Centera email Defence for Microsoft 365

Højere detektion af email baserede trusler i Microsoft 365

Dataark DK V.1.02

Størstedelen af alle cyberangreb og datalækager involverer e-mail, hvilket gør det til den største trussel mod virksomhedens it-sikkerhed.

Email Defence M365 for Microsoft 365 er en effektiv løsning til at beskytte din virksomheds IT-miljø, som detekterer og blokerer e-mailtrusler, derunder Business Email Compromise, CEO-fraud, Office 365 credential phishing og avanceret malware.

Bedre blokering af trusler

email Defence for Microsoft 365 integreres enkelt I virksomhedens Microsoft 365 og blokerer de trusler, som ellers vil være nået frem til de tiltænkte modtagere.

Stop bedrageriforsøg og avancerede trusler fra emails

Machine learning kombineret med datafeeds fra både global og regional cyber threat intelligence er grundlaget for en effektiv analyse og blokering af e-mails igennem i email Defence for Microsoft 365. IT-kriminelle benytter ofte de mest udbredte sikkerhedslag som sandkassetest for at deres kampagner når tiltænkte mål.
Ved både at øge analysegrad, metoder og tilføre regionale efterretninger om målrettede kampagner, øges virksomhedens email sikkerhed væsentligt.

Skab Overblik Over Potentielle Trusler

Centera's Threat dashboard angiver en løbende og generel risikoscore for virksomhedens e-mails. Dette hjælper administratorer med at prioritere evt. alarmer og reagere evt. øgede risici for virksomheden. E-mail-logføring og tilknyttede data vises i realtid. Rapporter, alarmer, operativ status kan tilsendes via SMS eller e-mail.

Enkel Udrulning og Total Dækning

Beskyt jeres brugere uanset om de på kontoret, hjemmearbejdspladsen eller ude ved kunder, løsningen dækker alle typer enheder og netværk hvor skadelige emails kan udgøre en trussel. Centera Email Defence M365 implementeres hurtigt og enkelt via få klik i Microsoft Office365. Herefter kan vi vælge om løsningen skal lære jeres email trafik via en transparent monitorering og rapportering, eller at løsningen skal blokere alle fundene trusler med det samme.

Funktioner

- **Blokering af trusler i Microsoft Office 365** Integreres direkte i jeres Microsoft 365 løsning, hvor emails behandlet som uskadelige af Microsoft, genanalyseres af Centera email Defence M365.
- **Blokér skadelige emails i indbakker** Identificer og blokér skadelige emails der allerede findes i brugernes indbakker
- **Analyse af email med filtre fra regionale efterretninger** om email trusler, som målrettede kampagner fra IT-kriminelle og andre former for målrettede angreb via email.
- **Analyse af email med machine learning** email analyseres i 550 dimensioner for trusler og nye metoder indenfor email angreb, via machine learning. Klassifikationen af en skadelig email kan efterprøves af administrator i alternative sandbox systemer.
- **email Risk & Threat View**, giver løbende status for virksomhedens risikoniveau for deres email, samt en oversigt og forensic adgang til email og trusler der udgør risici.
- **email Flow & Logs View**, giver et enkelt overblik over virksomhedens email trafik, men mulighed for at søge på tværs af email, real-tid, som

Detekterer og Blokerer:

- **Business Email Compromise**
- **CEO Fraud**
- **Phishing**
- **ID & Credential Theft**
- Reconnaissance campaigns
- Malware
- Ransomware
- Extortionware
- Non compliant emails

Skaber Overblik Over Potentielle Trusler

Centera's Threat dashboard angiver en løbende og generel risikoscore for virksomhedens e-mails. Dette hjælper samtidigt administratorer, SOC- og MDR teams med at prioritere eventuelle alarmer og øgede risici for virksomheden.
E-mail-logføring og tilknyttede data vises i realtid. Rapporter, alarmer, operativ status kan tilsendes via SMS eller e-mail.

Analyse af vedhæftninger

Vi benytter en række avancerede mekanismer til afdækning af trusler, som beriges med omfattende threat intelligence til at analysere enhver vedhæftet fil. Vores løsning kan karantænesætte e-mailen, indtil der er opnået en endelig analyse af om den pågældende email kan være skadelig. Alle ikke skadelige e-mails forbliver i brugernes indbakker, imens email med trusler erstattes af en email med oplysning om at den originale email er karantænesat. Samtidigt kan brugeren se indholdet af den karantænesatte email i et sikret miljø.

