

Threat Intelligence Sales Scenarios

Decision makers: SOC Manager

PROBLEM

Difficulties communicating with non-technical executives around risks and threats to the business



BENEFITS

- A team of analysts speaking dozens of languages
- Information on attacks from both surface web and the dark web
- Insights into non-public investigations
- Clarity on the risks associated with an organization's digital footprint
- Proactive protection against the most damaging threats



SERVICES



Kaspersky
Financial Threat
Intelligence
Reporting

Strategic

Tactical

- Exclusive insights into industry-specific threats
- TTPs
- Early warnings
- IoCs and Yara rules



Kaspersky
APT Intelligence
Reporting

Strategic

Tactical

- Insight into non-public APTs
- Detailed supporting technical data access
- Continuous APT campaign monitoring
- Early warnings
- Addressing technical and non-technical audiences
- Retrospective analysis
- Threat actor profiles
- Mapping to MITRE ATT&CK



Kaspersky
Digital Footprint
Intelligence

Strategic

Tactical

- Perimeter inventory and vulnerabilities
- Tailored vulnerability and exploit analysis
- Malicious campaigns by region, industry or customer
- Data leakages
- Threats from the Dark Net

Threat Intelligence Sales Scenarios

Decision makers: SOC Manager

PROBLEM

Cost pressures to increase the effectiveness of SIEM and other security controls by automating initial alert triage and enhancing machine-based prioritization with global insights into cyberthreats



PROBLEM

Decreasing mean time to respond by effective incident scoping and providing IT teams with timely and necessary information



SERVICES



Kaspersky
Threat Data
Feeds



Kaspersky
CyberTrace

Technical

- Broad coverage
- Rich context
- Rapid matching
- Situational awareness

SERVICES



Kaspersky
Cloud
Sandbox



Kaspersky
Threat
Lookup

Operational

- Investigation
- Links and analysis
- Investigation
- Links and analysis
- Browser plugin
- WHOIS tracking

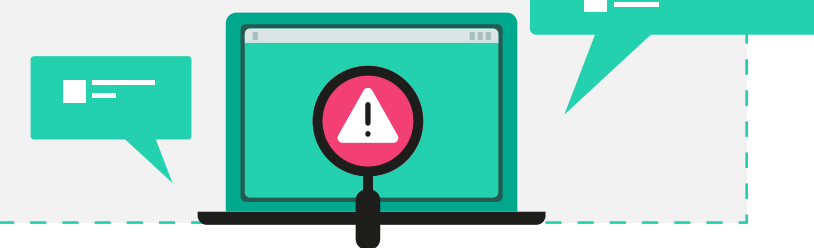
BENEFITS

- Reinforcing network security solutions such as SIEM, with continuously updated information about threats
- Increasing speed and effectiveness of analysis by determining whether each event requires immediate response or additional examination
- Preventing analyst burnout by providing meaningful context to eliminate false positives so analysts can focus on significant alerts alone



BENEFITS

- Meaningful information about threats and their various relationships to boost incident investigation and response

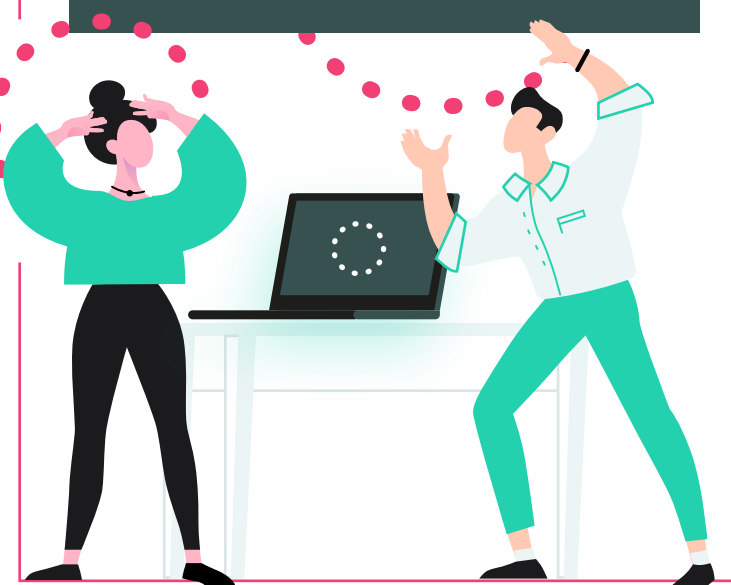


Threat Intelligence Sales Scenarios

Decision makers: SOC Manager

PROBLEM






Accelerating human analysis and improving resource allocation decisions



BENEFITS

- A team of analysts speaking dozens of languages
- Information on attacks from both surface web and the dark web
- Insights into non-public investigations
- Proactive protection against the most damaging threats
- Meaningful information about threats and their various relationships to boost incident investigation and response

SERVICES

|  Kaspersky Threat Lookup Operational |  Kaspersky Cloud Sandbox Operational |  Kaspersky APT Intelligence Reporting Tactical Strategic |  Kaspersky Financial Threat Intelligence Reporting Tactical Strategic |  Kaspersky Digital Footprint Intelligence Tactical Strategic |
|---|---|---|--|---|
| <ul style="list-style-type: none"> ● Investigation ● Links and analysis ● Browser plugin ● WHOIS tracking | <ul style="list-style-type: none"> ● Investigation ● Links and analysis | <ul style="list-style-type: none"> ● Insight into non-public APTs ● Detailed supporting technical data access ● Continuous APT campaign monitoring ● Early warnings ● Addressing technical and non-technical audiences ● Retrospective analysis ● Threat actor profiles ● Mapping to MITRE ATT&CK | <ul style="list-style-type: none"> ● Exclusive insights into industry-specific threats ● TTPs ● Early warnings ● IoCs and Yara rules | <ul style="list-style-type: none"> ● Perimeter inventory and vulnerabilities ● Tailored vulnerability and exploit analysis ● Malicious campaigns by region, industry or customer ● Data leakages ● Threats from the Dark Net |

