektiva. Därtill gjordes en subjektiv bedömning av artiklarnas valda taktik och teknik snarare än att gå på vad i sökströngen som identifierade artikeln. Resultaten utgår dock i de flesta fall från ganska många artiklar, vilket borde minimera påverkan av enstaka felbedömningar. Det finns inga tecken på att någon enstaka artikel skulle spela en avgörande roll för något resultat, annat än när det framgår av antalet artiklar för ett visst urval.

6.6 Framtida forskning

Försvarbarhet är ett ungt forskningsområde och det finns gott om möjligheter till framtida forskning. En möjlighet är att göra praktiska tester av de mest lovande artiklarnas lösningar, genom exempelvis att slå på och av olika förutsättningar (såsom möjligheten att röra sig fritt utan härdning, eller att ha mer detektionsförmåga) för försvarare i övningar. En annan möjlighet är att ta fram egna koncept och lösningar, exempelvis i kombination med utvärderingarna i förslaget ovan. En tredje möjlighet är att utvidga omvärldsanalysen från att vara litteraturbaserad till att även göra intervjuer med experter på försvar. Sådana intervjuer har utförts i projektet och kommer att redovisas separat. Intervjuerna planeras att framöver kompletteras med enkäter. Denna forskning kan delvis frångå fokus på lösningar och vara mer fokuserad på försvarbarhet som begrepp eller teori.

7 Slutsatser

Detta kapitel beskriver rapportens slutsatser, i form av kortfattade svar på forskningsfrågorna. Slutsatserna är indelade per forskningsfråga.

7.1 Vilka taktiker och tekniker använder forskarnas skydds- och försvarslösningar?

De allra flesta av forskarnas skydds- och försvarslösningar använder D3fend-taktiken detektion. Den forskningen rör främst nätverkstrafikanalys (77 % av artiklarna), men också filanalys (6 %), användarbeteendeanalys (7 %) med flera. Dessa resultat stämmer också bra med tidigare forskning.

Det finns också ett litet antal artiklar om annat än detektion. Det rör modellering av nätverksanslutna resurser, härdning med bland annat biometrisk autentisering, isolering av mjukvaror och nätverk, vilseledning med honungsfällor samt återställning med backuper. Ingen av artiklarna rör att avlägsna hot. Förmodligen hade andra sökströngar kunnat identifiera fler artiklar om dessa taktiker.

7.2 Hur påverkas försvarbarheten av forskarnas lösningar?

De allra flesta artiklar (85 %; 169 artiklar) presenterar skydds- och försvarslösningar som rapporten bedömer underlättar försvarbarheten. Fem artiklar har lösningar som istället bedöms försvåra försvarbarheten. En artikel har en lösning som bedöms både underlätta och försvåra. De lösningar som försvårar försvarbarheten rör mestadels isolering men också härdning, kompletterat med detektion och vilseledning. Försvarbarhet verkar alltså underlättas av främst detektion, men försvåras av flera olika taktiker. Det talar också för att detektion i huvudsak ökar försvarbarheten, medan arkitektoniska förändringar som härdning och isolering mer troligt minskar försvarbarheten.

Huruvida artiklarnas lösningar kan påverka försvarbarheten är baserat på bedömningar i denna rapport. Artiklarna själva diskuterar inte sådan påverkan. Anledningen till de uteblivna diskussionerna tyder på att de som föreslår tekniska lösningar för skydd inte brukar beakta försvararens roll. En del av de artiklar som underlättar försvarbarheten nämner människans roll och främst då hur lösningarna kan ge visualisering av loggar.

7.3 Hur hög mognad och kvalitet är det på forskarnas lösningar?

De allra flesta lösningar som forskningen producerat är på sin höjd prototyper i labbmiljö (TRL 3–4). Bland de sex artiklarna med TRL 5, vilka testats i relevanta miljöer, presenteras det typiskt ett system för detektion av nätverksintrång. Ett enskilt undantag är en artikel som presenterar ett verktyg som kartlägger nätverksanslutna system för att modellera dem.

Kvaliteten på lösningarna bedöms i rapporten utifrån artiklarnas vetenskapliga höjd. Enbart 16 % av alla artiklar bedöms vara av hög kvalitet. Hela 36 % bedöms vara av låg kvalitet. Kvaliteten är därmed betydligt lägre än man borde kunna förvänta sig av vetenskapliga artiklar som genomgått kollegial granskning.

