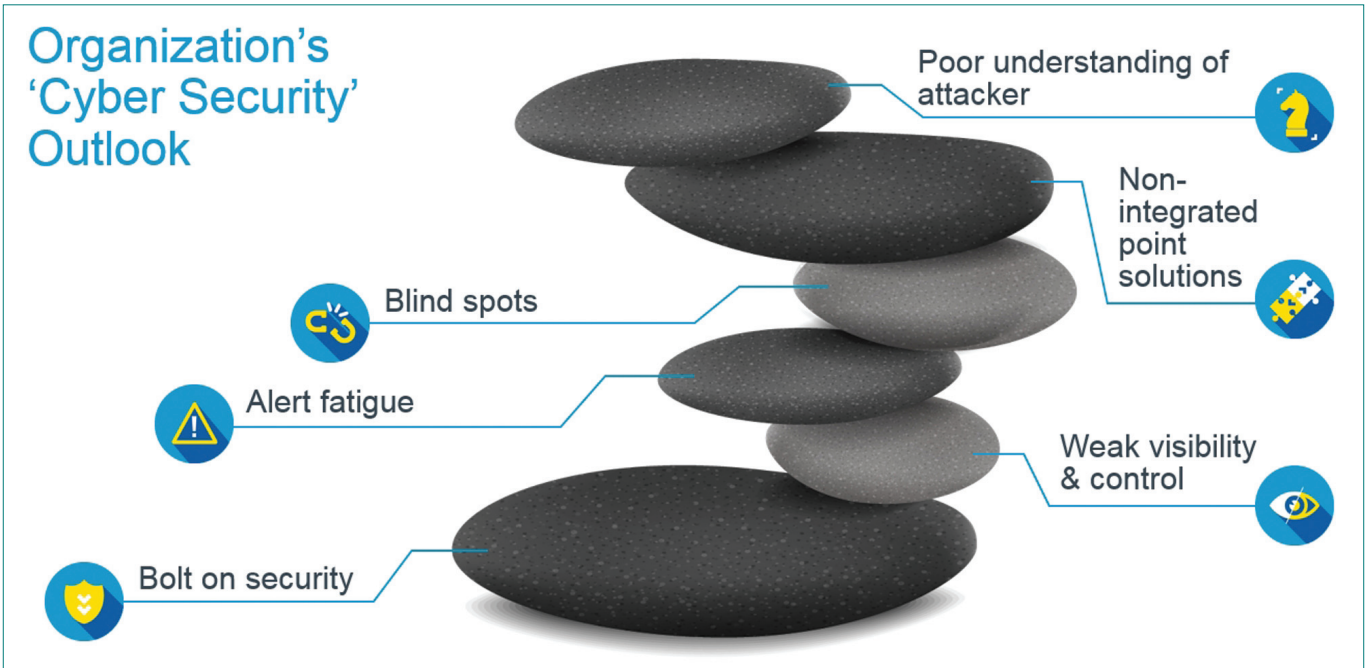


The Language of Deploying Tools vs the Language of Deploying Strategy

Militaries must switch from cyber security to cyber defense

In 2008, the US military woke up to a growing new threat to its computer networks. An infected flash drive was inserted in a military laptop in the Middle East with the aim of delivering classified data to unknown foreign adversaries. Then, Deputy Defense Secretary William Lynn called the incident a "digital beachhead" - an event that prompted new counter-attack strategies. It's now almost 10 years later, and cyber terrorists have developed ever more sophisticated ways to infiltrate networks and steal valuable military secrets. Experts agree that it's time to move from a cyber security to a cyber defense mindset, as explained by Noam Rosenfeld, SVP, Cyber Intelligence Solutions at Verint Systems Ltd.

Most organizations approach cyber security this way: Layer upon layer of bolt-on solutions, built year after year, without a clear, integrated strategy behind them. The problem with this unstable security structure is four-fold. One, it can be breached and collapse easily. Two, it will enable security analysts to detect specific malwares - maybe even understand the tactical picture - but it won't reveal the attacker's overall strategy, so they can't predict the next steps. Three, it won't show the full picture of the organization's weak spots. Lastly, while deploying a lot of point solutions, this approach won't enable a single picture that fuses all this information together - this approach leads to lack of visibility and poor command and control.

