AHK German American Chambers of Commerce
Deutsch-Amerikanische Handelskammern

TeleTrusT Pioneers in IT security.
IT Security Association Germany

German-American IT Security Forum

IT Security Association Germany (TeleTrusT) in cooperation with GACC – German American Chamber of Commerce

San Francisco, 2025-04-28

Future of AI-Support for SOC Analysts

DCSO Engineering Security. Together.

Dr. Andreas Rohr, CEO
DCSO Deutsche Cyber-Sicherheitsorganisation
HQed in Berlin, Germany

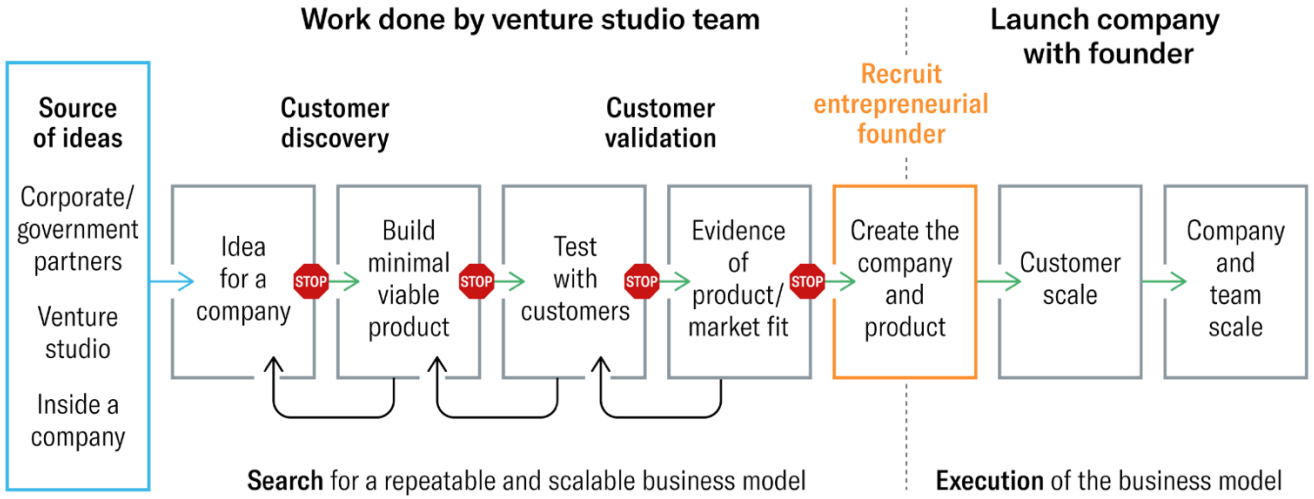
Combine security domain knowledge (DCSO) with AI implementation know how (GenLab)

CONNECT	DEFEND	IMPROVE
Advisory Board	Threat Intelligence	Security Assessments
DCSO Community	Detection and Hunting	Security Consulting
	Incident Response	Security Technology

focus

Collaboration follows a Venture Studio Model

Unlike an accelerator or incubator, a venture studio doesn't fund existing startups. It's a company that creates multiple startups in-house, then finds entrepreneurs who take them over to grow them.



Source: Haward Business Review 2022 (https://hbr.org/data-visuals/2022/12/how-venture-studios-work)

Co-Development	Co-development of joint products for DE, EU, and more
Data Architecture and Real-Environment Testing	DCSO provides access to its architecture know-how for data-collection to facilitate AI model learning. This ensures maximum compatibility in DCSO setups.
Managed Security Service Provider	Affiliates will be referred to DCSO as MSS provider
Channel Partnership	First class channel partnership for co-developed products; early access and market entry in DCSO home market
Revenue and Equity Participation (DCSO IP & DATA)	For cases where DCSO provides IP in co-developments DCSO shall participate with an equity share and through a shared revenue model
Advisory Role on the Cybersecurity Venture Studio	DCSO will hold an advisory role for the cybersecurity initiatives
Data Licensing and Joint Revenue Sharing	Any data licensed or provided by DCSO for use in connection with products of the Venture studio or companies is subject to revenue sharing (based on its value)

DCSO has 10 years experience providing actionable threat intelligence

Virtual TI Expert

A virtual TI expert supports in-house security teams by providing affordable, on-demand access through a chat interface to professional cybersecurity research and threat intelligence, making expert security guidance accessible to organizations of all sizes.

Opportunity: Staff shortage and less experienced analysts can benefit from DCSO knowledge when following up on MDR alerts or when investigating own alerts.

