

RANSOMWARE

The Best Defense Is A Good Offense (Swift & Automated Response)

Problem:

Ransomware is running rampant. In case you've missed the latest news - ransomware is a type of malware that holds users' data files hostage until a ransom is paid. While many early variants of ransomware just locked or hid access to files, most current ransomware strains use robust public key cryptography to encrypt data on local machines or network drives. The attackers then make you pay them to get your data back. Unlike typical data breaches, ransomware is quick and easy to monetize (from the attacker's perspective) so it is gaining in popularity.

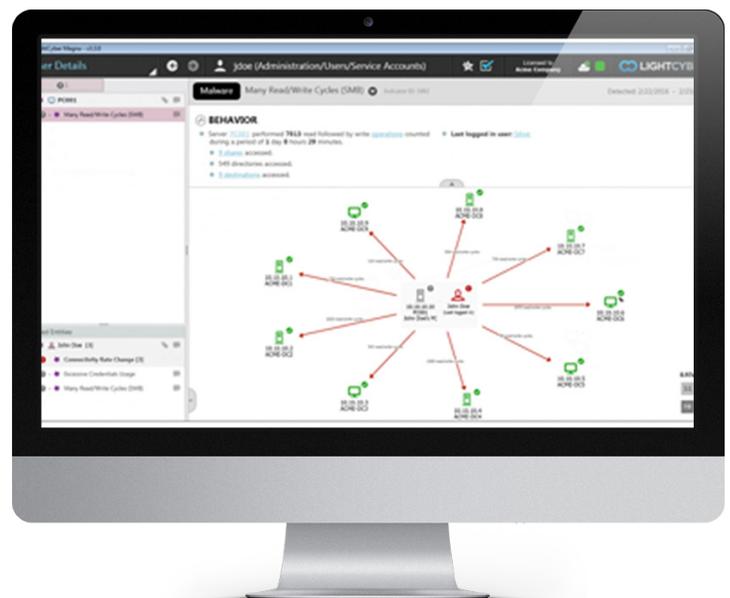
Of course, you want to prevent ransomware from infecting and encrypting in the first place, if you can... Today's reality, however, is that preventive anti-virus-style security is playing catch-up, and new ransomware variants are constantly appearing and compromising organizations, which is why we continue to see reports of new infections every day.

What's important is having an effective backstop – a plan to swiftly detect and respond to what could be a business-disrupting infection, before it proceeds too far. When ransomware impacts you, the severity of the damage (and the amount of the ransom) directly correlates to the amount of data locked up. So, if you can contain the damage by swiftly detecting and responding to active ransomware encryption activity on the network, you can limit the damage and quickly recover.

Solution:

Start with a good backup process (including securing offline backups), and make sure your systems are patched and your anti-virus is up to date. But if that doesn't work (and it often doesn't):

1. Quickly and accurately detect active ransomware. LightCyber provides a Network Traffic Analytics solution that continuously monitors internal network traffic looking for signs of malicious activity. This is not signatures- or agent-based, but instead utilizes data science to profile normal user and device activity. Then, if and when ransomware gains a foothold, LightCyber will quickly identify the anomalous pattern of file shares access and file read-write access as the malware encrypts files across the network (i.e., to networked file shares or other PC's with exposed file systems). This signature-less approach is not dependent on fore-knowledge of the specific strain of ransomware, and is thus effective even when signature-based systems such as anti-virus fail.

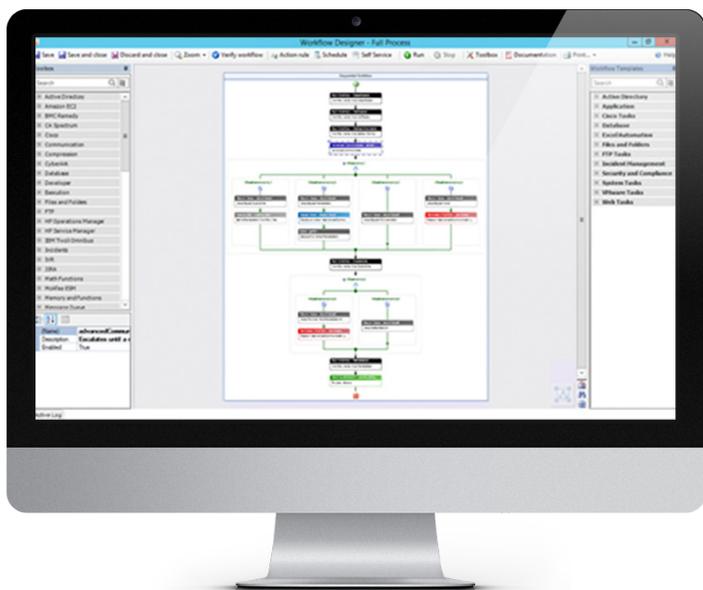


LightCyber Magna Showing Ransomware Alert – Swift response can ensure behavior does not continue for 1 day, 8 hours, and 29 minutes...

RANSOMWARE: The Best Defense Is A Good Offense (Swift & Automated Response)

2. Respond swiftly and effectively. In the case of a ransomware alert, you have an indication that damage is currently being done. Any delay means more data lost, and a higher ransom will be extorted to recover it.

eyeShare™ provides an Incident Response Automation platform that can execute workflows 24x7x365. One of the workflows can handle ransomware alerts, by isolating the damaged machine from the network, killing suspicious processes, and running anti-virus engines while getting input from the analyst or technician on duty.



eyeShare Workflow Designer



About Ayehu

Ayehu is a Cybersecurity Operations and Incident Response Automation Provider that helps Enterprise and Mid-market IT organizations improve cyber security incident response time, reduce risk, and mitigate damage from breaches by automating playbooks that enable best practice responses 24/7/365. We do this with eyeShare™, an easily deployed, industrial-strength, agentless solution that seamlessly integrates with numerous leading SIEM platforms and other security tools, like LightCyber. Gartner named Ayehu their “Cool Vendor” in IT Automation for 2016.



About LightCyber

LightCyber is a leading provider of Behavioral Attack Detection solutions that provide accurate and efficient security visibility into attacks that have circumvented traditional security controls. The LightCyber Magna™ platform is the first security product to integrate user, network and endpoint context to provide security visibility into a range of malicious activity, so it can be stopped before damage is done. Founded in 2012 and led by world-class cyber security experts, the company’s products have been successfully deployed by top-tier customers around the world in the financial, healthcare, legal, telecom, government, media and technology sectors.

LIGHTCYBER

5050 El Camino, Suite 226
Los Altos, CA 94022

Ph: (844) 560-7976
www.lightcyber.com