kaspersky

Security Operation Center (SOC) - Gestartet, gescheitert?

Marco Schopp

Was haben die Fußball WM 2018 und die Bundesregierung Deutschland gemeinsam?

Step-by-step Cybersecurity Strategy

STEP 3 — INTEGRATED CYBERSECURITY APPROACH

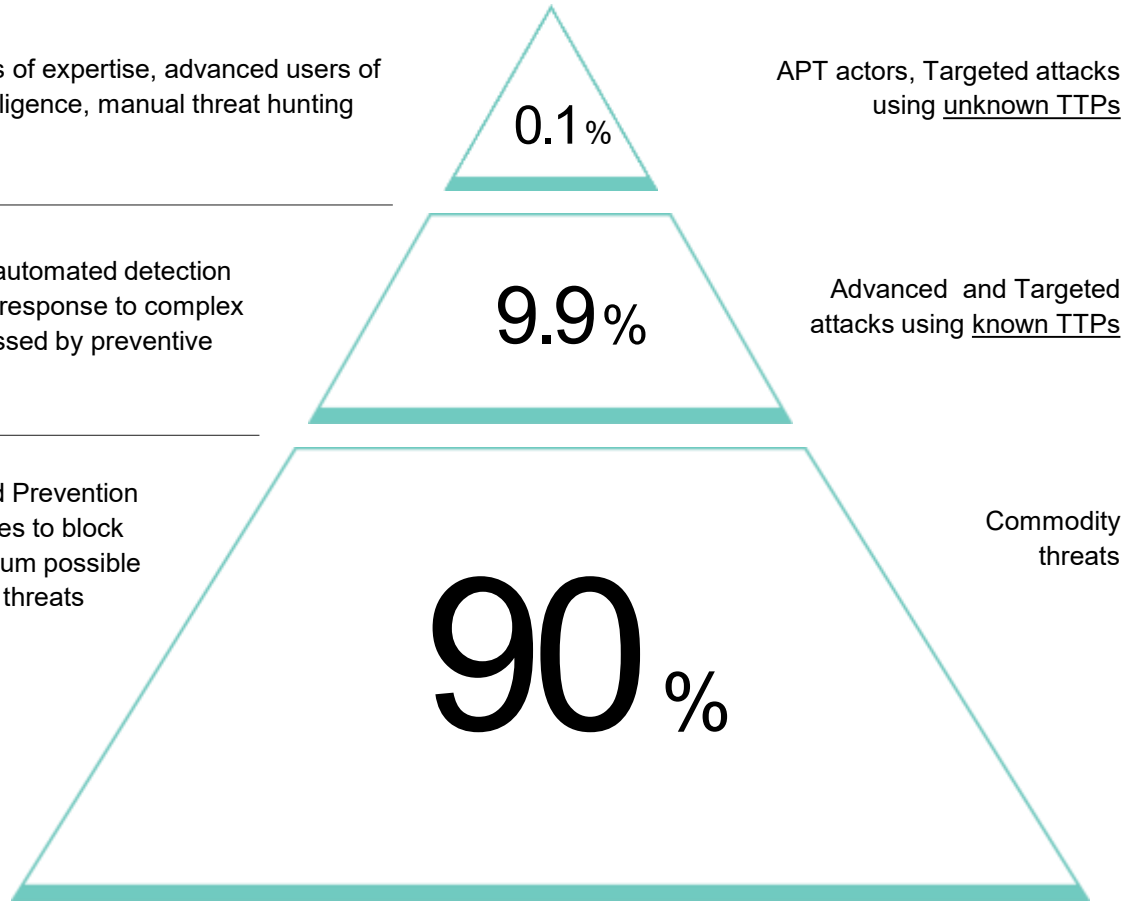
High levels of expertise, advanced users of threat intelligence, manual threat hunting

STEP 2 — ADVANCED DEFENSE

Focus on automated detection and a fast response to complex threats missed by preventive protection

STEP 1 — SECURITY FOUNDATIONS

Automated Prevention technologies to block the maximum possible number of threats



