Kaspersky Industrial Cybersecurity Conference 2021

Kaspersky OSMP– XDR платформа для выявления и реагирования на инциденты любого уровня сложности.

Антон Иванов, CTO

TEAM

Kaspersky RnD is …

Most Tested. Most Awarded Products and Services

B2C Development

B2B Development

Best Software Engineering Practices

Core Technologies

Internal Development Infrastructure

Cloud Infra Development (KSN)

20+ Years' Experience is embodied in a piece of art of engineering

Threat Processing Infrastructure

Top Notch Experts

Best Expertise and Outstanding Research Capabilities

Threat Research

Global Research and Analysis Team

Security Services

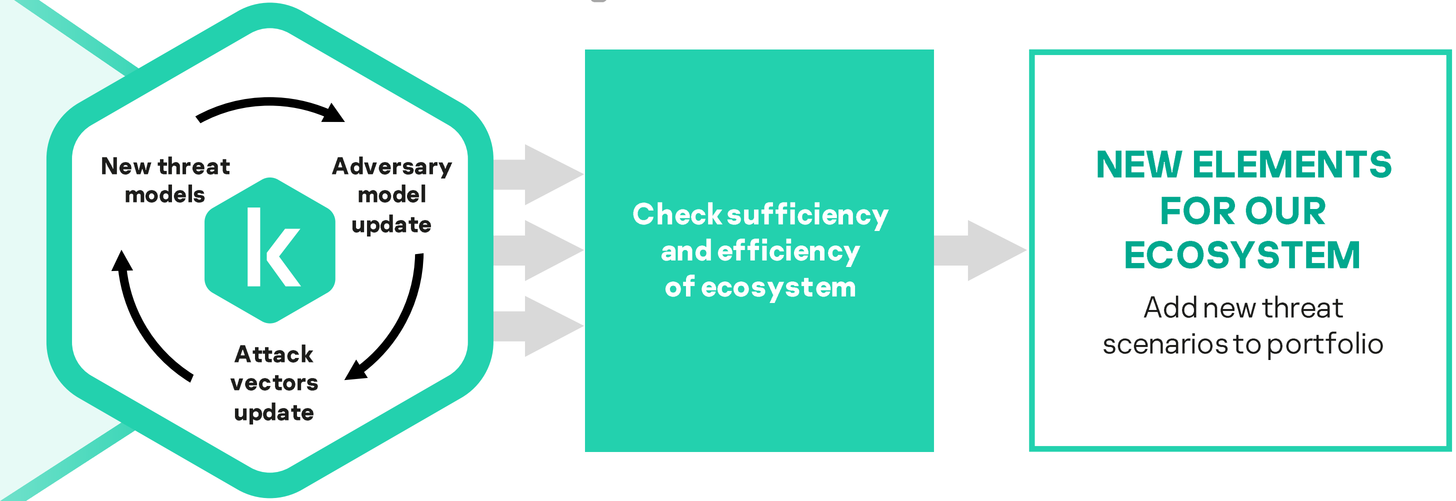
Kaspersky B2B Security Ecosystem

Ecosystem extending framework

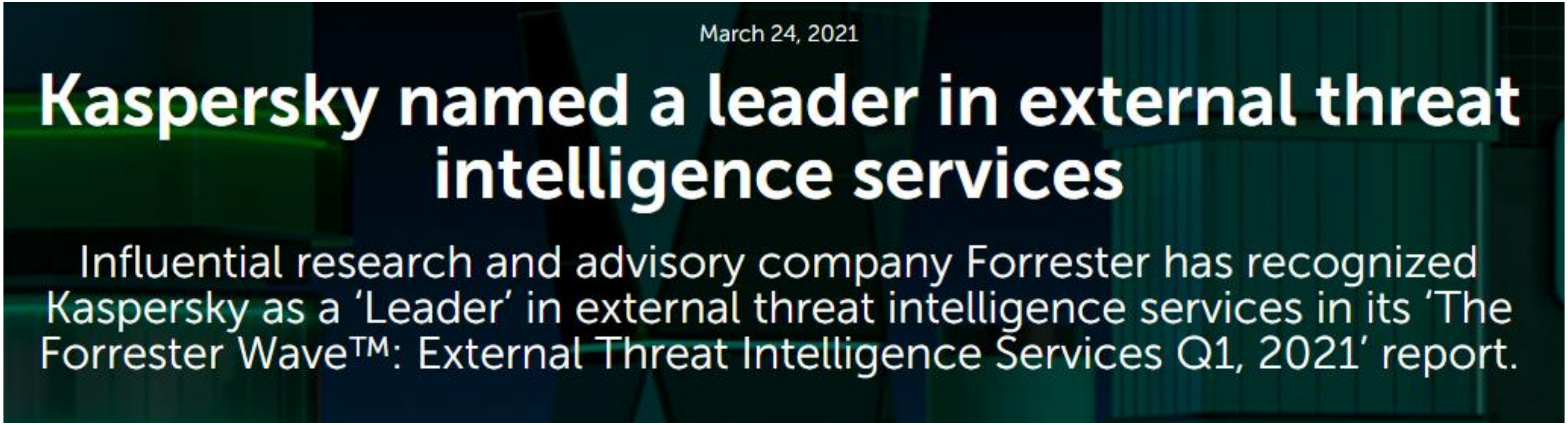
