

Вебинар

07 июля, 11:00 МСК

От иллюзий к реальности SOCa

взгляд практиков на заблуждения о SOC и работающие подходы к его построению



Евгений Буйволов

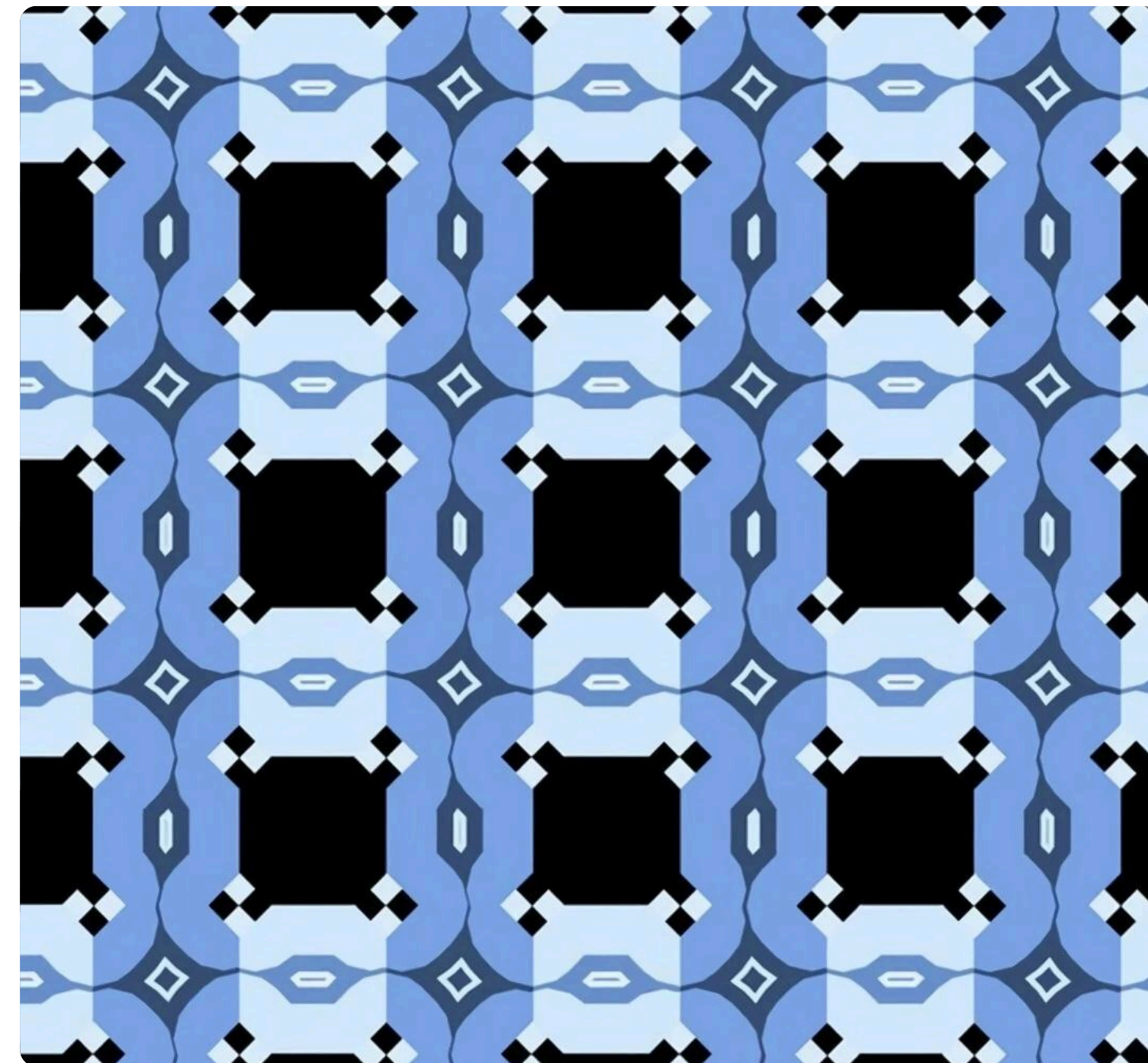
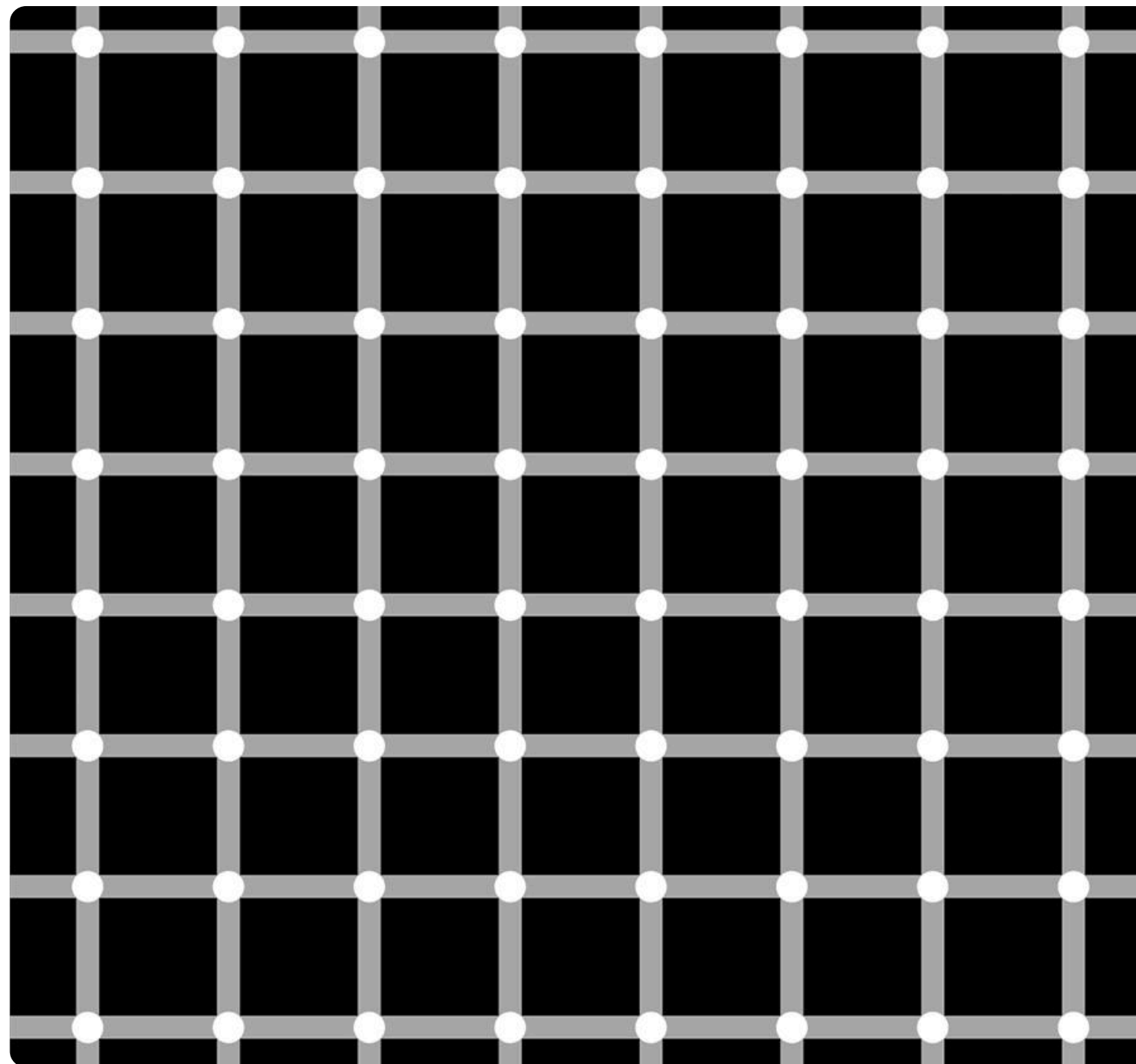
Заместитель руководителя
SOC



