cyberlev ins

Endpoint Detection and Response

ENTERPRISE-CLASS DETECTION, ISOLATION, AND REMEDIATION

FOR WINDOWS AND MAC

OVERVIEW

For cybercriminals, corporate endpoints, where data, users and corporate systems all come together to generate and implement business processes, remain the primary target. To protect your corporate endpoints and prevent them being used as entry points into your infrastructure, your IT-security team should be reviewing ways to boost your existing security. Implementing the full endpoint protection cycle, from automatic common threat blocking to responding swiftly and appropriately to complex incidents, requires preventive technologies supplemented by advanced defense capabilities. Cyber Lev Ins Endpoint Detection and Response (EDR) provides powerful security with comprehensive visibility across all endpoints on the corporate network together, with superior defenses, enabling the automation of routine tasks to discover, prioritize, investigate and neutralize complex threats and APT-like attacks.

EDR CHALLENGES

Attacks have doubled

Over 68% of firms suffered recent attacks and 80% were new "zero-day" threats.

High false positives

Almost 60% of firms need zero-day detection, but high false positives are a primary concern.

Complex solutions

Over 68% of firms suffered recent attacks and 80% were new "zero-day" threats.

Source: 2020 EDR Study, Ponemon Institute

THREAT HUNT AND ROLLBACK RANSOMWARE

Guided threat hunting and Windows ransomware rollback.

DEPLOY QUICKLY AND MANAGE WITH EASE

Deploy within minutes and manage with an intuitive cloud-native console.

DETECT, ISOLATE, AND REMEDIATE THREATS

Reduce risks and false positives; stop threats with multiple isolation modes.

EASY

Cyber Lev Ins Endpoint Detection and Response (EDR) for Windows and Mac can easily replace or compliment other endpoint security solutions, including Microsoft Defender. We've won high customer loyalty and praise because we're non-disruptive, straightforward, and economical to deploy via one endpoint agent, and offer robust integrations and compatibilities.

- Non-disruptive, deploy within minutes
- One endpoint agent, simple integration
- IIntuitive cloud-native management console

EFFECTIVE

Cyber Lev Ins EDR uses unique Anomaly Detection machine learning to not only detect known threats, but also find unknown threats. Cyber Lev Ins EDR boasts higher accuracy, which is why we have one of the industry's lowest false positive rates. Our granular isolation capabilities prevent lateral movement of an attack by allowing you to contain individual machines, subnets, or groups, and continue active response activities.

- Detects "zero-day" threats with low false positives
- Granular isolation for processes, networks, and Windows desktops
- Removes executables, artifacts, and changes

EFFICIENT

Cyber Lev Ins EDR offers ransomware rollback for Windows, and to avoid performance impacts, uses a lightweight agent that only requires three background processes as compared to an order of magnitude more for some other solutions.

- Single lightweight agent, no performance impact
- 72-hour ransomware rollback for Windows
- Low total cost of ownership (TCO)

INTEGRATED PROACTIVE ENDPOINT PROTECTION

Cyber Lev Ins EDR includes integrated endpoint protection and automated adaptive detection techniques that learn along each stage of the threat detection funnel. Unlike more reactive signature-based solutions that allow malware to execute before working, our endpoint protection finds and blocks threats before devices are infected. Cyber Lev Ins EDR proactively and accurately recognizes and prevents both hostile code and suspicious behavior.

OPERATING SYSTEM-SPECIFIC ISOLATION MODES

Cyber Lev Ins EDR is the first solution to provide multiple combined modes of end-

point isolation. If an endpoint is attacked, you can easily halt malware from spreading and causing harm and mitigate IT and user disruption during attacks.

- Network isolation limits device communications to ensure that attackers are locked out and malware can't "phone home."
- Process isolation restricts which operations can run, halting malware while still allowing users to remain productive.
- Desktop isolation for Windows workstations alerts users to threats and temporarily blocks access while keeping the device online for analysis.

AUTOMATED AND THOROUGH REMEDIATION

Our automated approach enables IT and security analysts to eliminate manual efforts to remediate attacks, freeing up valuable resource time. Typical malware infections can leave behind more than 100 artifacts, including files, folders, and registry keys that can propagate to other systems in an organization's network. Most solutions only remediate active malware components, such as executables, which exposes systems to reinfection (e.g; PUPs or PUMs). Proprietary Linking Engine detects and removes dynamic and related artifacts, changes, and process alterations. Our engine applies associated sequencing to ensure thorough disinfection of malware persistence mechanisms.

