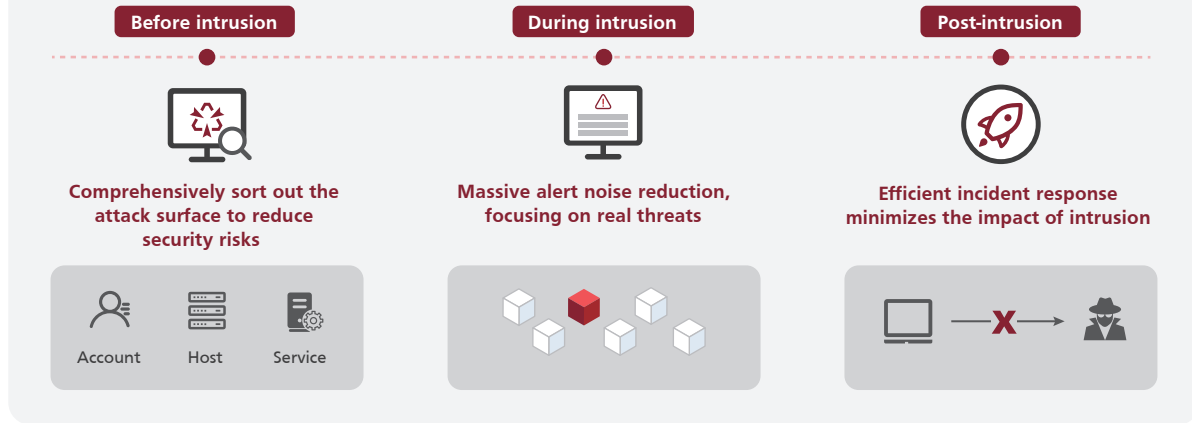# THREAT DETECTION PLATFORM-TDP®

Insight into traffic | TI Inside | Focus on threat | All-in-one-solution

Threat Detection Platform (TDP) is a network detection and response platform with TI inside which can automatically detect, analyze, de-noise and response to the most complex threats. Delivering an all-in-one network security solution to SecOps team.

Before intrusion	During intrusion	Post-intrusion
Comprehensively sort out the attack surface to reduce security risks	**Massive alert noise reduction, focusing on real threats**	**Efficient incident response minimizes the impact of intrusion**

Account   Host   Service

Core Capabilities

COMPREHENSIVE DISCOVERY
"You can't protect what you cannot see."

- Continuously discovering and profiling all assets and services
- Attack surface reduction
- Customizable asset risk behaviour

ACCURATE DETECTION
"When 1% of real alerts are flooded with 99% false positives, it's meaningless to monitor alerts."

- For known threats
- For unknown threats
- Massive alert noise reduction

MULTIDIMENSIONAL ANALYSIS
"In the confrontation with the APT group, the enemy is secretive, but you are trying to see clues from the massive logs?"

- Attack incident analysis
- Attack path analysis
- Attacker profiling

AUTOMATIC RESPONSE
"The attacker's tools are increasingly automated, while the defender is still doing it... manually?"

- Automate pinpoint malicious process
- Built-in TCP reset blocking
- Integrated with firewall

Product Advantages

Accurate Detection
- Threat detection of highly credible intelligence support
- In-depth tracking of hundreds of APT groups
- Precise detection of targeted attack
- Alert false positive rate < 0.03%, 0 day detection rate > 81%

Combat-Oriented
- Risk discovery from the attacker's perspective
- Intelligent aggregation of attackers to completely restore the attack process
- Discover unknown threats with the cloud sandbox

Automatic Response
- Automatic TCP reset blocking, the effectiveness of up to 99%
- Compatible with dozens of brands of firewall
- Automatic endpoint response with TDP agent