Service: Threat Intelligence – Reporting on Threat Research

Service v1: provide a conversational AI interface to the current & historic (est. 2016) DCSO content to

- allow better situational awareness & risk based decision making
- provide abstracts meeting executive language needs

SOC Analysis Support

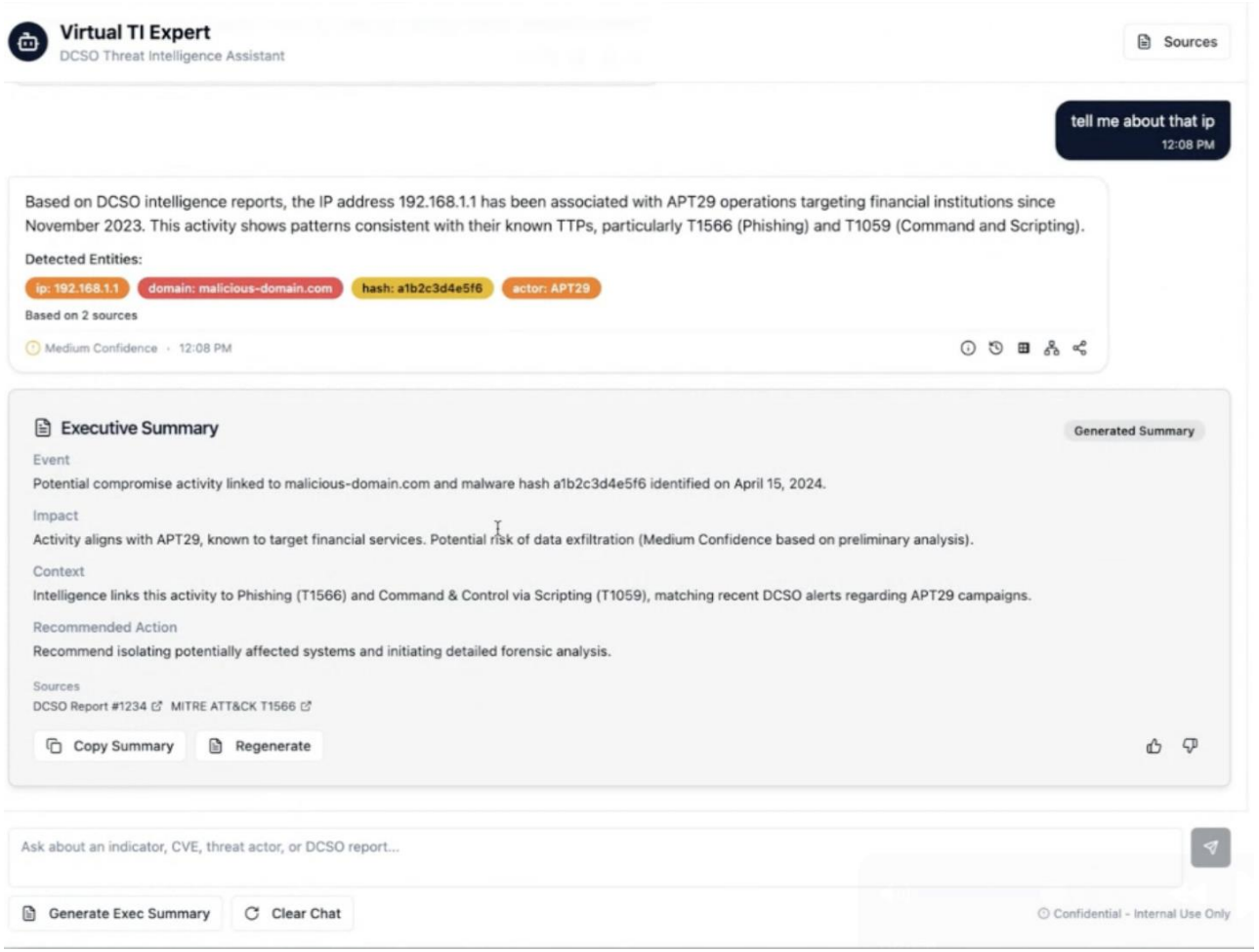
A SOC in a Box product supports a customer's in-house security team by providing affordable analysis of incoming events / alerts. Additionally, there is an on-demand access through a chat interface to professional cybersecurity research and threat intelligence, making expert security guidance accessible to organizations of all sizes.

