

Security Intelligence

AN EVOLUTIONARY APPROACH TO NETWORK SECURITY

Security Intelligence (SI) is an emerging information security discipline that seeks to recognize and understand sophisticated cyber adversaries, specifically why and how they threaten data, networks, and business processes while also developing better protective measures against them.

SI is defined as a threat-focused approach to cyber security where defensive strategies and solutions are driven by knowledge of sophisticated threats to business operations and networks.

The process of SI is similar to that of traditional business or military intelligence disciplines:

- Data is collected and analytic tradecraft is applied to develop usable threat intelligence.
- SI applies methodologies to develop a comprehensive understanding of adversaries by categorizing and classifying indicators of malicious activity to specific threat activity groups.
- This comprehensive knowledge is then used to make security decisions at all levels providing valuable input into proactive development of defensive countermeasures, focused incident responses, and driving remediation efforts.

Recent national media coverage of network intrusions perpetrated against the government, large defense contractors and commercial corporations attest to the fact that even the best resourced Information Assurance (IA) and network security teams cannot defend against sophisticated threats to their networks.

With an improved understanding of an adversary's capabilities and intent, SI individuals or teams work closely to create a feedback loop with network security and engineering teams in order to implement effective and timely remediation and countermeasures.

Not only does SI greatly diminish adversary efficacy, but it also lowers security costs by defending against individual real-world threats instead of applying a shotgun approach to unquantifiable potential scenarios. Since intrusions are less successful, remediation and clean-up expenses are less costly.

As use of SI grows, organizations are better able to factor lessons learned into defensive strategies that will prevent follow-on intrusions and persistent network exploitation.

Threat and Defensive Evolution

Existing cyber threats have evolved in complexity, while new threats with varying motivations, sophistication and capabilities have also emerged in the ever-changing cyber environment.

In the past decade, we have witnessed the emergence and rapid growth of Advanced Persistent Threats (APTs) and other sophisticated threats that are forcing an evolutionary shift in Computer Network Defense (CND), Information Assurance (IA), and Incident Response (IR) methodologies.

“Not only does SI greatly diminish adversary efficacy, but it also lowers security costs by defending against individual real-world threats.”

The motive of such cyber adversaries thus far has been to conduct cyber-espionage to steal diplomatic, industrial, military or economic data, but could evolve into more destructive motives such as seeking to deny, degrade or disrupt networks in a turbulent geo-political landscape.

True to their name, these sophisticated cyber adversaries do not give up easily. They are resourceful. They tend to quickly develop new measures and techniques in an effort to reacquire access when an organization's defensive strategies are successful. While this stubborn tenacity is the most frustrating aspect of these groups, it can also be their weakness. Just as a criminal that continues to come back and rob the same bank will soon be caught, so it is with APT when SI principals are employed. Cyber adversaries utilize an intelligence-led approach to steal sensitive data; sufficient and effective countermeasures likewise require an intelligence led-approach. SI provides a disciplined approach, intelligence tradecraft and technological advancements to effectively counter dynamic and evolving threats. SI is effective because adversaries are limited by available resources, skill level and human tendencies that form identifiable patterns of activity. With SI, it is possible to map the adversary's methods and techniques and then track, understand and ultimately mitigate them.

Why SI is Superior to Traditional IA

Traditional incident response procedures do not sufficiently capture or fully understand indicators gathered from a cyber attack that may be critical to preventing future incidents. Nor do they sufficiently capture the intent of the adversary, which is of great help in developing methodologies to direct defensive postures and investments within the network to strengthen protection around network "centers of gravity" (detailed later).

Highly publicized reports of sophisticated attacks into government agencies, non-profit, defense industry and increasingly commercial companies are more and more frequent. Advanced threats continue to undermine certified and accredited networks that contain up-to-date antivirus, patched systems and applications. They penetrate hardened security architectures that use time-tested security best practices, including public key infrastructure, access controls and cutting-edge commercial security solutions.

Effective information security can no longer be carried out solely by engineering or administrative staffs. A technical staff on its own cannot effectively mitigate a persistent nation-state-sanctioned or sponsored cyber threat over the long term. Therefore, traditional IA is significantly outpaced by increasing technical complexities, globally interconnected network reliance, and shifting geo-political winds.

How SI Enabled Protection Works

In past decades, security problems were often solved with technical and physical security solutions aimed at keeping the network secure. Traditional perimeter-based security models address access controls, policies and countermeasures to keep threats outside of the network. The traditional "defense in depth" model creates hardened layers, which protect network assets from unauthorized access.

"Advanced threats continue to undermine certified and accredited networks that contain up-to-date antivirus, patched systems and applications."

While such models are still applicable, they need to be adapted and extended in order to protect not only the network but also the logical extensions outside of the network as more and more organizations move applications and data to external clouds and servers. Ultimately, the attackers are not after your network, they are after your information. An attack seeks information from within your network or from sources outside of the network such as home VPN users, private and corporate web mail, or business partners.

Persistent threats have demonstrated a consistent ability to easily penetrate networks or gain access to sensitive information elsewhere, so the need to stop threats at the network perimeter has now become the need to conduct secure business operations alongside the adversary.

Instead of being thought of as a boundary, the network should now be considered contested space. This is an unsettling truth. Companies must accept that the goal is no longer to secure your network, but to secure your information and business processes; this is a necessary paradigm shift for understanding how to effectively deal with cyber threats. Once realized, SI can make this goal a reality.

SI consistently delivers knowledge about the nature of advanced threats and their perpetrators, providing details about why they are operating in the network, how they operate, and what they are after. Armed with this insight both business and technical decisions can be made and IA staff can develop strategies to manipulate the virtual domain of remote attackers. It is within this virtual space that SI supports traditional IA by focusing resources on targeted countermeasures that lower the efficacy of advanced threats. These countermeasures vary from network to network but can be identified when you know what the critical resources are, both virtual and physical, that your adversary must utilize to steal data or damage systems. These critical resources are effectively centers of gravity for the adversary's operation against your network.

Conclusion

Resourced and targeted attacks will continue to become more prevalent. They have long ago ceased to be a problem affecting just the government and military. In today's world, cyber espionage is a fact of life in the commercial and private sectors.

Cyber threats will not and cannot be stopped. They can only be deterred, and contained, and their resources exhausted. Within a contested network, today's defenders must have an intimate and doctrinal understanding of the remote adversary in order to quickly implement creative and innovative countermeasures with limited resources.

Business leaders and their technical cyber defense staff must use SI to understand today's sophisticated and persistent cyber threats or risk loss or revenue, embarrassment and operational interruptions.

“ Ultimately, the attackers are not after your network, they are after your information. An attack seeks information from within your network or from sources outside of the network such as home VPN users, private and corporate web mail, or business partners.”

About Cyber Squared Cyber Squared Inc., headquartered in Arlington, VA, protects critical information and strengthens network security for organizations that are targeted by sophisticated cyber adversaries. With a superior understanding of the relevant cyber threats to the clients' business operations, our security intelligence services can determine risk and develop individualized, effective security strategies and processes for risk avoidance. This, coupled with our capabilities in disrupting sophisticated threats, gives our clients an unparalleled ability to characterize and respond to the threat, and be more proactive in their day-to-day security operations. Contact Cyber Squared or visit www.cybersquared.com for more information.



Contact Cyber Squared Cyber Squared welcomes your questions, comments, and general feedback.

Email: info@cybersquared.com

Website: www.cybersquared.com

Phone: 703.224.4418

Toll Free: 1.800.965.2708

Fax: 703.852.3463