THE VALUE OF SECURITY TOOLS: WHAT WE WOULDN'T HAVE IF WE HAD EVERYTHING



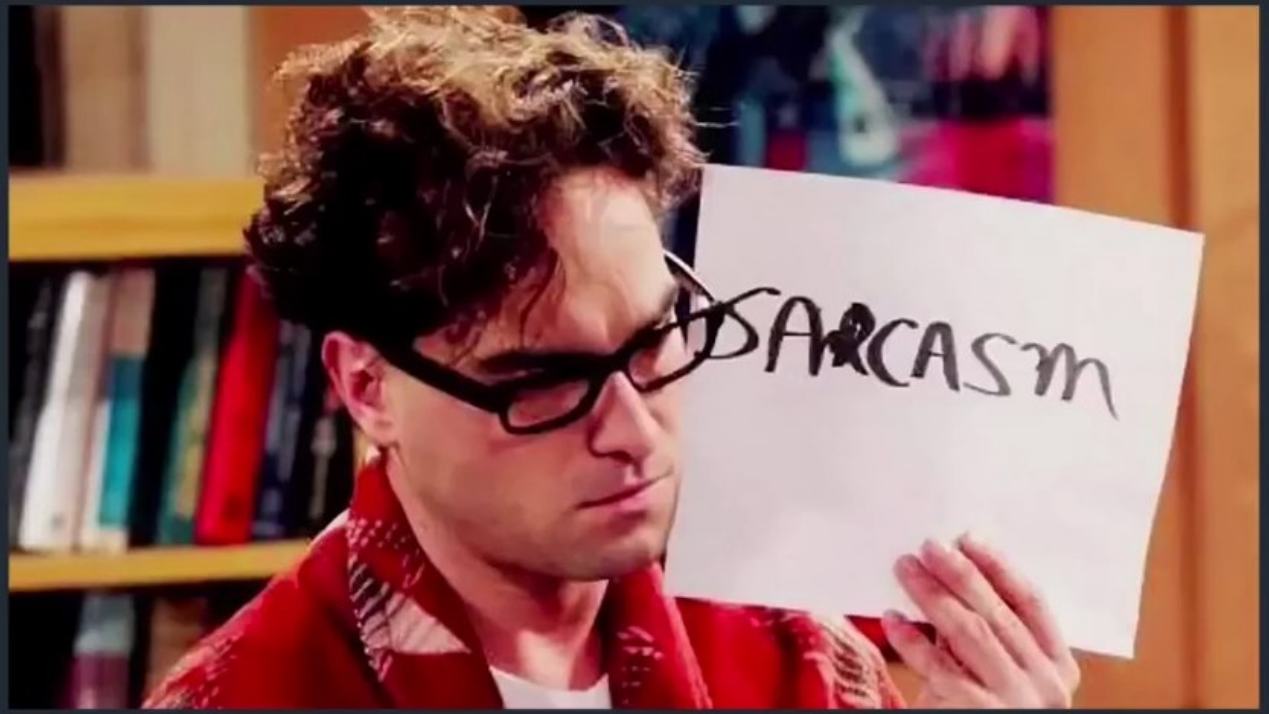
Словосочетания "кибер-зрелость" придуманное ИБ-маркетологами, чаще всего, звучит как: "У вас нет 5 млн. рублей за наш ВЕЛИКИЙ продукт? Ну так вы еще не доросли! Идите отседова, не мешайте торговать!"

😁 8 🔥 7 💯 5

756 23:41

Leave a Comment

© BEHOLDERISHERE


SARCASM

MYTHS OF REASONABLENESS AND MATURITY

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

Antivirus finds, blocks and removes malware.

Antivirus is the basic level of endpoint protection: users, office machines, servers. The very first step in a cybersecurity strategy.

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

NUANCES:

- False positives
- False sense of security
- Limited detection
- Poor integration with other security tools
- BYOD
- Difficulties in investigating incidents

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

WHAT AWAITS US WITHOUT ANTIVIRUS:

- Simple threats won't be blocked right away
- Higher load on other security systems
- Increased risk of infection “from below”
- Loss of the basic level of compliance
- Financial and reputational consequences

This is the foundation, the basics. If your company uses even one digital device — you need an antivirus.

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

DATA LOSS PREVENTION/PROTECTION

The basic task of DLP is to prevent leaks of data (personal, financial, confidential) by controlling the channels.

WHEN IT IS USED:

- When compliance with GDPR, HIPAA, ISO 27001, FZ-152 etc. is required.

  When the risk of insider or commercial information leaking is high.

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

MAIN DIFFICULTIES OF RUNNING DLP IN CORPORATE SECURITY:

- High demands on configuration and data classification
- False positives and “noise”
- Negative user reaction
- Technical limitations

Integration with business processes

- Leak channels evolve — constant re-tuning needed
- Balance (reasonableness!!!!111!11!) in everything

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

WHAT AWAITS US WITHOUT DLP:

- Higher risk of data leaks
- No control over transfer channels
- Financial and reputational losses
- Breaking the law and fines
- No incident investigations!
- Insider attacks become possible
- Hard to meet partners' requirements

DLP is good and important!

DLP put in “with the spare change” is bad — eats money, creates problems.

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

Endpoint Detection and Response (EDR) — monitors PCs and servers, but does it a bit more interestingly than antivirus: it records process behaviour, network connections, script launches and so on.

Extended Detection and Response (XDR) — a larger-scale EDR. It uses the network, email, clouds etc. as data sources, correlates events across systems and provides a single console for management and investigation.