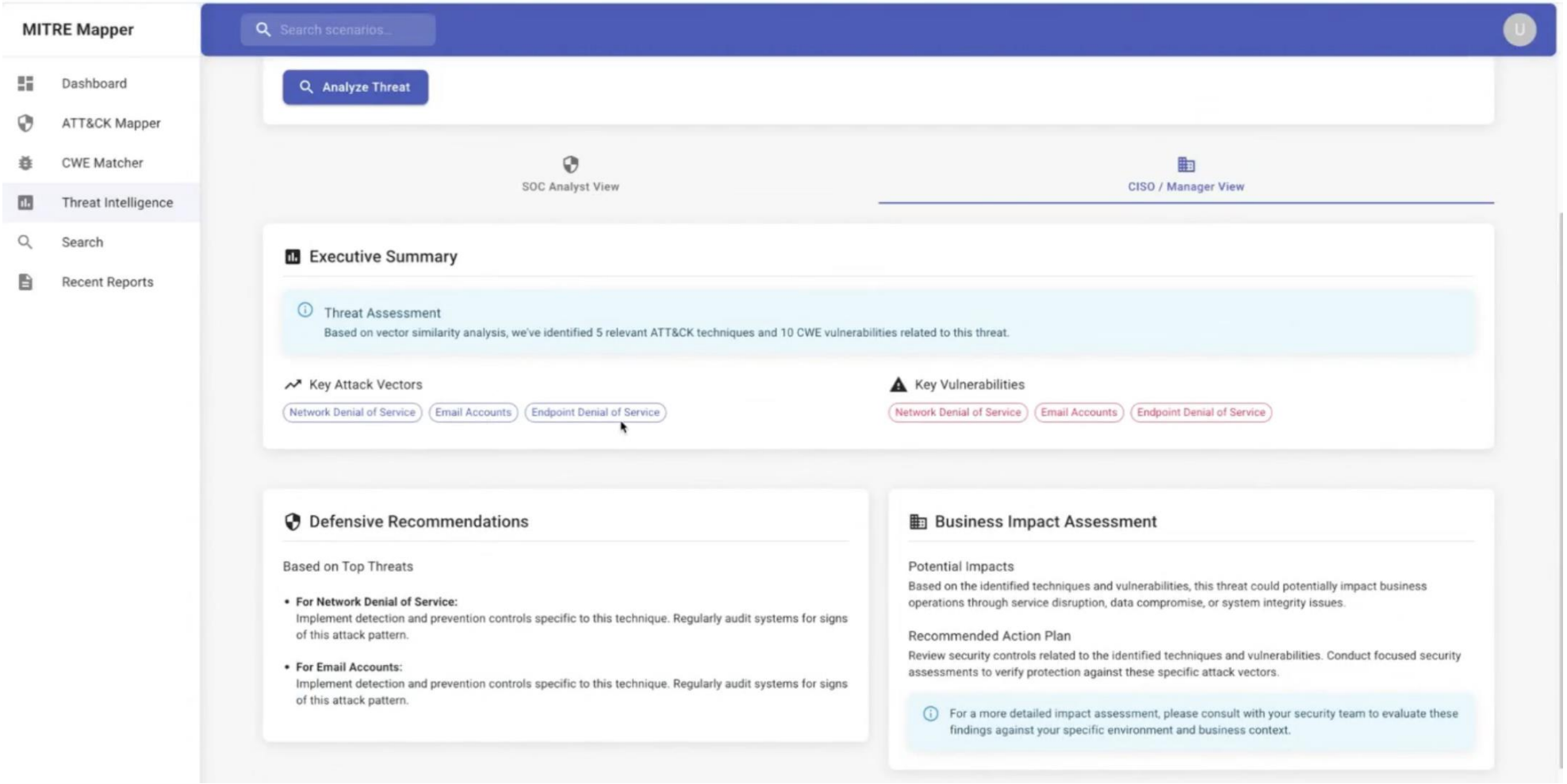
Opportunity: Staff shortage and less experienced analysts can benefit from DCSO knowledge for lower level 24/7 tasks. Customers can concentrate on "last mile of" analysis and remediation

Ideal Customer: This ideal customer is actively seeking cost-effective solutions that provide access to cybersecurity expertise to supplement a limited security team.

First prototype took <2 weeks

- kick-off: March 31, 2024
- business model / ideal customer first
- joint LLM-driven conversations (talk to own ideas / concept; remain memory)
- vibe coding sessions (describe what you want to achieve)
- DCSO internal expert review in May ‘25
- first customer review planned for Jun ‘25
- product launch end of Q3 ‘25





Creating new version is a matter of weeks