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 our main website at **www.creditcontrol.co.uk**.

IT Security

Scene of the Crime – Why Visibility and Forensics Matter in Cybersecurity

David Shefter

David Shefter
Chief Technology Officer
Ziften

Biography

David Shefter joined Ziften (https://ziften.com) as Chief Technology Officer from Citigroup, where he was SVP of Innovation and Emerging Technology. David is responsible for Ziften's long-term technology vision and strategy, strategic technology partnerships, and technical product strategy.

David is a seasoned executive with over 20 years of experience in technology and financial markets, having held SVP and related senior positions at Citigroup, IBM, DEC, Merrill Lynch, and several start-ups in the hosting, web services, consulting and legal industry spaces. In his career, he has been personally responsible for a portfolio of solutions that have generated over $1 billion in revenues and millions of dollars in savings. He has an expansive record of driving innovation initiatives, while providing vision and operational expertise in creating expanded capabilities. A leader in expanding the relationship of IT across a varied business landscape, David provides strategic direction in technologies and systems for high visibility environments in support of business initiatives.

He holds a BA from Pace University.

Keywords Endpoint Detection and Response (EDR), Security Operations (SecOps), Advanced Persistent Threats, Endpoint Visibility, Security forensics, Threat hunting, Systems and Security Operations (SysSecOps)
Paper type Research

Abstract

The threat posted by Advance Persistent Threats is growing, and research shows that organizations need to rethink their security models, and you can't find the root cause of problems if the data isn't available. In this article, the author explains why organizations need a Six-Point Checklist for making sure that their security teams have the capacity to track the root causes and progress of noxious malware.

Introduction

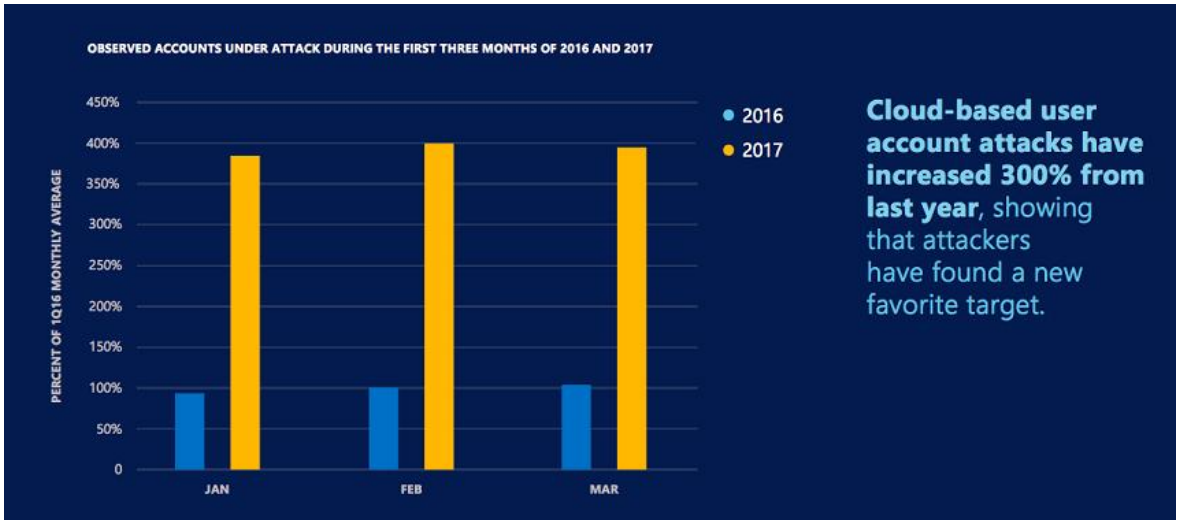
In the fight against Advanced Persistent Threats (ATPs), ranging from ransomware to malware and other destructive attacks, enterprises need a heightened ability to detect, view and investigate using forensics. What's more, they need to quickly respond to advanced hacks and attacks on the most popular operating systems, be it mobile, desktop, cloud, virtual machines – or containers and microservices.

Visibility must reach far and wide. Today the cloud has become a major attack vector. According to Microsoft's latest research[1], the security intelligence report (SIR), there has been an upsurge of 300% on cloud account attacks from 2016 to 2017.

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 our main website at **www.creditcontrol.co.uk**.

Figure 1: Observed accounts under attack during the first three months of 2016 and 2017



Considering the widening scope of cyber threats, security operations staff, whether they are part of a CISO organization or embedded within IT, will benefit from using a comprehensive systems and security operations platform to detect attacks and zero-day exploits, to uncover the full scope of a breach, and to quickly respond to attacks.

The Six-Point Checklist

Do your security teams have these enterprise-wise forensics capabilities?

1. Single source of truth visibility into every asset – laptops, desktops, servers, virtual machines, containers?

2. Continuous, rich data collection and storage from every managed endpoint including systems, user behaviour, network connectivity, application, binary, and process data?

3. Continuous device state and behaviour monitoring; real-time issue, threshold, and threat-based alerting and ticketing?

4. Actionable data from threat feeds, whether open-source or commercial?

5. Advanced threat detection and hunting capabilities across Windows, Mac, and Linux systems, including client devices, data centre, and cloud?

6. Capabilities for deep binary/file analysis and sandboxing of suspicious packages?

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 our main website at **www.creditcontrol.co.uk**.

What about forensics?

Forensic analysis in the cybersecurity world is typically performed as part of a scheduled compliance, legal discovery, or law enforcement investigation. Forensics provide a full understanding and thorough remediation of a breach. Deep forensics data accelerates tracking attacker's lateral movements and provides retroactive alerting on all systems that exhibit or have exhibited similar behaviours. Most importantly, forensics can identify the root cause of an issue to help close the gaps and stop future attacks across the entire environment.

The capability to conduct a six-month review of activities that have occurred on an endpoint, such as a desktop, smartphone, server, or virtual machine, is crucial to knowing what has occurred and how an attack has taken shape, and to evaluate the potential for harm to other places or users throughout the IT infrastructure. This is why security systems should store a minimum of half a year's worth, if not more, of robust forensic data storage.

Forensic analysis is a central discipline that can leverage the same tools and related data sets as incident response management, and then go beyond it. A thorough forensic investigation allows the remediation of all threats with the careful analysis of an entire attack chain of events. And that is no laughing matter. For this purpose, forensics research requires strong log analysis and malware analysis capabilities.

While interactions for threat containment are performed with other security and operations team members, forensic analysis typically requires interactions with a much broader set of departments, including operations, legal, HR, and compliance. This is when the attack transcends from a technology problem to a business problem, with repercussions ranging from lawsuits to a loss in reputation among stakeholders, such as investors and customers.

Conclusion

Following the storm of serious global cyber attacks in 2017, it is now widely understood just how damaging not having a well designed approach to security can be for enterprises. Only when IT departments, SecOps teams and the company as a whole take a "systematic" approach to security to incorporate visibility and forensics for prevention, along with the other critical functions of cybersecurity, can the challenge be overcome.

Reference

1 https://www.microsoft.com/en-us/security/Intelligence-report