KELA cheatsheet

07 WAYS

TO PROTECT YOUR ORGANIZATION FROM CYBER ATTACKS

EMPOWERED BY KELA

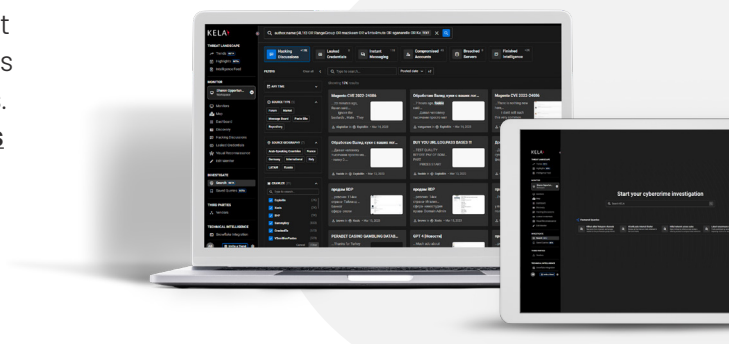
MONITOR. ANALYZE. LEARN. ACT.

The future of cybersecurity is uncertain, but one thing is clear: organizations need to adapt to dynamic cyber threat reality to meet the challenges that lie ahead. The best way to achieve this is to embrace a proactive approach to the organization's Cyber Threat Intelligence. Here are 7 simple ways to help you effectively turn your company into a threat-resilient organization.

BE THE EYES & THE EARS OF YOUR ORGANIZATION

01 UNDERSTAND HOW THE CYBERCRIME UNDERGROUND WORKS

Cybercriminals work together to share information about potential targets, develop tools and strategies for attacks and even buy and sell stolen data on illicit marketplaces. Understanding **how the cybercrime underground works** will better protect your organization against potential attacks. You will be able to see the signs of an attack before it happens and act to prevent it.



02 MONITOR CYBERCRIME SOURCES FOR COMPANY ASSETS' EXPOSURE

Embrace a proactive approach to security – actively monitor and look out for exfiltrated or released organizational assets. Invest in the training of security teams to perform cybercrime intelligence investigations. Provide them with an isolated network and dedicated workstations to perform investigations without compromising the rest of the company.

03 KNOW THE ENEMY

Learn the mindset and habits of adversaries who may likely attempt to attack your company. Analyze behavioral patterns, preferred methods of attack, areas of interest, and even personal details, if possible. This will help you anticipate their next move - and take action to protect your organization.

04 LEARN FROM PAST BREACHES

By understanding how previous attacks were executed, you can better understand the types of vulnerabilities your organization may be susceptible to. On the way, you will also learn about the different kinds of malware and hacking tools criminals use. If, for example, you know that an unsecured API resulted in a breach for another company, get all information you can about which weaknesses contributed to the attack and compare those vulnerabilities to APIs your organization uses. Often, victim organizations are willing to share details of an attack to help the security industry protect against future incidents. By building a supportive community that shares knowledge, organizations can overcome threats together and prevent attacks.

05 REDUCE ATTACK SURFACE

There are two basic ways to reduce attack surface: technical and organizational. Technical measures might include better firewall configuration, least privilege access controls and application whitelisting. Organizational measures include separating duties, so no one person has too much access, providing security training to employees and building your security plan around sound and accurate threat intelligence data. Ideally, a company would take both technical and organizational measures to reduce its attack surface. In practice, though, companies often focus on one or the other. In particular, they tend to view technical measures as more critical than organizational ones. This mindset is understandable: organizational measures are more challenging to get right. But it's a mistake. The people in an organization and the information they are armed with make a real difference in an organization's security posture.

06 PROTECT YOUR ORGANIZATION WITH THE LATEST TECHNOLOGY

Partnering with a good threat intelligence provider can be an invaluable asset in the fight against cybercrime. The provider should equip your organization with the latest tools and technologies that can help protect you from becoming the next victim, and more importantly, provide timely, ACTIONABLE, and reliable insights.

07 DEFINE GOALS AND PRIORITIZE CYBER THREAT INTELLIGENCE FOR THIS YEAR

Cybercrime underground continues expanding and growing. Threat actors are constantly searching for vulnerabilities they can exploit. The magic ingredient is to be PROACTIVE. Prioritize cybercrime threat intelligence in your organization, set goals, keep learning, train the personnel, use the right tools, and protect your data and assets from breach, theft, or exploit!

Want to learn more?

Read our cyber intelligence research updates here.

SIGN UP for a FREE TRIAL of KELA cyber threat intelligence platform.