7.4 Vilka indata använder forskarnas lösningar?

Av de studerade 198 artiklarna bedriver 172 någon typ av datainsamling. Det finns bara 29 artiklar (15 %) som använder indata från publika dataset med data från riktiga system. Anledningen till att det inte finns fler är förmodligen svårigheten för forskare att erhålla data gällande angrepp mot operativa (riktiga) system, eftersom data kan innehålla känslig information om de angripna målen. Å andra sidan är detta en begränsning med den identifierade forskningen eftersom det är en viktig utmaning att i riktiga system hantera rådata från olika källor och översätta till en enhetlig representation.

De vanligaste publika dataseten används i forskning om detektion av nätverksintrång. Några av dessa är NSL-KDD (sex artiklar), UNSW-NB15 (fem artiklar) och KDD-CUP (fem artiklar). De innehåller syntetiska angrepp och är dessutom föråldrade. NSL-KDD släpptes år 2018, UNSW-NB15 2015 samt KDD-CUP redan 1999.

De allra flesta indata har verkliga filformat och då främst relaterat till avlyssning av nätverkstrafik. En del av indata är istället abstraktioner. En vanlig abstraktion är att nyttja förbehandlade särdrag, exempelvis i datasetet CICIDS2017 som innefattar kommaseparerade ark med särdrag.

8 Referenser

Rapportens referenser listas i de två kommande avsnitten. Först ges allmänna referenser. Sedan ges de referenser som hänvisas till i texten och som ingår i själva litteraturstudien. Det är inte en komplett lista på de 198 artiklarna.

8.1 Allmänna referenser

Bier, V., & Gutfraind, A. (2019). Risk analysis beyond vulnerability and resilience–characterizing the defensibility of critical systems. European Journal of Operational Research, 276(2), 626-636. https://doi.org/10.1016/j.ejor.2019.01.011

Bodeau, D., Graubart, R., & Heinbockel, W. (2013). Mapping the cyber terrain: Enabling cyber defensibility claims and hypotheses to be stated and evaluated with greater rigor and utility. Mitre. https://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf

Bodeau, D., & Graubart, R. (2013). Characterizing effects on the cyber adversary: A vocabulary for analysis and assessment. Mitre. MTR130432. https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

Försvarsmakten. (2024a). DCO-konceptet. FM2024-9629:1.

Försvarsmakten. (2024b). Doktrinansats Cyberförsvar. Version 1.1. FM2024-21569:2. https://www.forsvarsmakten.se/contentassets/e61862b2384e42878adcb5cc303b5362/doktrinansats-cyberforsvar-1.1-bilaga-1.pdf

Ekstorm, B. L. (2022). Defining, Measuring, and Analyzing Defensibility in the Defensive Cyber Operations Context. Masteruppsats. Naval Postgraduate School. https://apps.dtic.mil/sti/trecms/pdf/AD1213786.pdf

Healey, J., m.fl. (2017). Building a defensible cyberspace: Report of the New York Cyber Task Force. Columbia University, School of International and Public Affairs. https://www.sipa.columbia.edu/sites/default/files/2022-09/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF

Healey, J. (2024). Measuring Policy Effectiveness of Cyber Deterrence and Defensibility. Strategic multilayer assessment. Lawfare. https://nsiteam.com/social/wp-content/uploads/2024/03/2024-03-26_SDF-SMA-Healey_Cyber_Deterrence_final.pdf

Healey, J., Jain, T., Deb, S. (2024). Is Defense Winning?. Measuring is cyberspace is becoming more defensible and resilient. Black Hat USA.

http://i.blackhat.com/BH-US-24/Presentations/US24-Healey-IsDefenseWinning-Wednesday.pdf

Husseis, A., Flores, J. L., Bregar, A., Mazzeo, G., & Coppolino, L. (2023). Enhancing Cybersecurity Proactive Decision-Making Through Attack Tree Analysis and MITRE Framework. In 2023 IEEE International Carnahan Conference on Security Technology (ICCST) (pp. 1-5). IEEE. https://doi.org/10.1109/ICCST59048.2023.10726853