TI Sources

- Managed Detection and Response, analysis
- Incident Response, service reports
- Penetration testing and Security Assessment, service reports
- MITRE Shield matrix analysis
- APT research

New findings


New threat models
Adversary model update
Attack vectors update
Check sufficiency and efficiency of ecosystem
NEW ELEMENTS FOR OUR ECOSYSTEM
Add new threat scenarios to portfolio

Ecosystem extending framework



March 24, 2021

Kaspersky named a leader in external threat intelligence services

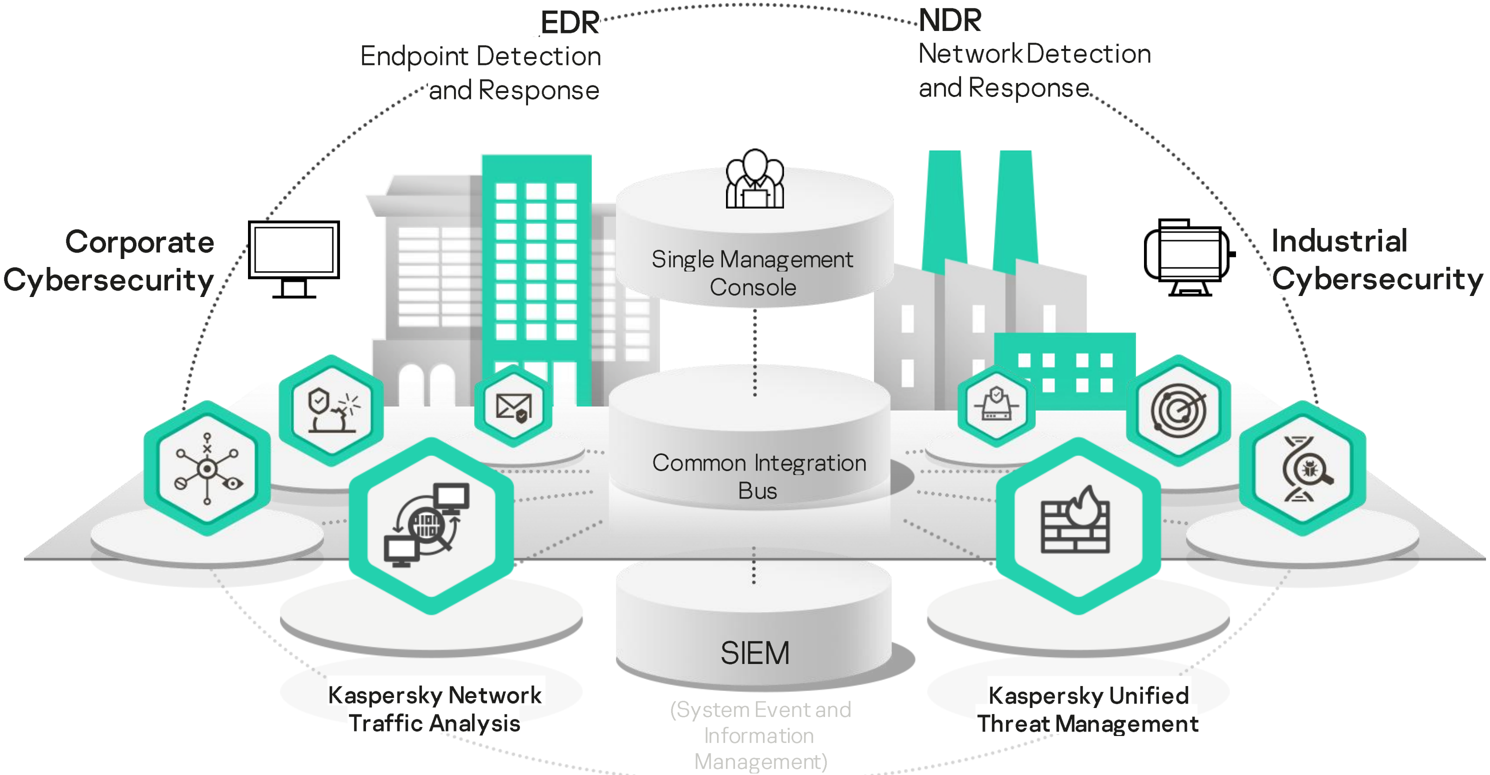
Influential research and advisory company Forrester has recognized Kaspersky as a ‘Leader’ in external threat intelligence services in its ‘The Forrester Wave™: External Threat Intelligence Services Q1, 2021’ report.

