incenter

TABLE OF CONTENTS

Introduction 3
Increased Attack Surface 3
Efficiency Through Prevention Over Detection 4
Consolidation of Security Tools 4
Decreased Workload and Increased Efficiency 5
Challenges Adhering to Compliance 6
Conclusion 6
Bibliography 7

INTRODUCTION

After years of meticulous research and development, OccamSec LLC introduced the Incenter platform. Created with the integration of AI, the Incenter platform is the most current and innovative security solution for continuous threat exposure management (CTEM), seamlessly merging cutting-edge automation technology with human expertise to resolve the most critical of cybersecurity issues.

While only 15% of companies believe they are ready for a cyberattack, over 82% expect an attack[1]; this expectation is justified by the reality that there is a malicious cyberattack every 39 seconds. However, organisational cybersecurity teams face a multitude of challenges in the rapidly evolving threat landscape.

These challenges include difficulty in detection, alert fatigue, and expanding attack surfaces. In addition, security teams are inundated with an excess of security tools and vendors. Organisational risk is further impacted by larger supply chains, remote work, and increased activity by threat actors.

Incenter was developed to overcome the challenges faced by organisations in breach prevention through continuous threat management. A milestone in the realm of preventive tools, the Incenter platform provides organisations a versatile approach to counter a wide spectrum of attack vectors through the convenience of a single tool.

INCREASED ATTACK SURFACE

In recent times, there has been a change to embrace remote work, which consequently has had repercussions on our cybersecurity.

There is an increased attack surface and less protection working from home, with 20%[2] of companies affected by a data breach via remote work. Companies that adopted the remote work model paid roughly $1 million more[3] to recover from data breach damages compared to companies without remote work clearance. Being

outside of a company's perimeter and defences leads to more exposure and a higher risk.

Incenter helps to proactively mitigate the increased attack surface, risk, and exposure that we now remotely face. Through a combination of automation and manual penetration testing, Incenter can detect high-risk vulnerabilities within your environment before they are exposed to malicious actors.

EFFICIENCY THROUGH PREVENTION OVER DETECTION

The overwhelming majority of cybersecurity attack costs go toward detection, recovery, and remediation. On average, it takes 287[4] days to detect and contain a data breach with a substantial financial investment made into remediation while over 70% of respondents[5] identified prevention as a better tactic than detection. The economic benefit of cybersecurity prevention is estimated to be between $400,000 to 1.4 million depending on the attack vector.

With a proven track record of preventing attacks before they occur, Incenter saves time in detection, remediation efforts, and containment while also minimising financial risk. Through continuous manual testing and robust automation, Incenter detects vulnerabilities and provides remediation details to prevent attacks before they occur.

CONSOLIDATION OF SECURITY TOOLS

Acknowledging the evolving capabilities of threat actors and the costs of a data breach, organisations invest in more than 45 tools on average. Even so, 53% of IT firms[6] were unsure of the effectiveness of their tools despite expending $18.4 million a year on their usage. Acquiring more tools does not equate to more efficiency, and organisations continuously spend millions for an overflow they never use.

The reduction of vendors and tools equates to both financial savings and a higher degree of security through the minimisation of attack surface. The more tools an organisation deploys, the more time is spent in management, oversight, and administration while also negatively impacting cybersecurity budgets.

Incenter is a complete offensive security solution, allowing for the reduction of vendors and tools. Fusing automation technology with CTEM capability, Incenter is cost-effective, comprehensive, and user-friendly, removing the inclination for additional tools. With Incenter, organisations will be assured of their investment in seeing its multi-faceted and dynamic capabilities, as Incenter detects and identifies vulnerabilities across API's, cloud services and web and mobile applications.