Kaiser, F. K., Andris, L. J., Tennig, T. F., Iser, J. M., Wiens, M., & Schultmann, F. (2022). Cyber threat intelligence enabled automated attack incident response. In 2022 3rd International Conference on Next Generation Computing Applications (NextComp) (pp. 1-6). IEEE. https://doi.org/10.1109/NextComp55567.2022.9932254

Karlzén, H., & Sommestad, T. (2023). Automatic incident response solutions: A review of proposed solutions' input and output. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-9). https://doi.org/10.1145/3600160.3605066

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. EBSE Technical report, ver. 2.3. Keele University, & University of Durham.

Ljung, B., Malmlöf, T., Neretnieks, K. (2010). Baltisk säkerhet: handlingsfrihet och försvarbarhet. FOI-R--3018--SE. Totalförsvarets forskningsinstitut. https://foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--3018--SE

McHugh, M. L. (2012). Interrater reliability: the kappa statistic. Biochemia medica, 22(3), 276-282. https://pmc.ncbi.nlm.nih.gov/articles/PMC3900052/

Menard, P., Reyes, E., & Bateman, R. (2025). Understanding Zero Trust Security Implementations via the MITRE ATT&CK and D3FEND Frameworks: Uncovering Trends Across a Decade of Breaches. https://doi.org/10.24251/HICSS.2025.231

Yousaf, A., & Zhou, J. (2024). From sinking to saving: MITRE ATT &CK and D3FEND frameworks for maritime cybersecurity. International Journal of Information Security, 23(3), 1603-1618. https://doi.org/10.1007/s10207-024-00812-4

Ziring, N. (2015). The future of cyber operations and defense. Journal of Information Warfare, 14(2), 1-6. https://www.proquest.com/scholarly-journals/future-cyber-operations-defense/docview/1967364269/se-2?accountid=28067

8.2 Litteraturstudiens artiklar

Abdelhay, Z., & Refaey, A. (2024). xg security: Zero-trust and moving target defense in decentralized learning environment. In 2024 International Wireless Communications and Mobile Computing (IWCMC) (pp. 1820-1825). IEEE. https://doi.org/10.1109/IWCMC61514.2024.10592368

Abhinav, B. V., Abhirup, M. V. N. S., Adithya, D. S., & Clara Kanmani, A. (2025). Dynamic Threat Detection and Mitigation Using AI-Infused Firewalls. In 2025 13th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE. https://doi.org/10.1109/ISDFS65363.2025.11011964

Alasmary, H., Anwar, A., Abusnaina, A., Alabduljabbar, A., Abuhamad, M., Wang, A., ... & Mohaisen, D. (2021). SHELLCORE: Automating malicious IoT software detection using shell commands representation. IEEE Internet of Things Journal, 9(4), 2485-2496. https://doi.org/10.1109/JIOT.2021.3086398

Ali, S., Wang, J., Leung, V., & Ali, A. (2025). Next-Generation Cybersecurity Solution: A Decentralized Ransomware Recovery Network (DRRN) with Secret Sharing. SN Computer Science, 6(5), 1-22. https://doi.org/10.1007/s42979-025-03858-w

AlQahtan, N., AlOlayan, A., AlAjaji, A., & Almaslukh, A. (2025). HoneyLite: A Lightweight Honeypot Security Solution for SMEs. Sensors, 25(16), 5207. https://doi.org/10.3390/s25165207

AsSadhan, B., Zeb, K., Al-Muhtadi, J., & Alshebeili, S. (2017). Anomaly detection based on LRD behavior analysis of decomposed control and data planes network traffic using SOSS and FARIMA models. IEEE Access, 5, 13501-13519. https://doi.org/10.1109/ACCESS.2017.2689001

Bishop, M., Conboy, H. M., Phan, H., Simidchieva, B. I., Avrunin, G. S., Clarke, L. A., ... & Peisert, S. (2014). Insider threat identification by process analysis. In 2014 IEEE Security and Privacy Workshops (pp. 251-264). IEEE. https://doi.org/10.1109/SPW.2014.40

Cabau, G., Buhu, M., & Oprisa, C. P. (2016). Malware classification based on dynamic behavior. In 2016 18th international symposium on symbolic and numeric algorithms for scientific computing (synasc) (pp. 315-318). IEEE. https://doi.org/10.1109/SYNASC.2016.057