multi-platform coverage

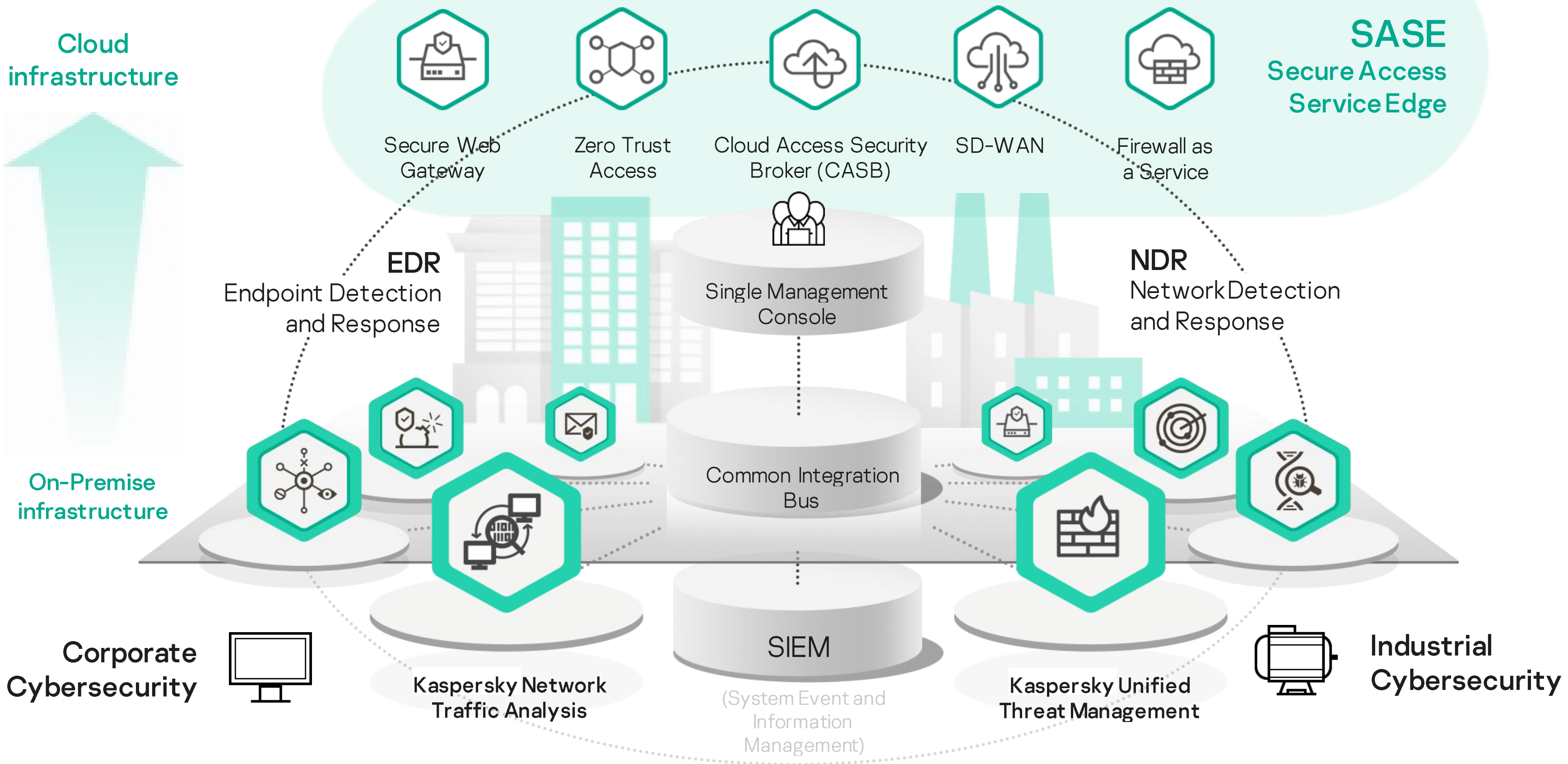
iOS
Powered by
Linux

Multi-platform

Kaspersky B2B Security EcoSystem


EDR
Endpoint Detection and Response
NDR
Network Detection and Response
Corporate Cybersecurity
Industrial Cybersecurity
Single Management Console
Common Integration Bus
SIEM
(System Event and Information Management)
Kaspersky Network Traffic Analysis
Kaspersky Unified Threat Management

Kaspersky B2B Security EcoSystem



Cloud infrastructure

On-Premise infrastructure

SASE
Secure Access Service Edge

Secure Web Gateway

Zero Trust Access

Cloud Access Security Broker (CASB)

SD-WAN

Firewall as a Service

EDR
Endpoint Detection and Response

NDR
Network Detection and Response

Single Management Console

Common Integration Bus

SIEM
(System Event and Information Management)

