IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Cybersecurity

It's Time to Overhaul Enterprise Cybersecurity Alerting Systems – What Every Storage Administrator should know about their SOC

Eric Herzog

Eric Herzog
Chief Marketing Officer
Infinidat

Biography

Eric Herzog is the Chief Marketing Officer at Infinidat (https://www.infinidat.com). Prior to joining Infinidat, Herzog was Chief Marketing Office and Vice President of Global Storage Channels at IBM Storage Solutions.

His executive leadership experience also includes: CMO and Senior VP of Alliances for all-flash storage provider Violin Memory, and Senior Vice President of Product Management and Product Marketing for EMC's Enterprise & Mid-range Systems Division.

Eric blogs at https://www.infinidat.com/en/blog

Keywords Storage administrators, Cyber attacks, Cybersecurity, Storage, Immutable snapshots, Enterprise data
Paper type Opinion

Abstract

Enterprises need to make sure they are fully securing their data, both at rest and in motion. With datastores moving between on-premises enterprise data centre and the public cloud in hybrid environments, storage administrators need to be ever vigilant for a cybersecurity event and 'firing on all cylinders' if they are to have a chance of protecting their enterprise data. After all, the entire enterprise's data infrastructure security is hanging in the balance, warns the author of this article.

Introduction

Storage administrators bear a lot of responsibility for their enterprise's data. Some would argue this is one of the most challenging aspects of the administrator role. As soon as the security team gets any indication that a cyberattack may be occurring, a phone call is immediately made to the storage admin, alerting them to the threat. It's all part of ongoing, reactive efforts to protect the enterprise's mission and business-critical data. Precious minutes and seconds tick by, as this manual


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

cyberattack warning system gets underway. The storage admin just has to stop whatever it is they are doing and focus on the fact that a cybersecurity incident could be underway.

When this happens, storage administrators need to be 'firing on all cylinders,' asking the key questions and ensuring the right outcomes. In these situations, there is really only one right outcome – that enterprise data, lifeblood of all organizations today, is properly safeguarded. But will the storage admins have been quick enough to respond? Will they have succeeded in taking an immutable snapshot of all the data during that split second window? Can all the data be recovered rapidly in the event of a ransomware attack or another type of malware incident?

Hanging in the balance is their entire enterprise's data infrastructure security. Can the storage admin guarantee that a known good copy of the data is recoverable? When one examines the critical stages in this process it's clear that a great deal of responsibility is resting on the shoulders of storage administrators and their ability to make lightning fast reactions. Is that even possible? What if something else goes wrong? Automation has crept into just about every other aspect of enterprise IT, so why is it that this process and one where the stakes are especially high, is still operating in a silo and dependent on manual intervention?

The reality is that without a fully automated process to capture immutable snapshots of the data before it gets encrypted, corrupted or taken hostage through a ransomware attack, the reaction time is, most likely, simply too slow. Cyberattacks happen so fast, that the loss of even seconds to reaction times can make a significant difference to whether an enterprise can resist, withstand and

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

recover with any certainty – and instead of being the heralded as a hero, the storage admin could be slated for poor performance in the aftermath of a security incident. Is that even fair?

How could the enterprise cybersecurity alerting process be improved?

One way to ensure a more dynamically cyber resilient storage infrastructure and improve security of the entire data centre as a whole, would be to seamlessly integrate automated cyber storage capabilities into an enterprises' Security Operation Centre (SOC). Currently, this lack of integration is the missing link between data storage systems and enterprise cybersecurity. In order to reach this point, the role of storage admin needs to gain a greater organizational appreciation. Chief Technology Officers (CTOs), Chief Information Officers (CIOs), and Chief Information Security Officers (CISOs) will need a deeper understanding of SOCs and how, by linking existing security systems with enterprise storage, they can give their organizations an immense advantage when it comes to recovery from a somewhat inevitable cyberattack.

A SOC has many applications, but is broadly designed to ensure that an enterprise has the most coordinated and effective capabilities for cyber threat detection and response, as well as cyberattack prevention. As most IT professionals know, a SOC is dedicated to monitoring the enterprise's entire IT infrastructure – and they do it seven days week, 24 hours a day, 365 days a year. It is supposed to detect and respond to any security-related incident in real-time. IT is continually analyzing threat data but are missing a trick when it comes to integrating SOC and storage systems.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Enterprise storage needs to be tightly integrated into a SOC strategy, because the SOC is a control centre and unifies all the cybersecurity technologies, including the emergence of cyber resilience tech. Rather like the conductor of an orchestra. Now, due to new technological innovation, cyber resilient storage capabilities can help reduce the threat window – if the alerting triggers the right split second protection mechanisms.

What if a trigger can be defined for cyber storage to proactively take action based on a security incident?

An enterprise's security team can put all its information from security operations through an enterprise storage intelligence grid to create highly sensitive triggers that may otherwise get missed by existing technologies and techniques. IT solution providers have identified this ability to automate data snapshot commands and data pathways as critical to early detection and worry-free cyber recovery that minimizes the effects of even the most vicious and deceptive cyberattacks of malicious actors. There are three 'must haves' to guarantee rapid action:

1. Your enterprise needs automated cyber protection, utilizing triggers that security teams define based on security incidents. These may even be barely detectable aberrations that require a deep scanning of the cyber infrastructure.

2. You need an enterprise-wide cyber storage capability that orchestrates the automatic taking of immutable snapshots of data, at the speed of compute, to stay ahead of cyberattacks by creating a cyber realm to cut off the proliferation of data corruption.

3. You need an automated cyber protection solution that seamlessly integrates into SOC environments to add a powerful cybersecurity capability to an infosec teams' toolbox in the security infrastructure. It enables more dynamic monitoring that speeds up response to the start of a cyber issue and enables a "handshake" between monitoring for security incidents (the event) and expressing the fabric of core storage – the data (the outcome).

This integration of cyber resilient storage into SOC needs to be considered mission critical because the stakes are simply too high. It extends our thinking beyond traditional enterprise storage to span the layers of cyber infrastructure that need to be reshaped for today's emerging cyberattack vectors and more sophisticated AI-driven infiltration designed to inflict harm to enterprises.

Today it's less a question of 'if' a cyberattack will take place and rather a matter of 'when.' It's time for enterprise storage to stop being relegated as a backroom function and it's time to 'put a SOC' into it.