Сергей Прохоров

Эксперт в области
кибербезопасности

Есть много иллюзий
по работе SOC



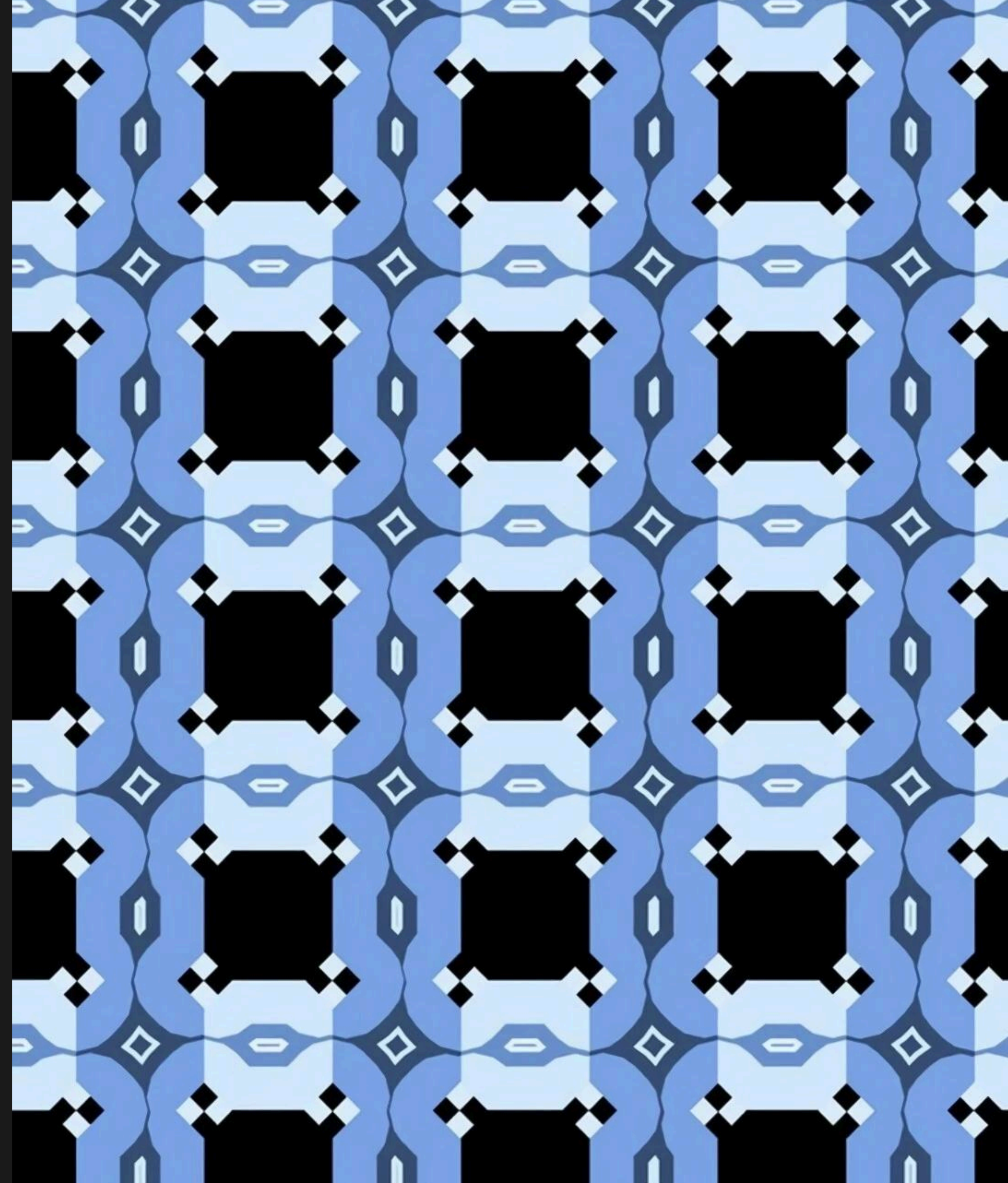
Иллюзия №1

- Может ли SOC заменить ИБ?
- SOC как суррогат ИБ



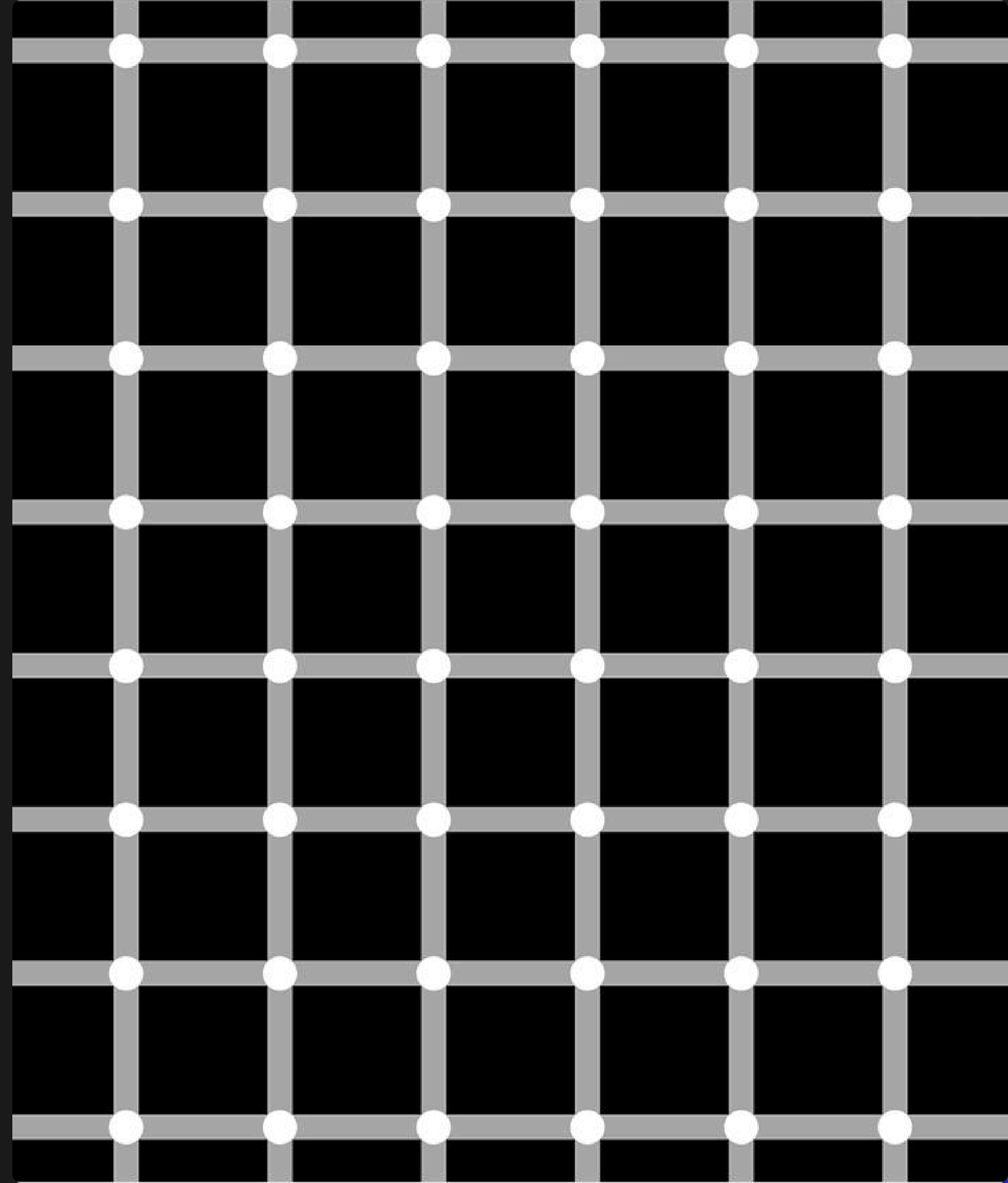
«Нет» иллюзии SOC features

- SOC это не SIEM
