# מודיעין סייבר

**דדי גרטלר**

## תקציר עברי

התקפות סייבר נמצאות בעלייה! יריבים ברחבי העולם מנסים לקבל נתונים טכניים, פיננסיים, אסטרטגיים, וביטחוניים לאומיים מממשלות, תעשייה פרטית, ספקי התשתיות שלנו, כמו גם אזרחים פרטיים. תוקפים משתמשים בשיטות מתוחכמות יותר ואגרסיביות הדורשות אמצעים תקיפים באותה מידה כדי לזהות, להגיב, ולהסתגל במהירות לאיומי סייבר חדשים שעלולה לסכן את הביטחון.

האויב הוא צופה. ארגונים כמו חברות גלובלית, תוכניות שירות על תשתיות קריטיות ותשתית טכנולוגיית המידע של הממשלה נמצאים בסכנה. סביר להניח שהאויב הוא כבר בפנים ואיסוף נתונים על הרכוש של ארגון, עובדים ולקוחות אינטלקטואליים. טכניקות "דייג" משמשות למצוא חולשות שיאפשרו לפתח התקפות ביום מסוים ולחדור לרשתות יעד. צבאות של רובוטים פגעו בארגונים מצדדים שונים בדרך שקשה לתאם ולהגן. חומות אש מתוגברות בצוותי פיקוח, בקרה על יומני פעילות והתראות אינן הגנה מספיקה כדי להגן על הנכסים הקריטיים ביותר. האמת היא שחברות וממשלות לא יכולות להגן באופן סביר על התשתיות שלהם הטכנולוגיות ועל המידע והנתונים באמצעות הפתרונות של אתמול מפני איומים המתוחכמים של היום.

מה שארגונים חסרים הוא מרכז מבצעי Cyber Security עם תהליך מתודולוגי, כלי ניתוח מתקדמים, טכנולוגית BIGDATA וזרימת עבודה אוטומטית לאירועים שאינם קשורים לכאורה להתקפה הקרובה.

יכולת מודיעינית מאפשרת לארגונים לזהות איומים ונקודות תורפה פוטנציאליים כדי למזער את "חלון התקפת איום" ולהגביל את כמות זמן גישת היריב לרשת לפני שהוא מתגלה. ארגונים שמאמצים גישה זו מבינים שאיום היא אינטליגנציה והמנגנון שמניע את השקעת אבטחת סייבר וניהול סיכונים תפעולי.

בעוד עלייה במודעות של איום אבטחת סייבר היא במגמה חיובית, אינדיקציות מראות כי ארגונים רבים עכשיו צריכים להתמקד בניהול המודיעין כדי לקבל ערך אמיתי מאיומי המודיעין. זה יהיה תנאי מוקדם להקניית ביטחון בחברי דירקטוריון, רגולטורים והמנהלים על מנת להבטיח שהארגונים מצוידים להתמודדות עם האתגרים הולכים ומתפתחים של אבטחת סייבר.

ניתן ללמוד הרבה מאכיפת החוק וארגוני מודיעין. הם הכירו בזמן שקבלת החלטות נשענת על מודיעין יושבת בלב התרבות הארגונית שלהם.

העקרונות הבאים יעזרו לארגונים לנהל את האיום הקיברנטי באופן יזום ולמזער את הסיכון ללקוחות, בעלי מניות ועובדים:

- להוסיף סיכוני סייבר למדיניות ניהול סיכונים שלה
- יישום מודל תפעולי ביטחוני מרכזי בצורה של SOC
- בניית תהליך קבלת החלטות כאשר המודיעין במרכזו

Intellitech Ltd.

Intelligent Consulting

# Intelligence-Led Cyber Security Operation Center (CSOC)

*Next Generation Cyber SOC for Governments, Global Enterprises and MSSPs*

April 2015

# Intelligence-Led Cyber SOC

*Next Generation Cyber SOC*

## Introduction

Cyber-attacks are on the rise! Adversaries around the globe are attempting to obtain technical, financial, strategic, and national security data from governments, private industry, our critical infrastructure providers, as well as private citizens.

Attackers are using more sophisticated and aggressive methods that require equally assertive measures to detect, respond, and quickly adapt to new cyber threats that may jeopardize security.

The enemy is watching. Organizations as Global Enterprises, Critical Infrastructure Utilities and Government's Information Technology infrastructure are compromised. Most likely the enemy is already inside and collecting data on organization's intellectual property, employees and customers. Phishing techniques are used to find weaknesses as the enemy develops zero-day attacks to penetrate target networks. Armies of bots hit organizations from different sides in a way it is hard to correlate and defend.

Running a Firewall, IDS/IPS and a SIEM with a staff to periodically review logs and alerts is not a sufficient defense to protect the most critical assets. The truth is that Enterprises and Governments can't reasonably defend their information technology infrastructure and data using yesterday's solutions against today's sophisticated threats.