Making the shift from a *security* to a *defense* state of mind to achieve better cyber solutions is no small matter. It's a tactical versus strategic issue. Most military security infrastructure is focused on compartmentalized security solutions that give a tactical picture, but don't give the overall big picture explanation of the enemy attack strategies deployed and why these strategies were selected – what vulnerabilities they discovered and exploited e.g. the weak spots in the current military attack surface.

Approaching today's cyber challenges from the tool deployment perspective is important, but it doesn't provide the intelligence necessary to devise a strategy to win the cyber war. After all, guarding military (or business) networks, weapons systems, and secrets requires a thorough, nuanced system based on intelligence, operational ability, and technology, not a one-dimensional security solution.

It's also essential to remember that both military and commercial organizations often face *hundreds of thousands* of attacks a day, some of them state sponsored and well financed.

If you're ready to switch to cyber *defense* and speak the language of *strategy*, know that a quality defense strategy is built on the combination of three things: Intelligence, operational ability, and technology - each complementing the other and with the right ploys and processes to manage them.

Intelligence

Effective cyber defense necessitates an in-depth knowledge of the defense capabilities and the attacker's capabilities and the organization's attack surface (the potential penetration points in the defender network) that attackers target to enter data to or extract data. In other words, the defense commanders and their teams need to create and analyze a detailed intelligence picture that includes:

1. Thorough understanding of the attacker's strategies and attack methods, not just the malware used. After all, malware is just a tool. It's not the about hammer, it's about the attacker wielding the hammer.
2. Keen awareness of the organization's current human abilities: Is the security staff capable of dealing with the increasing sophistication and volume of attacks?
3. Detailed knowledge of the organization's attack surface, particularly its weak spots among the 'crown jewels' and other key areas.

Operational ability

Now that you've gathered your intelligence, what do you do with it? Operational ability is the set of sophisticated actions the defense operations team needs to take using both intelligence and technology. This usually includes a range of ploys or tactics, and organizations who want to succeed in operational ability must develop skills in:

1. Proactively searching for the attacker, using specially created teams with investigative skills - Red teams to find your weak spots and hunt teams to find the attackers (response teams are utilized during the response phase).
2. Easily compartmentalizing the network to contain an attack, a skill that requires intimate knowledge and planning of the network.
3. Dynamically changing the attack surface to disrupt the attacker, for example, dynamically changing IPs or passwords.

Operational ability also includes building two additional defense layers in addition to strengthening existing defense on the home front – the internal network, so organizations don't meet the attacker for the first time inside their networks - and incur high damages.

1. Front-end Layer – Located outside the organization classified network, this could be honeypots on the Internet, several tools in ISPs, or other activities of special teams that work according to targeted intelligence.
2. Organizational Perimeter - Organizations can use internally developed tailor made solutions that the attacker can't buy and try to bypass. He can only try to bypass them when they are already installed. This layer also minimizes access to the classified network by the organization's suppliers, allowing better control and management.
3. The Home Front - This area consists of military networks (Army, Air Force, Navy, etc.) where you can use layered defense - differentiating between users, applications, infrastructures. By applying dynamic defense based on changing the 'attack surface,' you will be better able to defend the crown jewels of confidential military data.

Technology

You may have the best intelligence and the most effective operational capabilities, but without the right combination of technologies, you can't win. Optimum technological solutions work synergistically to give you the ability to execute an operational concept. In cyber defense, the main operational concept is to morph from being hunted to being the hunter.

So, how can we accomplish this? An attacker has close to infinite ways to reach the target, but one thing is always constant - an attack chain that has clear, consecutive stages. Thus, it is critical to spread point solutions along the attack chain, but it is more important to collect and fuse the 'digital footprints' that the attacker leaves over these point solutions.