Canali, D., Balzarotti, D., & Francillon, A. (2013). The role of web hosting providers in detecting compromised websites. In Proceedings of the 22nd international conference on World Wide Web (pp. 177-188). https://doi.org/10.1145/2488388.2488405

Caprolu, M., Raponi, S., Oligeri, G., & Di Pietro, R. (2021). Cryptomining makes noise: Detecting cryptojacking via machine learning. Computer Communications, 171, 126-139. https://doi.org/10.1016/j.comcom.2021.02.016

Cejka, T., Bartos, V., Svepes, M., Rosa, Z., & Kubatova, H. (2016). NEMEA: a framework for network traffic analysis. In 2016 12th International Conference on Network and Service Management (CNSM) (pp. 195-201). IEEE. https://doi.org/10.1109/CNSM.2016.7818417

Demertzis, K., Kikiras, P., Tziritas, N., Sanchez, S. L., & Iliadis, L. (2018). The next generation cognitive security operations center: network flow forensics using cybersecurity intelligence. Big data and cognitive computing, 2(4), 35. https://doi.org/10.3390/bdcc2040035

Fei, K., Zhou, J., Zhou, Y., Gu, X., Fan, H., Li, B., ... & Chen, Y. (2025). LaAeb: A comprehensive log-text analysis based approach for insider threat detection. Computers & Security, 148, 104126. https://doi.org/10.1016/j.cose.2024.104126

Gao, M., Mok, R., Carisimo, E., Li, E., Kulkarni, S., & claffy, K. (2024). DarkSim: A similarity-based time-series analytic framework for darknet traffic. In Proceedings of the 2024 ACM on Internet Measurement Conference (pp. 241-258). https://doi.org/10.1145/3646547.3688426

Gingade, S. S., Nagashree, B., & Mohan, R. (2023). Real Time Network Traffic Analysis and Visualization using Wireshark and Google Maps. In 2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 1289-1295). IEEE. https://doi.org/10.1109/ICIMIA60377.2023.10426152

Hu, Y., Yang, A., Li, H., Sun, Y., & Sun, L. (2018). A survey of intrusion detection on industrial control systems. International Journal of Distributed Sensor Networks, 14(8), 1550147718794615. https://doi.org/10.1177/1550147718794615

Jawed, H., Ziad, Z., Khan, M. M., & Asrar, M. (2018). Anomaly detection through keystroke and tap dynamics implemented via machine learning algorithms. Turkish Journal of Electrical Engineering and Computer Sciences, 26(4), 1698-1709. https://doi.org/10.3906/elk-1711-410

Ji, S. Y., Jeong, B. K., Kamhoua, C., Leslie, N., & Jeong, D. H. (2020). Estimating attack risk of network activities in temporal domain: A wavelet transform approach. In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0826-0832). IEEE. https://doi.org/10.1109/UEMCON51285.2020.9298153

Landauer, M., Wurzenberger, M., Skopik, F., Settanni, G., & Filzmoser, P. (2018). Dynamic log file analysis: An unsupervised cluster evolution approach for anomaly detection. computers & security, 79, 94-116. https://doi.org/10.1016/j.cose.2018.08.009

Lashkari, A. H., Gil, G. D., Mamun, M. S. I., & Ghorbani, A. A. (2017). Characterization of tor traffic using time based features. In International

conference on information systems security and privacy (Vol. 2, pp. 253-262). SciTePress. https://doi.org/10.5220/0006105602530262

Li, R., Liu, Z., Guo, M., Gao, W. & Liu, H. (2024). Experimentation and analysis of network anti-mapping security access techniques for illegal scanning. Applied Mathematics and Nonlinear Sciences, 9(1), 2024. https://doi.org/10.2478/amns-2024-1548

Marksteiner, S., Lernbeiß, H., & Jandl-Scherf, B. (2016). An iterative and toolchain-based approach to automate scanning and mapping computer networks. In Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (pp. 37-43). https://doi.org/10.1145/2994475.2994479

