SIEMantics matter!

(Cyber Security at machine speed)

Seccom Global Whitepaper

August 2015

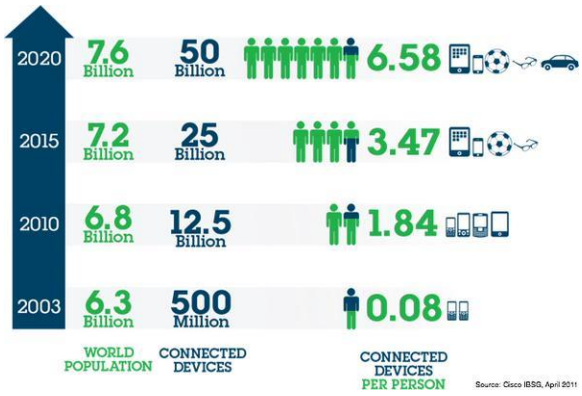
Author: Geoffrey Brown

SIEMantics matter!

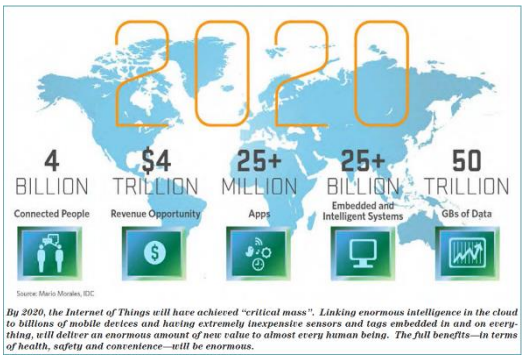
(Cyber Security at machine speed)

As the complexity and scale of connection massively expands new approaches to security has become a business (and personal) imperative.

Current estimates by Gartner and IDC indicate that there will be almost 5 billion connected devices in 2015 and that this number will increase to 25 billion by 2020. Cisco is predicting an even higher number – 50 billion!



The growth will most substantially come from increased usage of phones, tablets and The Internet of Things (IoT). As cars, medical equipment, home appliances, parking spaces, watches and so on become increasingly connected through 3G/4G, Wifi and Bluetooth the IoT interconnection fabric is exponentially growing. These smart device or sensor endpoints have connections to networks and therefore increase the opportunities for interception / intrusion.



In April CNN Money reported that major IT security organisations are detecting around 1 million new malware (malicious software) variants being released into the internet every day (or around 12 every second!).

The ever expanding list of malware includes many well publicised viruses and trojans including CryptoWall, CrypoLocker and HeartBleed. In an attempt to combat this onslaught cybersecurity organisations are having to release more frequent and ever growing security updates. As an example Kaspersky is currently releasing an average of 274 virus signatures every month. Testing of servers and devices across all of the permutations of operating systems before deployment is no longer an option.

In an article in the Wall Street Journal, Symantec declared that the traditional approach to security software is only preventing around 45% of attacks. Most cyber security providers have declared that they have shifted their stance from a predominantly defensive postures towards detection and response capabilities.

This industry-wide repositioning recognises that, for most organisations (maybe all?), breaches will occur. To minimise the impacts of successful breaches every organisation needs to be prepared to Defend, Detect and Respond at machine speed – relying on humans is no longer possible.

Contemporary cyber security protection entails an integrated approach, bringing together capabilities including Next Generation Firewalls, Sandboxing, User Behaviour Monitoring and End Point management.

In addition to implementing these approaches, Security Information and Event Management (SIEM) is becoming an imperative for organisations to address the scale and complexity of digital threats.

Through sophisticated near real-time log correlations and data analysis SIEM enables policy based actions to be rapidly applied to the network minimising the exposure to digital attacks.

Additionally SIEM is bringing is the ability to extend the data analysis and reporting capabilities to business operational management which is often significantly more tangible for business funding approval.

Rather than developing the skillsets, committing the capital and consuming resources to building an in-house capability, many organisations are using a managed cloud SIEM service.

For assistance on how to assess your security environment and opportunities for managing at machine speed contact us:

seccomglobal.
information security services

Suite 21.03, Level 21
25 Bligh Street
Sydney, NSW, 2000
Local Call: 1300 FIREWALL
Telephone: +61 02 9688 6933
Fax: +61 02 9688 6977
E-mail: info@seccomglobal.com

Understanding some key aspects of the

Cyber Security Environment

Some Threats To Consider

Advanced Persistent Threats – APT's

APT's are purpose-built threats designed to breach targeted network defenses and steal information, intellectual property, and communications from these networks without being detected. The primary difference between what we will describe as a normal attack and an APT is, a normal attack will generally be short term, an APT on the other hand once a network is compromised, attempts to stay in the network for as long as possible evading discovery and achieving ongoing access - **Persistent**.