What organizations are missing is a Cyber Security Operation Center with an Intelligence process and methodology, the advanced Analysis tools, Big-data technology and automated workflow to correlating seemingly unrelated events into a map of a coming attack.

An intelligence capability enables organizations to identify potential threats and vulnerabilities in order to minimize the 'threat attack window' and limit the amount of time an adversary gains access to the network before they are discovered. Organizations that take this approach understand that threat intelligence is the 'mechanism' that drives cyber security investment and operational risk management.

While increased awareness of the cyber security threat is a positive trend, indications show that many organizations now need to focus on putting in place the fundamentals of intelligence management to gain real value from threat intelligence. This will be a pre-requisite for instilling confidence in board members, Regulators and managers to ensure that the organizations are equipped to meet the ever-evolving challenges of cyber security.

Much can be learned from law enforcement and intelligence organizations. They have long recognized that intelligence-led decision making sits at the heart of their organizational culture and operations.

The following principles will help organizations manage the cyber threat proactively and minimize the risk to customers, shareholders and employees:

- Add Cyber Risk to its Risk Management policy
- Implement a central security operating model in form of SOC
- Build an intelligence-led decision-making process

With Cyber Security Operations Centers(CSOC) reporting a record number of incidents and threats originating from all directions – external (syndicated crime, foreign intelligence agencies, activists); internal (disgruntled employees, unintended disclosures); and supply chain (counterfeit hardware, unsecure software, poor coding practices), Chief Information Security Officers (CISOs) can no longer just be security subject matter experts. Under the new Cyber Risk Management and Cyber Intelligence Ecosystem, CISOs will be looking at the whole organization in determining ways to enhance its security and business continuity.

Building and operating a successful CSOC is a crucial step many organizations have to take this days in order protect their assets, manage risk and achieve better business continuity, however, most of the organizations cannot afford the effort. The barriers to entry are high from the following reasons:

- **Budget** - Building and operating an effective CSOC requires the organizations to heavily invest in hardware, software and human resources
- **Time** – Building and operating an effective CSOC requires the organizations to plan and manage a long and complex IT integration project with many risks involved
- **Knowhow** - Building and operating an effective CSOC requires the organization to recruit a professional team of experts with strong technical skills and strong cyber security methodology which are rear to find.

Following the given barriers of entry the two new market verticals have been created:

1. **Managed Security Service Providers (MSSP)** – Security service providers utilizing a common IT infrastructure set of product, own designed and build based on Cloud services to offer professional Cyber Security as a Service (SaaS) to as many customers as possible. There are MSSPs in all size and level (Global, National, Local). As for Gartner, in 2013, the global market for security outsourcing was $12 billion, with a forecast compound annual growth rate of 15.4% through 2017.

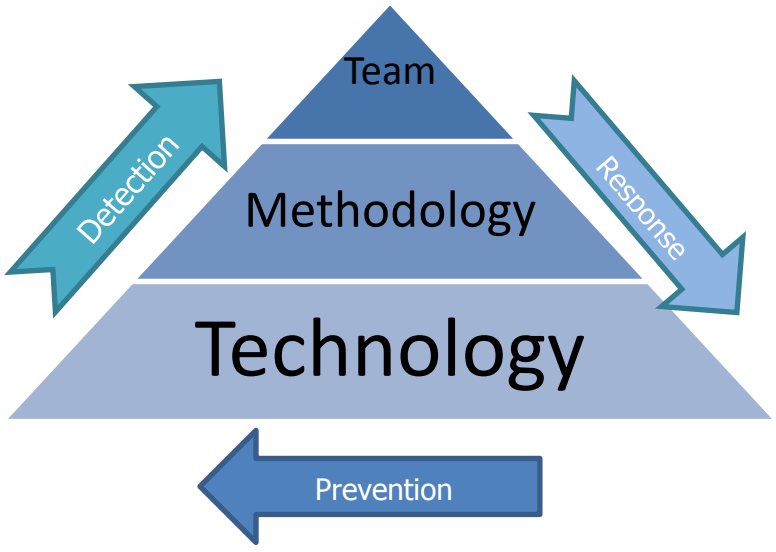
2. **Cyber Threat Intelligence Service Providers (TISP)** – To build and maintain a high Cyber Threat awareness is a very demanding and professional task. It requires an ongoing continues effort to collect, analyze and distributes threat intelligence feeds to its customers online. According to new research from International Data Corporation (IDC), worldwide threat intelligence security services spending will increase from $905.5 million in 2014 to more than $1.4 billion in 2018. As advanced malware, APT, DDoS, and other difficult-to-detect attacks proliferate, it will become that much more essential to the success of predicting threats and, therefore, protecting the enterprise.

