Joint Value Proposition

Key benefits

- *Automated refinement* – IdoubleS platform enables automated refinement of sophisticated CTI, such as CrowdStrike's Falcon Adversary Intel Standard and Premium.

- *Automated operationalization* – IdoubleS platform automatically generates Cyber Threat Models, for producing bespoke detection rules of an organization's detection systems, such as CrowdStrike Falcon Next-Gen SIEM or Falcon EDR systems.

- *Support of automated Investigation, Threat Hunting and Incident Response* – IdoubleS platform streamlines automated Investigation, supports proactive Threat Hunting and through integration with a SOAR system like Crowdstrike's Falcon Fusion SOAR, it delivers effective reports that serve as the starting point for Incident Response analysts.

For more information, reach out to:

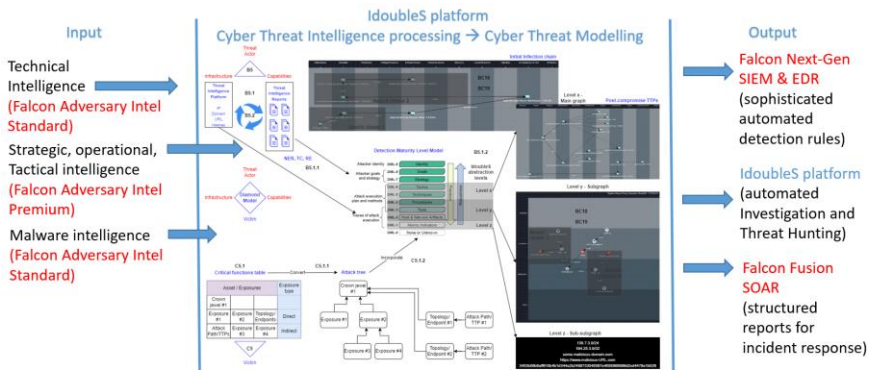
IdoubleS Cybersecurity GmbH
https://www.idoubles.net

Download this one-pager:

The Scaling Crisis in Operationalizing Cyber Threat Intelligence

Sophisticated strategic, operational and tactical Cyber Threat Intelligence (CTI) is provided by Threat Intelligence Providers in natural language prose. For defending against relevant threat actors and scenarios, threat intelligence analysts need to manually review and interpret dozens of these reports. To facilitate the operationalization of this sophisticated CTI, analysts manually refine and structure the unstructured data, transforming it into bespoke Cyber Threat Models. This labour-intensive refinement process is essential but highly inefficient and unable to scale. As a result, producing Cyber Threat Models is costly and considerably slower than the pace of attackers, which leaves organizational assets exposed for a prolonged time. This inefficiency also puts pressure on Threat Intelligence Providers, who risk losing subscription clients due to their limited ability to refine and operationalize sophisticated CTI.

What an organization needs to overcome the non-scalable manual work is an open system that ingests and automatically processes large amounts of sophisticated CTI, such as CrowdStrike's Falcon Adversary Intel Standard and Premium. Deploying the AI-driven IdoubleS platform enables ***automated refinement and operationalization*** of this CTI, rapidly producing precise and bespoke, threat-centric Cyber Threat Models at scale. It saves cost by reducing analyst workloads and closes the exposure window before attackers can exploit it.



IdoubleS platform within the value chain

This diagram illustrates the IdoubleS platform within the value chain. The platform ingests any Threat Intelligence and automatically generates Cyber Threat Models by leveraging AI and natural language processing algorithms. Based on these models, it produces bespoke detection rules for an organization's SIEM and EDR systems, such as CrowdStrike's Falcon Next-Gen SIEM or Falcon EDR. In addition, the platform streamlines automated Investigation and supports proactive Threat Hunting. Through seamless integration with a SOAR systems like CrowdStrike's Falcon Fusion SOAR, the platform delivers structured reports that serve as the starting point for Incident Response analysts, enabling them to initiate and prioritize their investigations more effectively.

IdoubleS platform summary

1. *Defence Preparation:* IdoubleS platform is an open system that mitigates risk by providing recommendations and actions for proactively reducing exposures from the attack surface. It enables users to ingest any OSINT or commercial CTI provided in natural language to generate automated attack graphs that holistically represent attacker capabilities

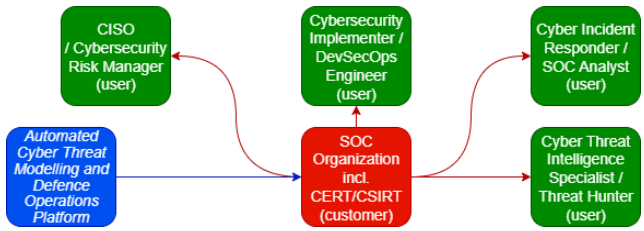
2. *Threat Detection*: IdoubleS builds automated CTMs to derive effective SIEM and EDR detection rules, which reduce alert fatigue and deployment time in a SOC.

3. *Incident Investigation and Threat Hunting*: Bespoke CTMs support effective Investigations and Threat Hunting by providing attack graphs and enabling automated testing of predefined hypotheses, giving clues to uncover potential security threats.

4. *Incident Response:* Enables the cross-correlation of attacker events and determine cohesive chains of intrusion activity to identify known and unknown threats, delivered in the form of a structured report that provides clear insights for Cyber Incident Responders.

IdoubleS platform overview

IdoubleS is an *Automated Cyber Threat Modelling and Defence Operations* platform that supports human intelligence by utilising AI, Natural Language Processing and automation to process large quantities of CTI data in natural language, thereby producing Cyber Threat Models (CTM), which are represented as attack graphs. The platform offers a holistic view by modelling the techniques of threat actors – *the threat-centric aspect* – and aligning these with the exposures of an organisation's attack surface – *the system- and asset-centric aspect*. These combined threat models are presented to the users shown in the diagram above, with the objective to facilitate *Defence Preparation*, *Threat Detection*, *Intrusion Investigation, Threat Hunting* and *Incident Response*.



IdoubleS users

Defence Preparation – IdoubleS platform mitigates risk by aligning attacker capabilities with an organization's specific attack surface. Through automated ingestion of OSINT or commercial CTI, it builds tailored CTMs that represent complete threat scenarios. These models reveal how relevant actors might target an organization's critical assets and provide actionable recommendations, enabling organizations to proactively address exposures before they are exploited.

Threat Detection – IdoubleS platform builds bespoke CTMs to derive effective SIEM or EDR detection rules for any vendor platform. These rules are pushed automatically to the SIEM or EDR for real-time monitoring, helping to detect and mitigate security incidents. This approach reduces noisy false-positive alerts. Due to leveraging automation, it further reduces the operationalization time and cost of deploying the detection rules.

Incident Investigation and Threat Hunting – IdoubleS platform implements automated and structured analysis methodologies for hypotheses formulation and testing, enabling SOC Analysts and Threat Hunters to streamline their investigative processes. Hypotheses are tested against various 3rd party systems that store security telemetry data in response to real-time SIEM or EDR alerts.

Incident Response –IdoubleS platform enables Cyber Incident Responders to rapidly scope and analyse security events by uncovering intrusion chains. It identifies the cause, effect and impact of incidents while supporting attacker attribution and the discovery of hidden threats. Findings are delivered as structured reports that give incident response analysts a clear starting point, helping them initiate and prioritize investigations with greater speed and precision.