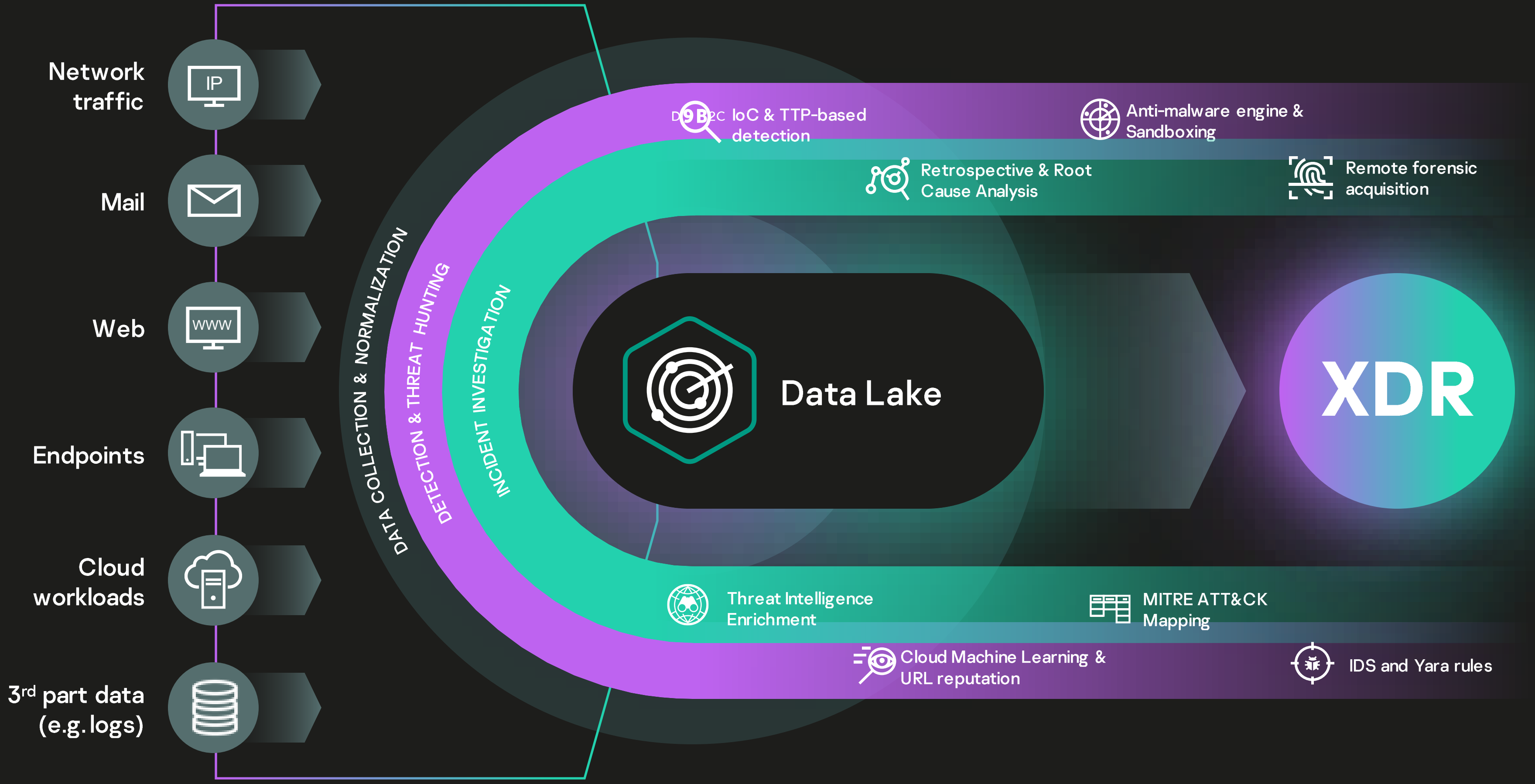
Kaspersky Network Traffic Analysis

Kaspersky Unified Threat Management

Corporate Cybersecurity

Industrial Cybersecurity

XDR



Network traffic

Mail

Web

Endpoints

Cloud workloads

3rd part data (e.g. logs)