# Cyber Security Operation Center

The cyber security landscape has changed dramatically over the past few years creating new challenges for those charged with protecting Federal systems and information. The public and private sectors' cyber security efforts are matched, if not outpaced, by the sophistication of nimble opponents from other nations, cyber terrorists, cyber-criminal syndicates, malicious cyber intruders, and fraudulent insiders

As any SOC, the Cyber SOC is based on similar disciplines however the Cyber domain is relatively young, much more dynamic and sophisticated. The Next Generation Cyber SOC solution should be based on the unique mixture of the following operational and technical fundamentals:

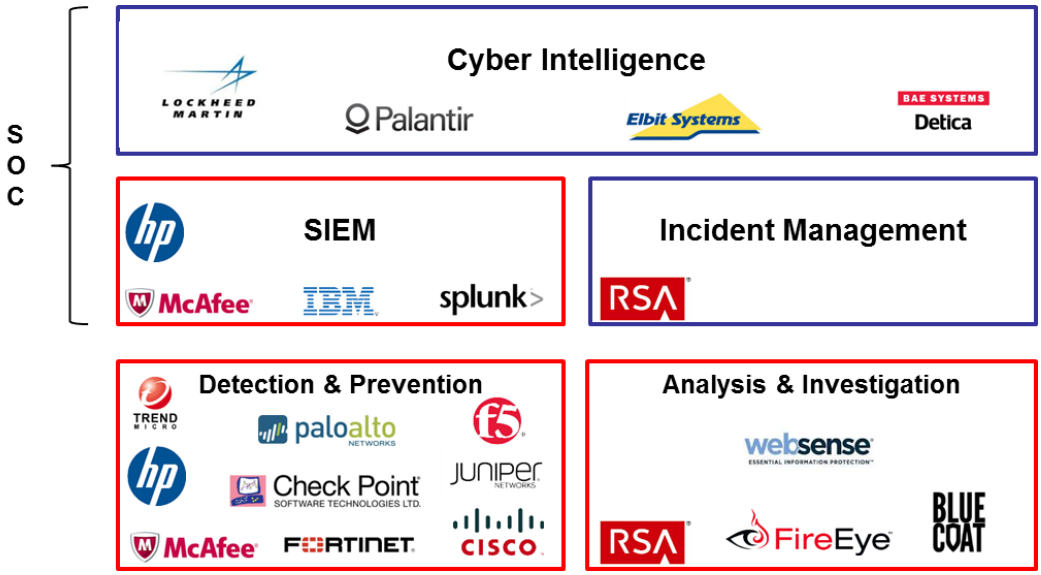
- **System Technology** infrastructure and applications to support big-data collection and analysis, entity extraction and link analysis. The system should provide the Cyber Analysts the means to support the desired workflows.
- **Workflow & Methodology** of work to be translated to work procedures, rules, alerts and reports that should be continuously adaptive to the evolving risks, minimize false alarms and provide comprehensive investigative functionality
- **Skilled Team** of highly trained cyber security and forensics professionals to execute the methodology using the technology



Today, CSOC are equipped with a suite of different technology products from different vendors that are somehow integrated on a project basis and provide some visibility into their IT environment. Beside the technology tools, the SOC needs to assign a qualified security team that can identify exactly which tools are right for the job. This team is needs to evaluate products from multiple vendors, considering system integration requirements, assessing interoperability with existing infrastructure and conducting solution demos and trials.

Some of the required tools may include intrusion detection and prevention technology; SIEM solutions; threat and vulnerability management tools; filtering technologies; traffic/packet inspection solutions; data analytics platforms; and reporting technologies. In addition, depending on the scope of the responsibilities, the SOC may also have access to other business systems such as enterprise forensic tools in support of incident response investigation efforts

The following figure illustrates the Cyber SOC eco-system:



# Cyber Intelligence

Fusion of Internal and External data from multiple sources into a unified big data store for advanced and rapid analytics, including but not limited to:

- Internal **Network & Machine data** - Structured network and machine logs: proxy, firewall, IDS/IPS, VPN, antivirus, DLP, DNS queries, honeypots, servers, databases, SNMP traps, Netflow, AD application access logs and PCAP files, memory dumps.
- Internal **Contextual data**: email and attachments, print logs, facility access logs, internal chat logs, and HR data
- External **WEBINT** - Unstructured data gathered from open sources and Deep Web sources such as: Social Networks, web Forums, Hacker blogs, mailing lists using web crawling and scraping techniques to collect information about targeted Persons, Groups and Topics.
- External **3rd party Intelligence Feeds** – Structured threats data feeds, unstructured reporting, vendor reports, government intelligence reports, databases of cyber threat actors, IP information, and domain reputation feeds