- SOC это не мониторинг



«Да» иллюзии SOC features

- Внешний SOC это дорого
- SOC это страховка



Немного теории для следующего мифа. Виды *DR

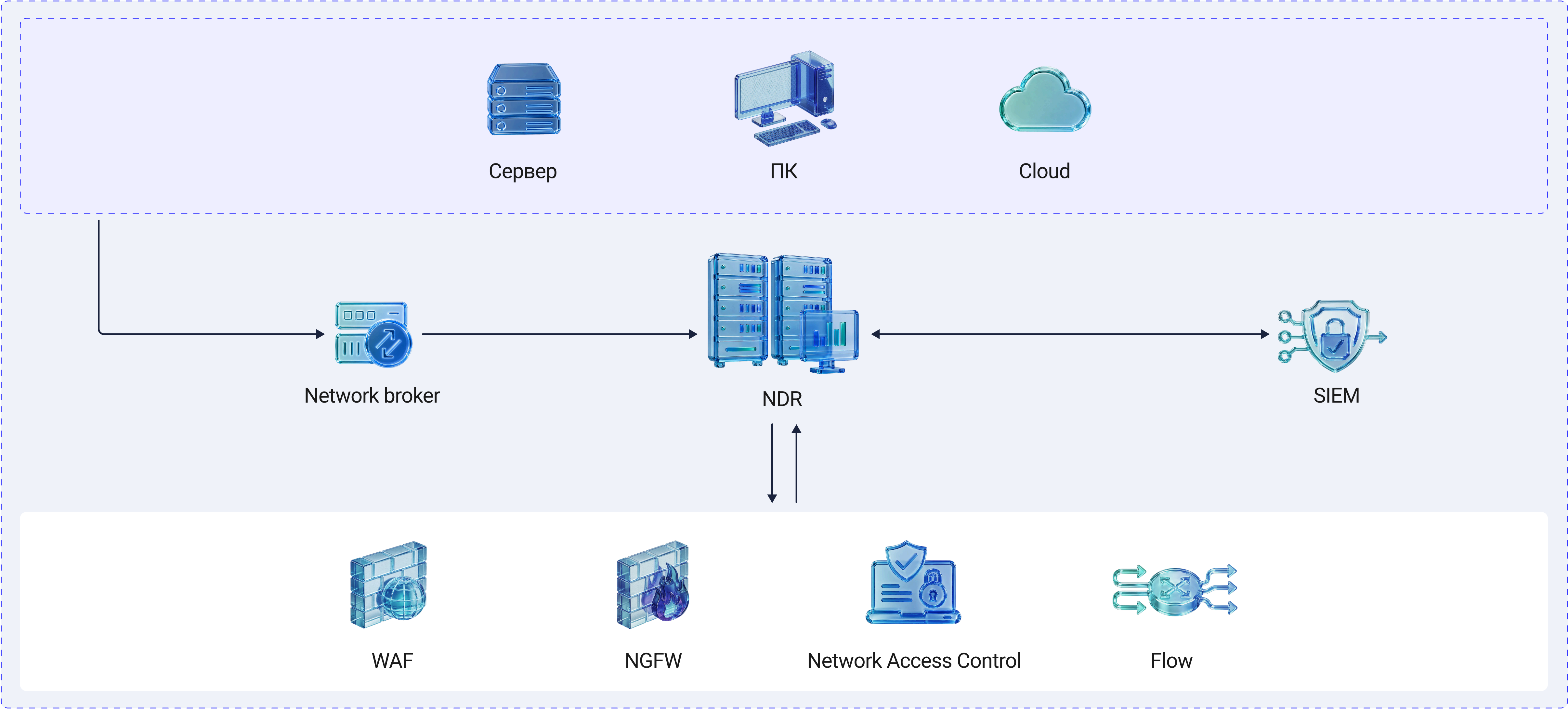
$$XDR \supseteq \{NDR, EDR, ITDR, CDR, emDR\}$$
$$\times$$
$$MDR$$
$$=$$
$$MXDR$$


Username

.....