DATA COLLECTION & NORMALIZATION

DETECTION & THREAT HUNTING

INCIDENT INVESTIGATION

IoC & TTP-based detection

Anti-malware engine & Sandboxing

Retrospective & Root Cause Analysis

Remote forensic acquisition

Data Lake

XDR

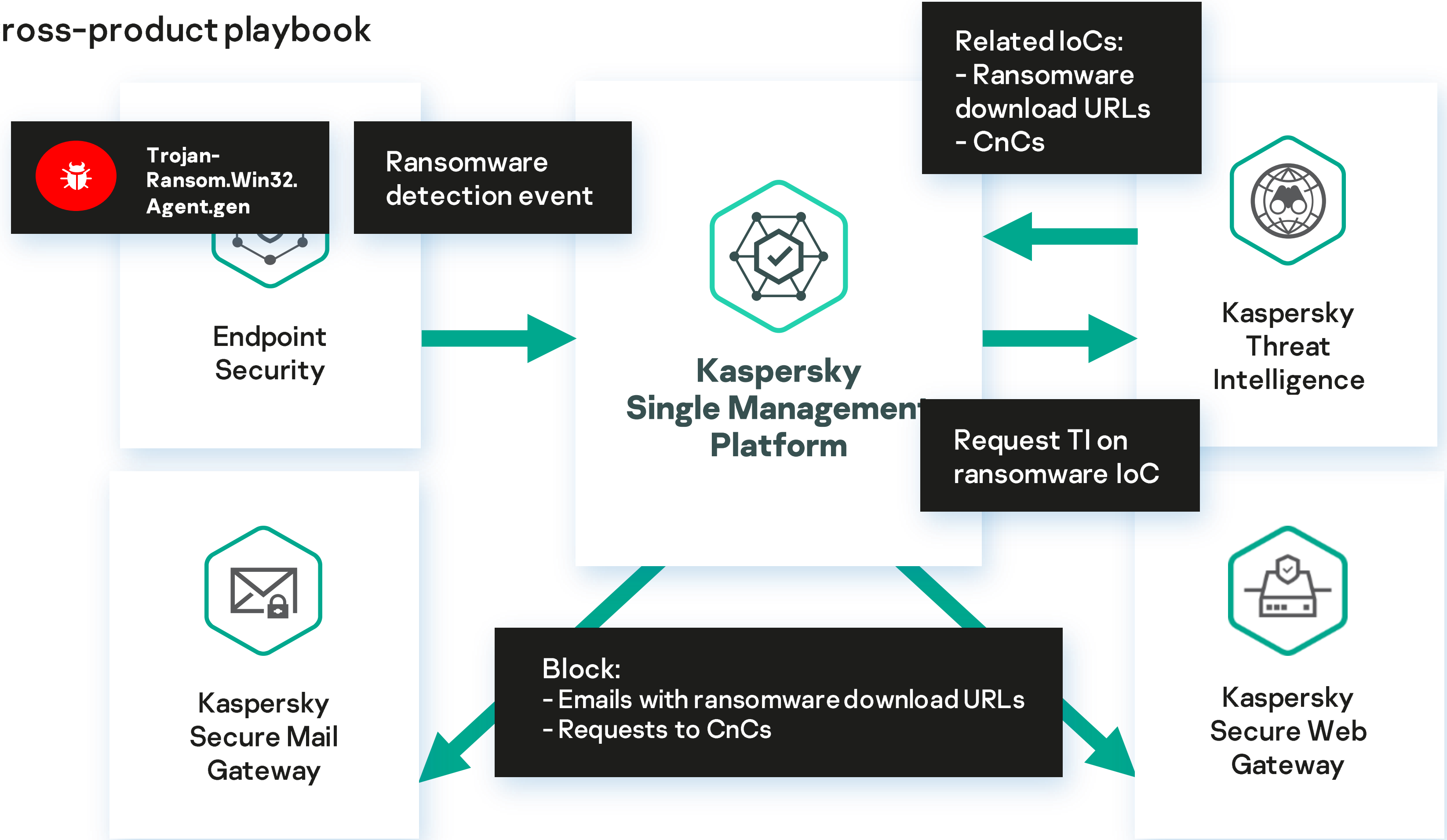