DECREASED WORKLOAD AND INCREASED EFFICIENCY

Despite the significant and concerted investments organisations pour into cybersecurity, chief information security officers (CISO) are resigning in record numbers. The pressure has become tremendously crushing, with 32% of CISOs considering leaving their positions due to an inability to withstand the workload and expectations set upon them, as well as an ineffectual tool arsenal. Organisation security personnel are getting burnt out, and this weakens the infrastructure of our security with less individuals too dispirited to defend it. Concurrently, smaller companies with less than 100 employees are 350% more likely[7] to sustain a cyberattack or breach compared to companies with a larger staff.

The Incenter platform is the solution for staff shortages and employee discontent, While Incenter utilises advanced automation capabilities to streamline data and free up inventory management, Incenter needs human expertise to supervise the AI. Human talent is invaluable in the field of cybersecurity, and it is unrealistic to rely on AI alone. Incenter integrates human and machine in a perfect balance, reducing the stress levels and workloads of already strained IT security departments and ensuring small and large-scale businesses maximum success.

CHALLENGES ADHERING TO COMPLIANCE

Organisations large and small face an uphill battle in adhering to cybersecurity compliance. On average, organisations lose $5.87 million[8] in revenue from a single non-compliance failure as non-compliance costs have increased by 45% since 2011. The rapid pace of technological innovation, alongside increasing regulations and non-compliance costs, poses challenges for companies, placing the burden on internal stakeholders to bridge the widening gap.

Incenter's breakthrough technology boasts state-of-the-art features, adhering to the latest security regulations to help organisations avoid penalisation and navigate the complex territory of compliance. Incenter simplifies penetration testing for the regulatory process with continuous testing and resilient automation abilities, ensuring strict adherence to GDPR, HIPAA, PCI DSS, FISMA, and ISO/IEC 27001 regulations.

By incorporating Incenter, organisations follow compliance practices while continuously fortifying a strong security posture.

CONCLUSION

Incenter is a large step forward in revolutionising cybersecurity tools via AI, automation, and expert human intervention. With a proven track record, Incenter is at the forefront of CTEM and attack and breach prevention.

Through Incenter, organisations can bolster a proactive and preventative security program that will reduce overall risk and costly investments in detection and breach mitigation. Offering a simplified, user-friendly, cost-effective solution, Incenter stands unrivalled in CTEM performance and automation, designed to assist you in achieving and upholding the most robust security posture as easily as possible.

Empower your organisation with Incenter.

BIBLIOGRAPHY

1. Cisco. (2023). Cisco Cybersecurity Readiness Index: Resilience in a Hybrid World.

https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-index-report.pdf

2. Cisco. (2023). Cisco Cybersecurity Readiness Index: Resilience in a Hybrid World.

https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-index-report.pdf

3. Malwarebytes Inc. (2020). *Enduring from Home: COVID-19's Impact on Business Security*. https://www.malwarebytes.com/resources/files/2020/08/malwarebytes_enduringfromhome_report_final.pdf

4. IBM Security, Ponemon Institute. (2022). *Cost of a Data Breach Report 2022*. *https://www.ibm.com/downloads/cas/3R8N1DZJ*

5. IBM Security, Ponemon Institute. (2022). *Cost of a Data Breach Report 2022*. *https://www.ibm.com/downloads/cas/3R8N1DZJ*

6. Deep Instinct, Ponemon Institute (2020). *The Economic Value of Prevention in the Cybersecurity Lifecycle*. https://info.deepinstinct.com/value-of-prevention

7. AttackIQ, Ponemon Institute. (2019). *The Cybersecurity Illusion: The Emperor Has No Clothes*.

https://go.attackiq.com/PR-2019-PONEMON-REPORT_LP.html

8. Barracuda Networks. (2022). *Spear Phishing: Top Threats and Trends*. https://www.barracudamsp.com/resources/reports/spear-phishing-threats-and-trends#:~:text=Spear%20phishing%20is%20a%20threat,business%20email%20compromise%2C%20and%20blackmail.

9. Globalscape, Ponemon Institute. (2012). *The True Cost of Compliance with Data Protection Regulations*.

https://www.globalscape.com/resources/whitepapers/data-protection-regulations-study