Login

NDR



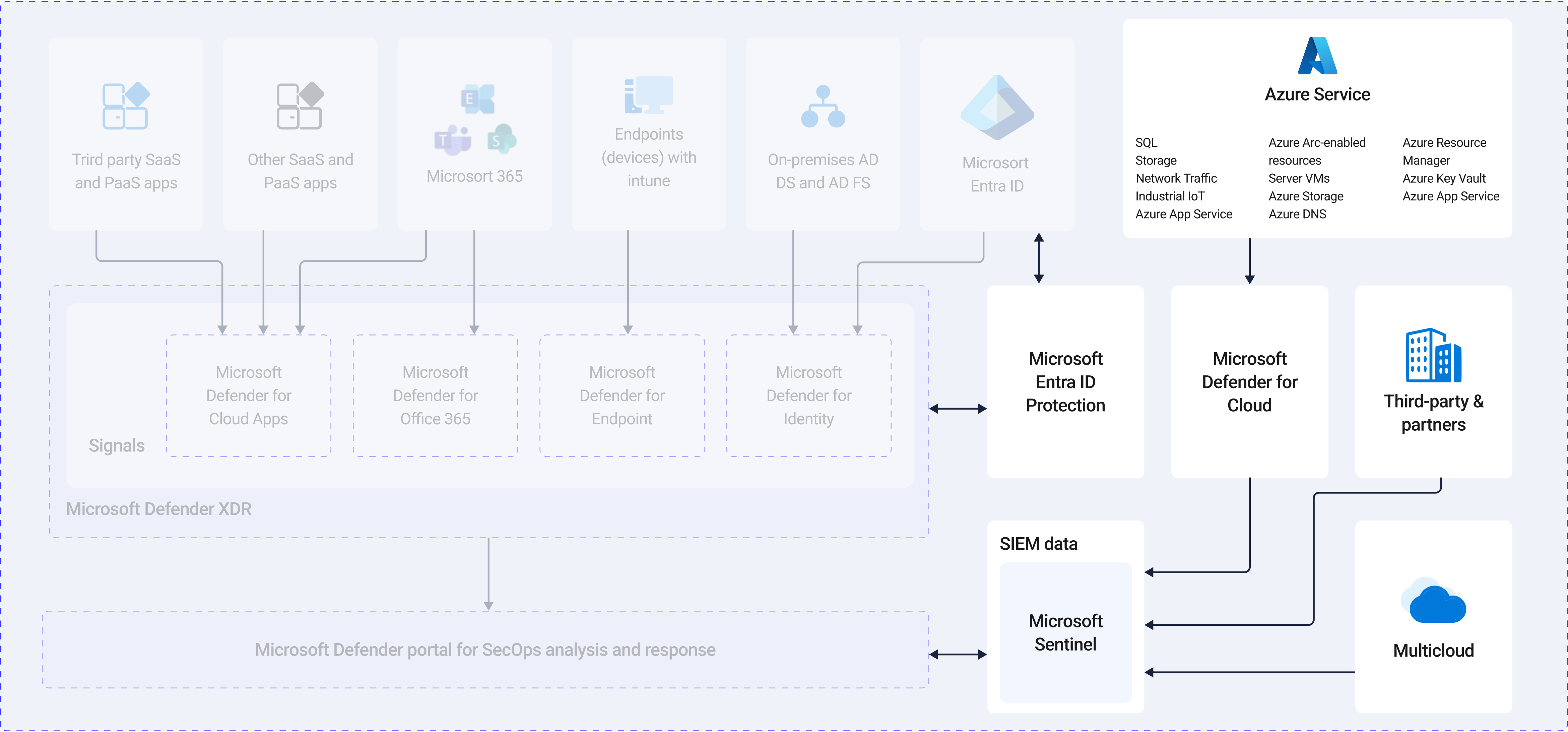
Виды XDR

Top 18 XDR Tools (2025 Edition)

Xcitium XDR  ZeroDwell™ Containment with AI analytics for detection-less protection and unified visibility.	Cynet Security XDR  Advanced, holistic threat detection with precision-driven automated incident handling.	Trend Vision One  Cross-layered detection and integrated threat intelligence for proactive breach prevention.
CrowdStrike Falcon  Comprehensive endpoint protection with advanced network and endpoint response.	SentinelOne XDR  Comprehensive endpoint, cloud, and identity protection with autonomous response capabilities.	Cybereason Defense  Continuous end-to-end visibility and response for increasingly complex threats.
Heimdal XDR  Prevents advanced endpoint and network attacks with intelligent automated detection and response.	Microsoft Defender  Unified protection for identities, endpoints, and cloud delivering seamless security.	Cisco XDR  Integrates threat intelligence across endpoints, networks, and cloud for unified defense.
IBM Security QRadar  Delivers broad visibility and advanced analytics for faster, more accurate threat detection.	Sophos XDR  Detects and responds across endpoints, network, email, and cloud with unified intelligence.	McAfee MVISION XDR  Enriches threat intelligence through multiple data sources with adaptive correlation.
Elastic Security XDR  Centralized threat hunting and analytics on Elastic Stack enabling proactive defense.	FireEye XDR  Combines advanced threat intelligence and extended visibility for unified protection and agility.	Fortinet FortiXDR  AI-driven analytics and response across the entire stack enabling proactive defense.
Rapid7 InsightXDR  Correlates user, endpoint, and network data for fast insights and automated containment.	Arctic Wolf XDR  24/7 monitoring, proactive threat detection, and response ensuring continuous defense.	Palo Alto Networks  Uses AI and behavioral analytics to detect and stop threats across endpoints, networks, and cloud.