Threat Intelligence Enrichment

MITRE ATT&CK Mapping

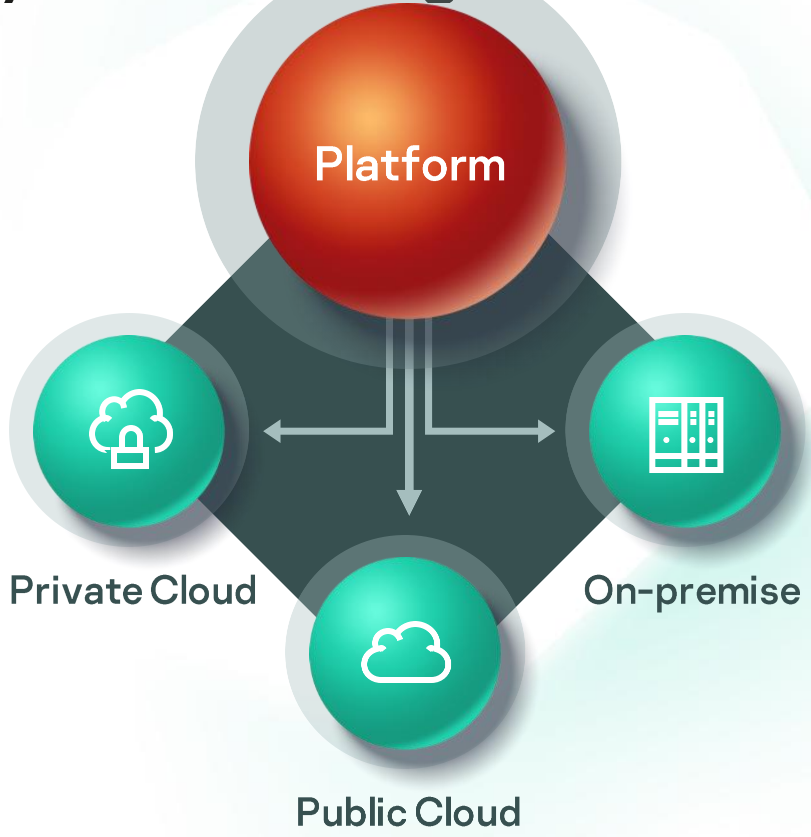
Cloud Machine Learning & URL reputation

IDS and Yara rules

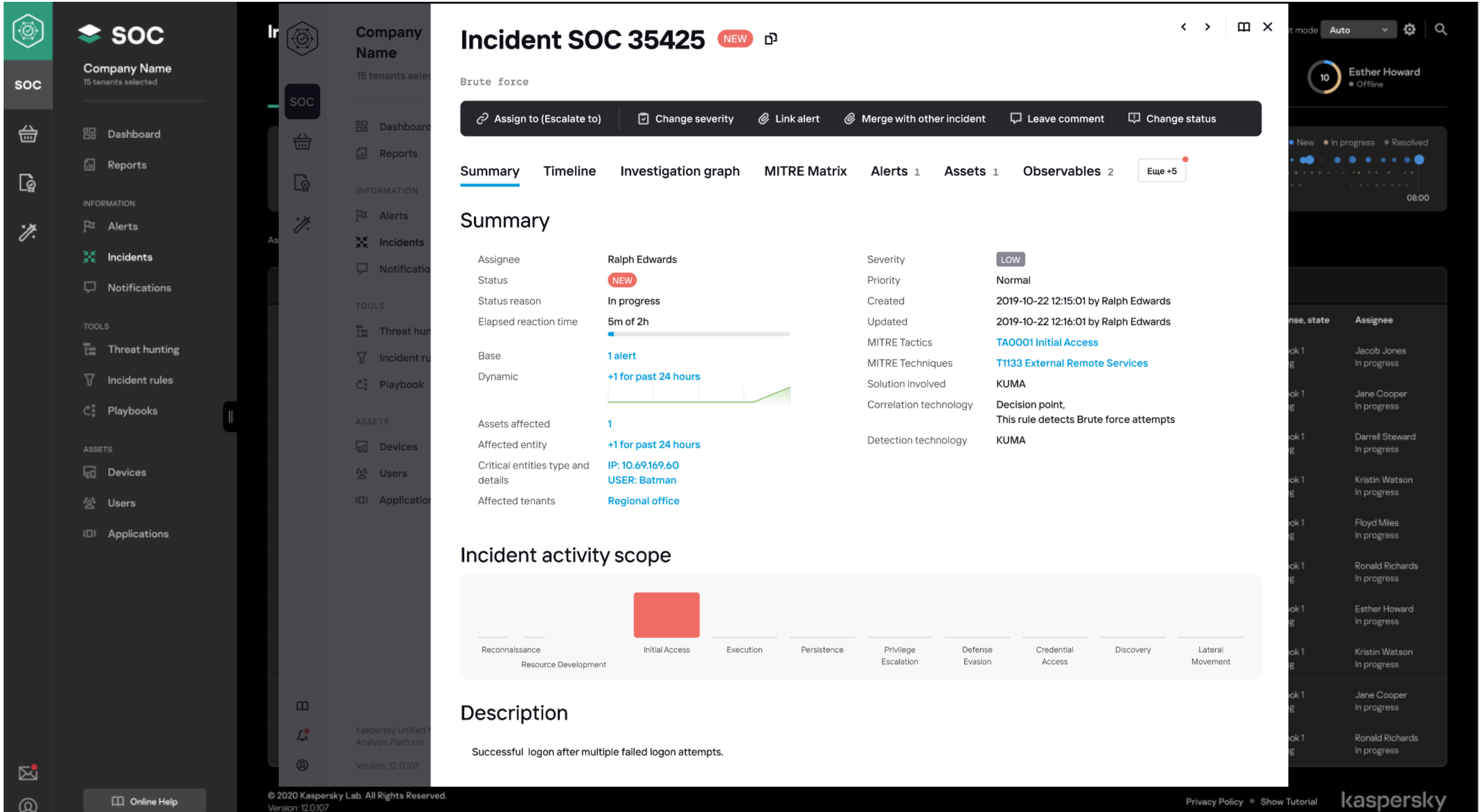
Cross-product playbook


Trojan-Ransom.Win32.Agent.gen
Ransomware detection event
Related IoCs:
- Ransomware download URLs
- CnCs
Endpoint Security
Kaspersky Single Management Platform
Kaspersky Threat Intelligence
Request TI on ransomware IoC
Kaspersky Secure Mail Gateway
Block:
- Emails with ransomware download URLs
- Requests to CnCs
Kaspersky Secure Web Gateway