APT actors, Targeted attacks using unknown TTPs

Advanced and Targeted attacks using known TTPs

Commodity threats

Mature IT Security Team or SOC

IT Security Manager

IT Manager

Security Operations Centers

INTELLIGENCE-DRIVEN SOC

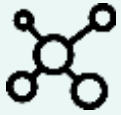
Pentest and red teaming	Security assessment services	Advanced security training
Malware analysis and Digital Forensics	Threat Intelligence services	Threat hunting services

ENDPOINT DETECTION AND RESPONSE

ANTI TARGETED ATTACK

SECURITY OPERATIONS CENTERS

CLASSIC SOC


Log collection & correlation


Monitoring and alerting

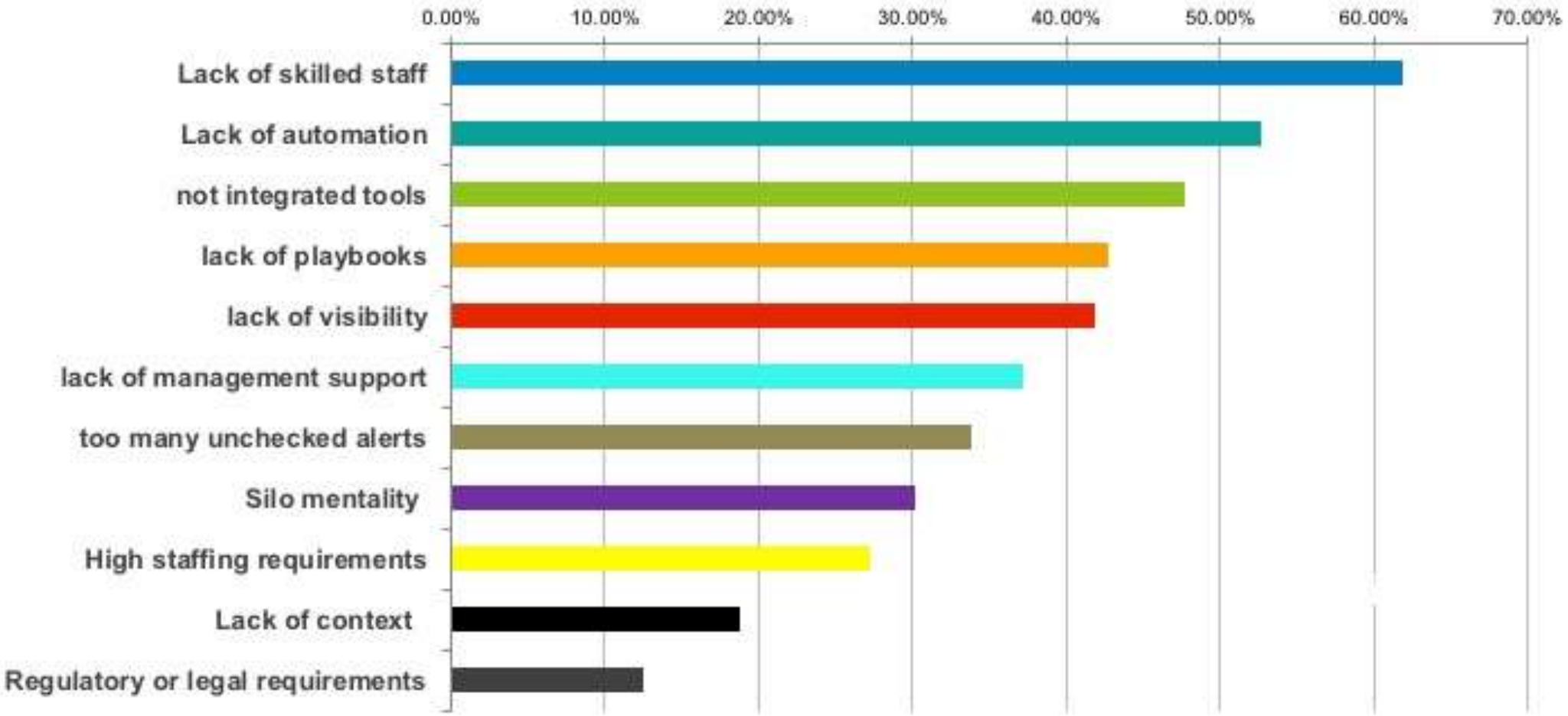

Case management


Incident reporting

CORE

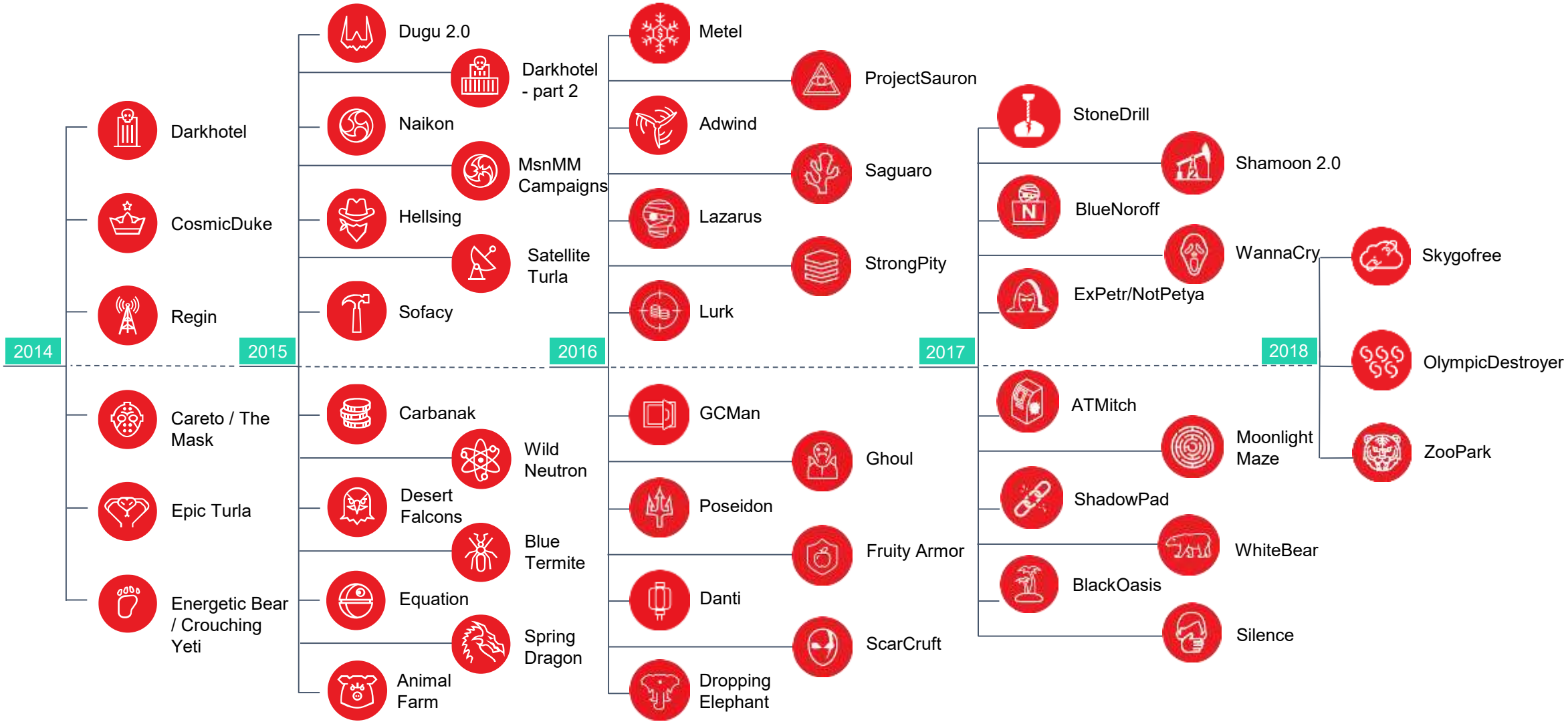
62%

SOC Challenges:



Source: 2018 SANS Survey

Our Research



kaspersky

Vielen Dank!

Wir freuen uns auf Ihren Besuch in Halle 9, Stand 430.

kaspersky.com