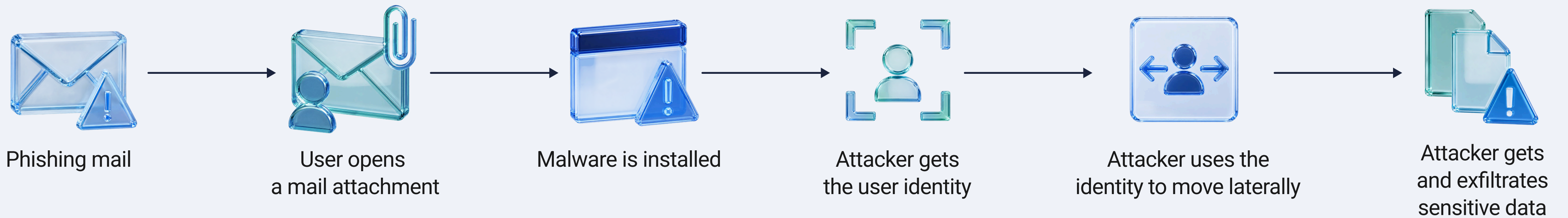


Open XDR



Native XDR

Attack attempts:



Mitigated by:



Чудеса рынка

«А у нас XDR!»



ECS (Elastic Common Schema)

314	device	device.vendor.name	keyword	extended		SanDisk	Vendor name of the device
315	dll	dll.code_signature.digest_algorit...	keyword	extended		sha256	Hashing algorithm used to sign the process.
316	dll	dll.code_signature.exists	boolean	core		true	Boolean to capture if a signature is present.
317	dll	dll.code_signature.flags	keyword	extended		570522385	Code signing flags of the process
...							
1294	process	process.entry_leader.user.name...	match_only_text	core		a.einstein	Short name or login of the user.
1295	process	process.entry_leader.vpid	long	core		4242	Virtual process id.
1296	process	process.entry_leader.working_di...	keyword	extended		/home/alice	The working directory of the process.
1297	process	process.entry_leader.working_di...	match_only_text	extended		/home/alice	The working directory of the process.
1298	process	process.env_vars	keyword	extended	array	["PATH=/usr/local/bin:/usr/bin", "USER=ubuntu"]	Array of environment variable bindings.
...							
2298	threat	threat.indicator.marking.tlp_ver...	keyword	extended		2.0	Indicator TLP version
2299	threat	threat.indicator.modified_at	date	extended		2020-11-05T17:25:47.000Z	Date/time indicator was last updated.
2300	threat	threat.indicator.name	keyword	extended		5.2.75.227	Indicator display name
2301	threat	threat.indicator.port	long	extended		443	Indicator port
2302	threat	threat.indicator.provider	keyword	extended		lrz_urlhaus	Indicator provider
2303	threat	threat.indicator.reference	keyword	extended		https://system.example.com/indicator/0001234	Indicator reference URL
2304	threat	threat.indicator.registry.data.by...	keyword	extended		ZQBuAC0AVQBTAAAZQBuAAAAA=	Original bytes written with base64 encoding.
2305	threat	threat.indicator.registry.data.stri...	wildcard	core	array	["C:\\rta\\red ttp\\bin\\myapp.exe"]	List of strings representing what was written to the registry.
...							
2793	vulnerability	vulnerability.classification	keyword	extended		CVSS	Classification of the vulnerability.
2794	vulnerability	vulnerability.description	keyword	extended		In macOS before 2.12.6, there is a vulnerability in the RPC...	Description of the vulnerability.
2795	vulnerability	vulnerability.description.text	match_only_text	extended		In macOS before 2.12.6, there is a vulnerability in the RPC...	Description of the vulnerability.
2796	vulnerability	vulnerability.enumeration	keyword	extended		CVE	Identifier of the vulnerability.
2797	vulnerability	vulnerability.id	keyword	extended		CVE-2019-00001	ID of the vulnerability.
2798	vulnerability	vulnerability.reference	keyword	extended		https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6111	Reference of the vulnerability.
2799	vulnerability	vulnerability.report_id	keyword	extended		20191018.0001	Scan identification number.
2800	vulnerability	vulnerability.scanner.vendor	keyword	extended		Tenable	Name of the scanner vendor.
2801	vulnerability	vulnerability.score.base	float	extended		5.5	Vulnerability Base score.
2802	vulnerability	vulnerability.score.environmental	float	extended		5.5	Vulnerability Environmental score.
2803	vulnerability	vulnerability.score.temporal	float	extended			Vulnerability Temporal score.
2804	vulnerability	vulnerability.score.version	keyword	extended		2.0	CVSS version.
2805	vulnerability	vulnerability.severity	keyword	extended		Critical	Severity of the vulnerability.
2806	vulnerability	vulnerability.status	keyword	extended		open	Lifecycle state of a vulnerability finding.