Miao, Z., Xinsheng, J., Jianjian, A., & Chao, Y. (2017). Secure assignment strategy of virtual machines based on operating system diversity. In 2017 3rd IEEE International Conference on Computer and Communications (ICCC) (pp. 1411-1415). IEEE. https://doi.org/10.1109/CompComm.2017.8322775

Moraes, H., Vieira, M. A., Cunha, Í., & Guedes, D. (2016). Efficient virtual network isolation in multi-tenant data centers on commodity ethernet switches. In 2016 IFIP Networking Conference (IFIP Networking) and Workshops (pp. 100-108). IEEE. https://doi.org/10.1109/IFIPNetworking.2016.7497251

Piet, J., Nwoji, D., & Paxson, V. (2023). Ggfast: Automating generation of flexible network traffic classifiers. In Proceedings of the ACM SIGCOMM 2023 Conference (pp. 850-866). https://doi.org/10.1145/3603269.3604840

Priyadarshini, R., & Barik, R. K. (2022). A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University-Computer and Information Sciences, 34(3), 825-831. https://doi.org/10.1016/j.jksuci.2019.04.010

Rivera, A. O. G., White, E. M., Acosta, J. C., & Tosh, D. (2022). Enabling device trustworthiness for SDN-enabled Internet-of-Battlefield Things. In 2022 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-7). IEEE. https://doi.org/10.1109/DSC54232.2022.9888903

Sharma, N., & Swarnkar, M. (2025). DLAZE: Detecting DNS Tunnels Using Lightweight and Accurate Method for Zero-Day Exploits. IEEE Transactions on Network and Service Management. https://doi.org/10.1109/TNSM.2025.3541234

Song, W., Beshley, M., Przystupa, K., Beshley, H., Kochan, O., Pryslupskyi, A., ... & Su, J. (2020). A software deep packet inspection system for network traffic analysis and anomaly detection. Sensors, 20(6), 1637. https://doi.org/10.3390/s20061637

Su, H., Qin, S., Wu, Z., Peng, T., Liu, S., & Zhou, Y. (2023). Graph sketch based heavy change detection for temporal network traffic analysis. In 2023 International Conference on Cyber-Enabled Distributed Computing and

Knowledge Discovery (CyberC) (pp. 200-209). IEEE. https://doi.org/10.1109/CyberC58899.2023.00041

Tripathi, V. R., Tangirala, S., Sasanka, D. V., Reddy, D., Dalal, C. S., & Mitra, B. (2024). SINTTRA: Sliding Window Based Temporally Aware Network Traffic Analyzer for IoT Device Fingerprinting. In 2024 IEEE 12th International Conference on Intelligent Systems (IS) (pp. 1-7). IEEE. https://doi.org/10.1109/IS61756.2024.10705258

Tundis, A., & Cauteruccio, F. (2025). On Machine Learning for Digital Forensics Investigation in Network Traffic. In 2025 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT) (pp. 1027-1033). IEEE. https://doi.org/10.1109/DCOSS-IoT65416.2025.00155

Vigna, G., Valeur, F., Zhou, J., & Kemmerer, R. A. (2002). Composable tools for network discovery and security analysis. In 18th Annual Computer Security Applications Conference, 2002. Proceedings. (pp. 14-24). IEEE. https://doi.org/10.1109/CSAC.2002.1176274

Vivek, V., & Veeravalli, B. (2024). A Survey on Machine Learning Approaches for Intrusion Detection in Cloud Computing Environments for Improving Routing Payload Security and Network Privacy. In 2024 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT) (pp. 79-85). IEEE. https://doi.org/10.1109/IAICT62357.2024.10617793

Zhang, E., Tafreshian, A., & Masoud, N. (2019). Parallel computing algorithm for real-time mapping between large-scale networks. In 2019 IEEE Intelligent Transportation Systems Conference (ITSC) (pp. 4087-4092). IEEE. https://doi.org/10.1109/ITSC.2019.8917463

Zhang, G., Wu, M., Zhang, L., Wang, Y., Liu, Y., & Zhu, J. (2024). An End-to-end Online DDoS Mitigation Scheme for Network Forwarding Devices. In 2024 7th World Conference on Computing and Communication Technologies (WCCCT) (pp. 1-5). IEEE. https://doi.org/10.1109/WCCCT60665.2024.10541398

ISSN 1650-1942