CLOUD SANDBOX

Cyber Lev Ins applies powerful threat intelligence to our sandbox to provide for deep analysis of unknown threats to increase the precision of threat detection and ensure prepackaged analysis of actionable IOCs. Potentially harmful malware can be detonated within the sandbox for evaluation and analysis.

GUIDED THREAT HUNTING

Threat hunting allows for on-demand and scheduled endpoint scanning for custom IOC threat investigation; user-initiated remediation scans through integrations with existing IT system management tools; and continuous monitoring for suspicious files and process events, network connections, and registry activity. Asset management capabilities collect and display endpoint details including installed software, updates, and startup programs. Visual graphs help you investigate processes spawned by a threat and determine where they moved laterally. Integrated incident response enables you to isolate and remediate all traces of a threat or globally exclude non-threatening activity—all with a few simple clicks rather than complex scripts. Cyber Lev Ins EDR collects detailed endpoint threat information for analysis and investigation to enable organizations to

search for indicators of compromise (IOCs) and go from infection to recovery within seconds.

WINDOWS RANSOMWARE ROLLBACK

For Windows platforms, Cyber Lev Ins EDR includes unique 72-hour ransomware rollback technology that can wind back the clock and rapidly return your firm to a healthy state. If an attack impacts user files, our SOC can easily roll back these changes to restore files that were encrypted, deleted, or modified in a ransomware attack. Data storage is minimized by using proprietary dynamic exclusion technology.

CONTINUOUS MONITORING

The Flight Recorder search feature in Cyber Lev Ins EDR provides continuous monitoring and visibility into Windows and Mac workstations for powerful insights. Included are search capabilities for MD5 hashes, filenames, network domains, IP addresses, and file/ process paths or names. You can also automatically display suspicious activity, view full command line details of executed processes, and store thirty days of rolling data in the cloud.

HIGH ROI, LOW TCO

With our cloud-native solution, Cyber Lev Ins EDR easily scales to meet future requirements. Our cyber intelligence expertise in remediation provides you with a solution that's powered by threat intelligence. The Cyber Lev Ins API makes it simple to integrate with SIEM, SOAR, ITSM, etc. to further drive automation and compatibility. Cyber Lev Ins EDR ensures a high Return on Investment (ROI) and low Total Cost of Ownership (TCO), and we're also known for our superior service and support.

YOUR SAFEST CHOICE FOR EDR

Cyberone enterprise-class Endpoint Detection and Response for Windows and Mac platforms effectively and efficiently detects suspicious activity, isolates attacks, investigates threats, and remediates damage. Other solutions can be difficult to deploy and manage and are usually not compatible with other security software like Microsoft Defender. Most other EDR solutions only remove executables and don't provide multiple layers of isolation to stop threats before they can cause harm. They are also designed to alert on almost every threat, which is why they have high false positive alerts. Cyber Lev Ins EDR seamlessly integrates with and is compatible with most other endpoint security solutions, including Microsoft Defender. We're easy to deploy and manage through our Nebula cloud-based console and we uniquely detect suspicious activity and isolate processes and networks to mitigate damage. Desktop isolation is also available for Windows workstations. Proprietary Linking Engine removes artifacts, chang-

es, and process alterations while providing unique 72-hour ransomware rollback for Windows workstations. Cyber Lev Ins EDR for Windows and Mac uses a single lightweight agent that does not impact performance. Don't wait until it's too late. Cyber Lev is your safest choice for Windows and Mac EDR. We've won high customer loyalty and praise for enterprise-class EDR that's easy, effective, and efficient

ABOUT THE SOC

Our SOC is 100% focused on cybersecurity. In fact, that's all we do. We are fully committed to combating cyber threats to ensure that our customers are fully protected.

Our specialists monitor more than 1,000 cyber threats every day. By investing in the best technology and the brightest geniuses in the industry, we provide effective detection, analysis and response to cyberattacks. This means that we identify the attack as it occurs and take the right steps to eliminate the risk to you and your information systems.

CONTACT DETAILS

If you are interested in learning more about Cyber Lev Ins EDR please reach out to us by phone or email and one of our experienced sales people will take the time to answer any questions you may have.

Phone: +359 882 600493, +359 2 4049840

Mail: office@cyberlevins.com