URL Crawling & Analyse

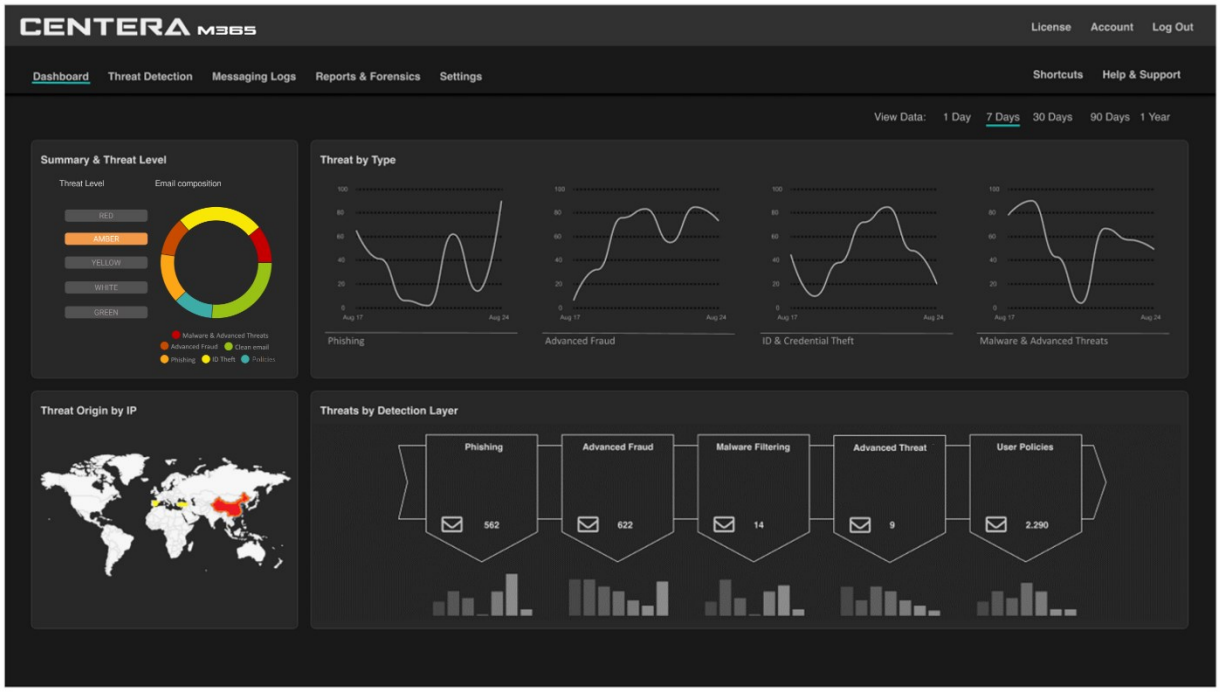
Via machine learning, der løbende tilføres regionaliserede efterretninger om it-trusler, analyseres og opdages trusler i links. E-mails, der indeholder ondsindede links, sættes øjeblikkeligt i karantæne, mens den tilsigtede modtager kan gives mulighed for at se e-mailen i et sikret og uskadeligt format.

Centera Client Aware Threat Detection

Centera Email Defence omfatter en unik kombination af detektions-lag med machine learning og regionaliserede efterretninger om email relaterede trusler.

Hver kundes detektionsprofil tilpasses individuelt for effektivt beskyttelse af virksomhedens e-mail mod trusler, samtidigt med at blokeringer af legitime emails holdes på et minimum.

CYBERSECURITY™
MADE IN EUROPE



Om Centera Security

Centera Security blev grundlagt i København i 2019. Vi er en it-sikkerhedsudvikler med fokus på nordiske virksomheder.
Vores primære mål er at beskytte virksomheder og organisationer mod IT-relaterede trusler gennem bedre designede cybersikkerhedsløsninger.
Centera Security kombinerer gennemprøvet teknologi med machine learning og efterretninger
om målrettede cybertrusler.