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

EDR/XDR NUANCES IN CORPORATE SECURITY:

- Noise and alert overload
- Complex to deploy and configure
- High demands on staff competence
- Integration with other systems
- Balance between security and user convenience
- Expensive to scale (and you will have to!!!)

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

WHAT AWAITS US WITHOUT EDR/XDR:

- Poor visibility of endpoints
- Late detection of incidents
- Investigation difficulties (DFIR)

Ineffective SOC

- Growing damage from attacks
- Failure to meet modern security standards

EDR and XDR are powerful tools for protecting corporate infrastructure that provide a high level of security. But before deploying them it is important to weigh carefully all the pros and cons, and the company’s readiness for such changes.

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

SECURITY INFORMATION & EVENT MANAGEMENT

SIEM collects logs and stores events, applies correlation rules.

IMPORTANT:

It does not respond automatically (unlike SOAR) and does not protect by itself — it detects and informs; it can take data from EDR, AV, network devices, DLP and other systems.

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

THORNS ON THE WAY TO SIEM:

- "Garbage" at the input
- Detailed rules have to be written for your infrastructure

  You must be sure you have the resources for manual or automatic response to SIEM's call, otherwise there is no point

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

WHAT AWAITS US WITHOUT SIEM:

- No single picture of security events
- Poor real-time visibility of attacks
- SOC goes “blind”
- Investigations become hard (DFIR)
- Failure to meet requirements and standards

At scale, without SIEM a company effectively loses the central brain of monitoring. All the other systems work, but each on its own, and the business has no full security picture.

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

SECURITY ORCHESTRATION, AUTOMATION & RESPONSE

SOAR is an automatic problem-shoveller.
This system does not collect data itself, but it automates the response.

WHAT AWAITS US? WE WANT SOAR!

- Complex to configure and integrate
- Writing playbooks
- Danger of automatic actions
- Pushback from other teams

  Reality: SOAR has to interfere in other teams' processes (sysadmins, IT, the support desk)

SOAR ≠ artificial intelligence. SOAR will decide nothing by itself. It does not "think"

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

WHAT AWAITS US WITHOUT SOAR:

- Slow response to incidents
- SOC overload and analyst burnout
- More errors
- Uneven level of protection
- Difficulties in scaling
- Financial consequences

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

SECURITY OPERATION CENTER

SOC is an information security monitoring centre. An organizational unit that receives signals from everywhere, sorts through them and responds accordingly.

GREAT AND TERRIBLE!!!

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

WHAT AWAITS US WITHOUT SOC:

- Cost
- Shortage of decent staff
- Flow of incidents and alert fatigue
- Complex integration of different systems
- Incident response — manual and slow
- Hard to run 24/7

No business support

- Attacks evolve

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

WHAT AWAITS US WITHOUT SOC:

- No round-the-clock monitoring
- Slower response
- No centralized picture of threats
- More undetected incidents
- Chaos in response
- Financial and reputational losses
- No investigation expertise
- Difficulties with compliance

SOC is not an “option” but a necessary element of mature cyber defence at a certain scale.

A successful SOC = a balance of technologies (SIEM, SOAR, EDR/XDR, DLP), processes and people.

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOC

SOAR

DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

DFIR = investigation + incident response.

Working with DFIR is like investigating an accident on a nuclear submarine, but a week later, from the wreckage, with no access to the log book, with management that wants the “topic closed by lunchtime”.

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOAR

DFIR

HERE TOO IT IS NOT SIMPLE:

- No proper recording of information
- Time is critical
- Huge experience required
- Myriads of complex tools (vendor + open source + home-brewed)
- High demands on data collection and storage

ANTIVIRUS

DLP

EDR/XDR

SIEM

SOAR

SOAR

DFIR

MAYBE WE DON'T NEED IT? WE DO!

- The cause of incidents is unclear
- No certainty that the attack has been shut down
- No digital evidence
- Impossible to trace the attacker's actions
- Trouble with regulators and law enforcement
- Growing business risks

CHEAT SHEET REMINDER:

TECHNOLOGY / SYSTEM	REAL-WORLD ANALOGUE	EXPLANATION
Antivirus (AV)	A guard at the entrance with a metal detector	Checks everyone coming in for weapons. Responds to known threats (signatures)
EDR	Cameras in every office + an analyst watching behaviour	Watches what goes on inside, records strange actions, raises the alarm
XDR	A security system combining cameras, motion sensors, electronic locks etc.	Centralized visibility — links behaviour at the entrance, in the offices, in the car park
SIEM	A control room with logs and an event archive	Stores and analyses data from all systems: who came in, what they opened, where they went
SOAR	An auto-response system: alarm → door locked → guards called	On detecting a threat it runs pre-programmed actions
DLP	An X-ray at the exit checking whether secret documents are being carried out	Makes sure nobody carries confidential data out
SOC	A guard room staffed around the clock	The team watches all the signals, responds to alarms, coordinates actions
DFIR	An investigation team after the incident: analysis of prints and logs, questioning the guards	Investigates what happened, how the thief got in, what they stole and how to prevent it in future

INSTEAD OF A CONCLUSION:

Don’t fall for bare advertising

- Assess, consult, communicate, count everything in figures (don’t want to think — go to the pentesters)

  Without a sensible approach any tool (even antivirus) is just an expensive toy that eats money and nerves

THANK YOU

CONTACTS:

+7 (495) 909-92-78

clients@mko-systems.ru

mko-security.ru