Миф №5

- Security OPERATION Center
- MSSP/MIS vs Monitoring
- MDR & MXDR



СТІ

HoneyPot

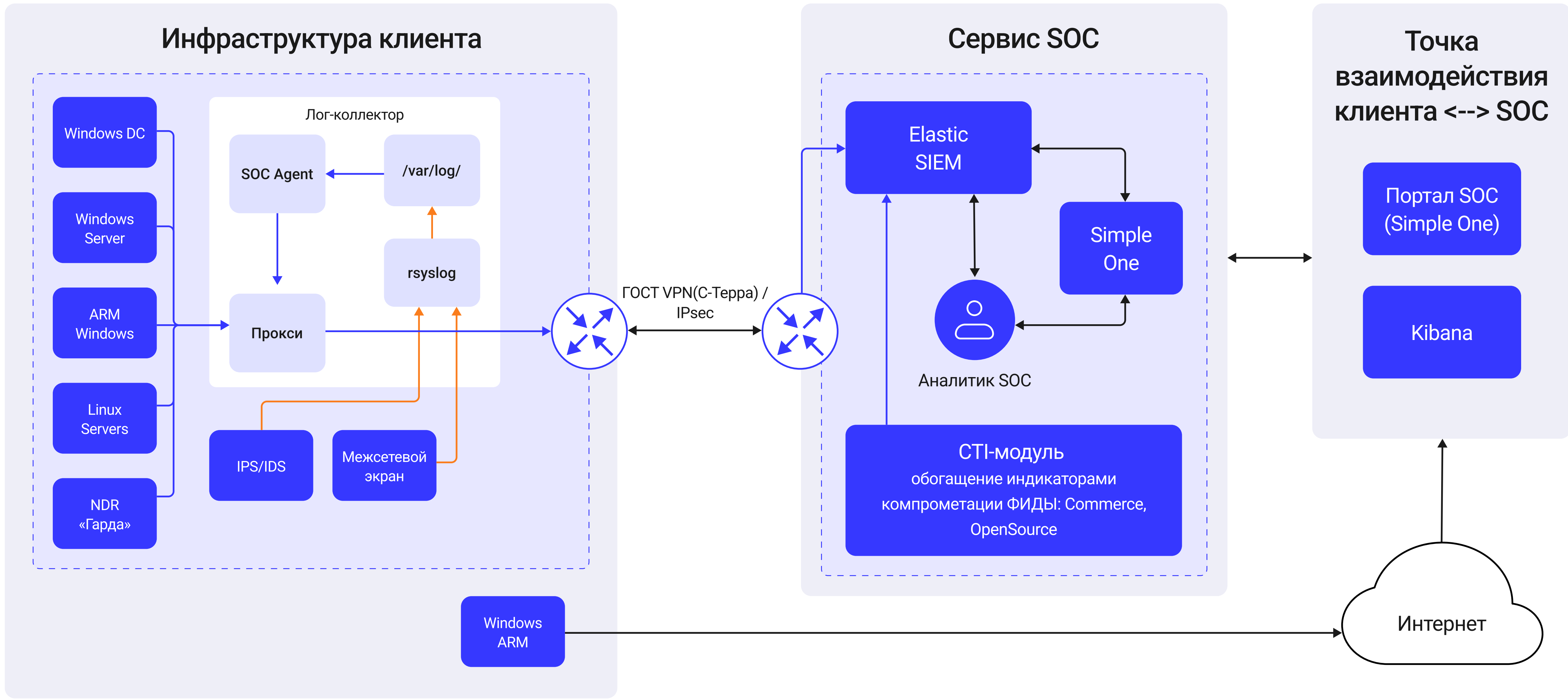
AI/ML

Подготовка к атаке

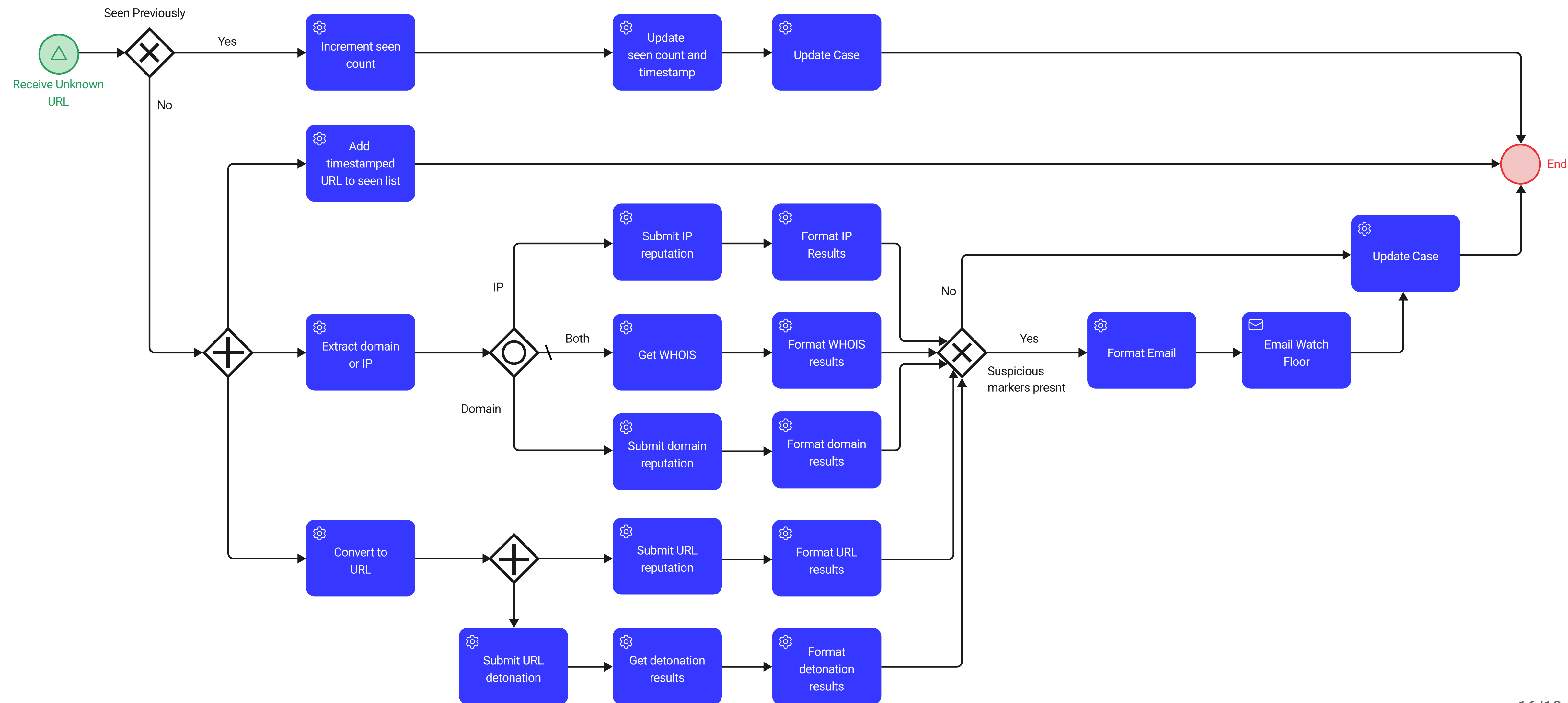
Аналитик (MDR)