OSMP– Deployment model agnostic



OSMP first release



Incident SOC 35425 NEW

Brute force

Summary

Assignee	Ralph Edwards	Severity	LOW
Status	NEW	Priority	Normal
Status reason	In progress	Created	2019-10-22 12:15:01 by Ralph Edwards
Elapsed reaction time	5m of 2h	Updated	2019-10-22 12:16:01 by Ralph Edwards
Base	1 alert	MITRE Tactics	TA0001 Initial Access
Dynamic	+1 for past 24 hours	MITRE Techniques	T1133 External Remote Services
Assets affected	1	Solution involved	KUMA
Affected entity	+1 for past 24 hours	Correlation technology	Decision point, This rule detects Brute force attempts
Critical entities type and details	IP: 10.69.169.60 USER: Batman	Detection technology	KUMA
Affected tenants	Regional office		

Incident activity scope

Description

Successful logon after multiple failed logon attempts.

Assignee
Jacob Jones In progress
Jane Cooper In progress
Darrell Steward In progress
Kristin Watson In progress
Floyd Miles In progress
Ronald Richards In progress
Esther Howard In progress
Kristin Watson In progress
Jane Cooper In progress
Ronald Richards In progress

Kaspersky Unified Monitoring and Analysis Platform

Version: 12.0.107

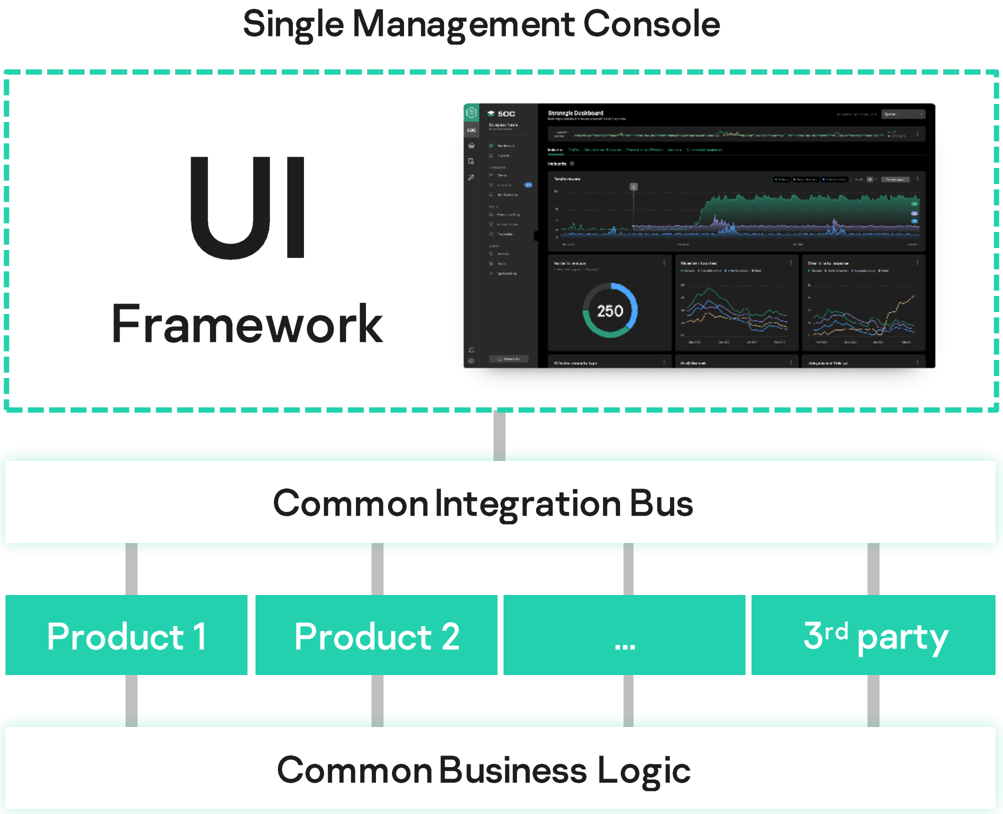
© 2020 Kaspersky Lab. All Rights Reserved.

Version: 12.0.107

Kaspersky Single Management Platform

Kaspersky Single Management Platform

SMP Demo



Single Management Console

UI Framework

Common Integration Bus

Product 1

Product 2

...

3rd party

Common Business Logic

Thank you!

kaspersky