So, when building or upgrading a Cyber Security Operations Center and selecting the prime technologies, ensure that the combination:

1. Is sensitive enough to identify even a 'single' mistake the attacker makes along the attack chain.
2. Has the width and depth to detect and prevent attacks on the internal network and across the organization's business ecosystem.
3. Contains one place that fuses all the cyber sensors to create a picture of all the attack dimensions, enabling you to act and act effectively.
4. Includes automatic investigation to help reduce the incident/alert ratio and turn many alerts into a handful of meaningful incidents.
5. Includes a decoy mechanism to force the attacker to make mistakes and leave digital footprints.

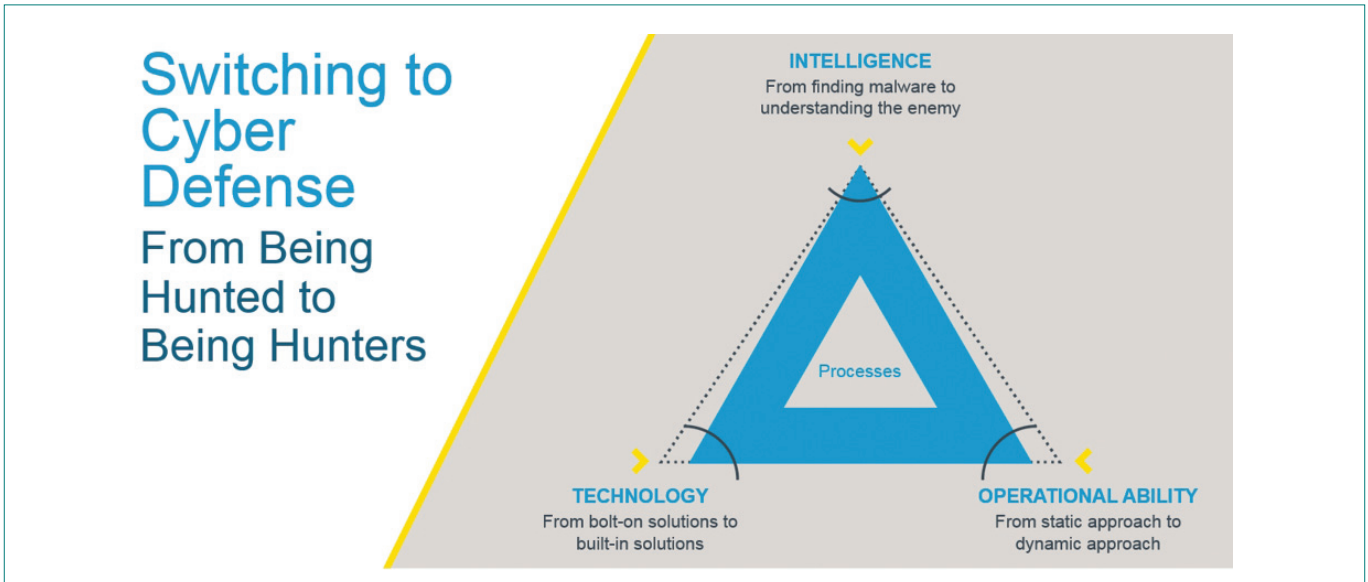
Worried about the financial implications of implementing these three pillars into your cyber defense strategy? Just consider the cost of a critical breach in terms of potential casualties when they have access to your critical assets or weapons systems.

How next-gen solutions advance your cyber defense strategy

In today's cybersecurity market, you'll find an abundance of point tools, some of them very mature and advanced, that focus either on detection, prevention, remediation, etc.

But next-generation technology looks beyond individual solutions and meets the cyber challenge more holistically. In fact, the ideal answer is a full-platform solution that blends intelligence and technology - a combined man/machine operational ability that outsmarts the attacker. The next-gen solution will contain not just technology in a box, but also a strategy in a box, helping security professionals manage strategy using automated and prediction tools.

Now that would really be a cutting edge cyber defense arsenal. **GMC**



Switching to Cyber Defense: From Being the Hunted to Being the Hunter