Люди и процессы

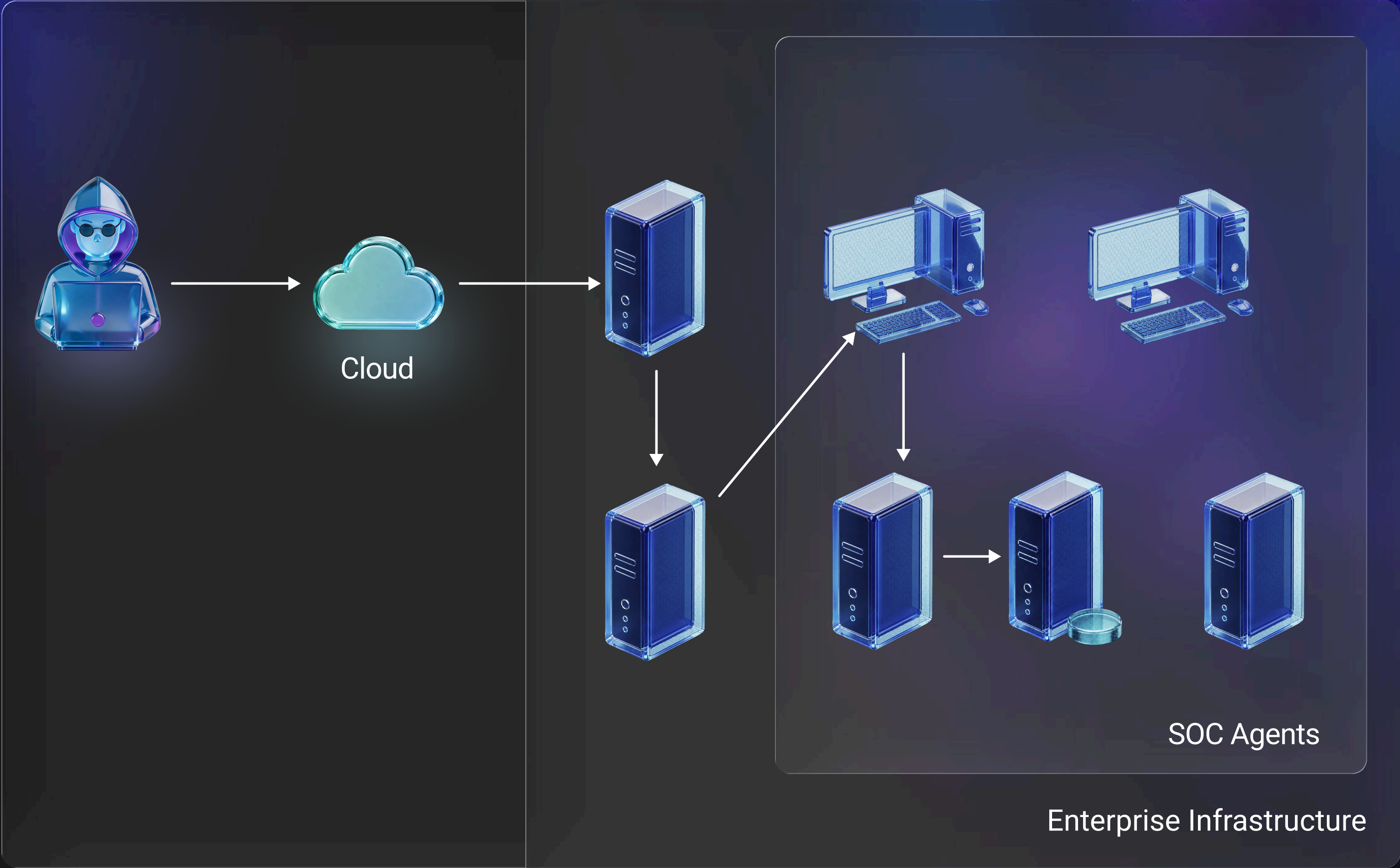


Playbooks



А у нас..

- Скорость подключения
- Канарейки, канарейки..
- Цены на рынке



Спасибо за внимание

 itgsecurity.ru

 info@itgsecurity.ru

 sales@itgsecurity.ru