With an APT the attacker will often use phishing to gain access to the network, once access is gained the attacker will attempt to gather valid user credentials – preferably admin or root. Once this is gained the attacker will move laterally through the network to create "Ghost Infrastructure" to install Trojans that are often very difficult to discover.

Detecting APT's often relies on being able to recognise changing patterns and anomalies in network traffic. Also implementing defense in depth similar to what will be required in the IoT.

Zero Day Threats

A Zero Day threat is a vulnerability that exists in code that for all intensive purpose is still undiscovered. The risk of this vulnerability is that it may be discovered by someone with criminal intent who could create an exploit to take advantage of this flaw. Most security technologies rely on knowing about a vulnerability to enable the technology to protect against any potential exploits. But in the case of a Zero Day vulnerability only the hacker who has uncovered the flaw knows that it exists.

There are a number of technologies however that will assist you to protect your network from Zero Day exploits. It all starts with having a secure network design, strong passwords, authentication, encryption and firewall policy. Application visibility, sandboxing and Anomaly detection are also technologies that will assist in uncovering and protecting from Zero Day exploits. It is also very important to understand normal and abnormal behavior on your network, this is where technologies such as SIEM will be of great benefit.

Ransomware

Ransomware is the terminology used for software that is used to infect a victim's network, an example of this is CryptoLocker and CryptoWall, malware used to encrypt

the contents of a computing device enabling hackers to demand a ransom to decrypt it.

Ransomware is malicious software (Malware) that restricts access to a computer or the files/systems on the computer. Some forms of Ransomware will lock access to the computer while other forms may encrypt all files on the system with access to the system or files given only once the ransom has been paid.

In April, criminals began advertising RIG, a so-called exploit kit, which automates the exploitation of software vulnerabilities. For $60 a day or $300 a week, criminals could use it to infect victims' machines with an 8 to 12 percent success rates, according to advertisements. Almost immediately, security researchers began noticing the kits being used across the Internet, in many cases to distribute CryptWall.

In many of these cases, the attacker was using a malicious advertising attack known as malvertising. This was done on legitimate websites, then using the exploit kit to burrow into customers' machines and encrypt their contents with Cryptowall. Often victims would find a message informing them that their data had been encrypted by criminals and would remain unreadable until they paid a $200 fee. When victims did not pay the specified ransom by the deadline, often they received a second message tripling the ransom demand to $600.The largest share of their infections occur in the United States, followed by England and Australia.

With Ransomware although attackers may incorporate different exploits or payloads in their attack, the traffic generated by the final malware when communicating with the command-and-control servers remains consistent. By detecting these communications, organizations can readily implement security measures to prevent the attack from further escalating.

Denial of Service Attack

A Denial of Service attack (DoS) is designed to disable a network or a network resource by consuming available resources disabling legitimate user access to the resource. There are two general forms of DoS attacks: those that crash services and those that flood services.

A DoS attack can be perpetrated in a number of ways with attacks generalised into five types.

1. Consumption of computational resources, such as bandwidth, memory, disk space, or processor time.
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.
4. Disruption of physical network components.
5. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

A Distributed Denial of Service DDoS attack utilises a number of compromised computers that have been infected by a Trojan, a small application (virus) that allows remote command-and-control capabilities of the computer without the user's

knowledge. An infected computer is known as a Zombie or a Bot with the controller of the Trojan network known as the Bot Master. A number of compromised computers is known as a robot network, or Botnet.

To ensure your computer or network does not become part of a Botnet it is important to ensure you have adequate up to date virus protection installed on all computers and servers and your network is protected by industry recommended security controls.

Phishing and Waterholes

An advanced form of phishing is a triangulation attack, with this form of attack the person conducting the attack (swindler) will steal credit card information by use of a phoney website such as an online auction or ticketing site, or using an online classified ad. By posting a product online at a severely discounted price, the mark (customer) will be coerced to purchase from the site using a valid credit card. The swindler uses other stolen payment credentials to purchase and ship the product from a legitimate website to the customer. Neither the merchant nor the customer suspect anything has occurred, yet both have been duped. In the meantime, the attacker now has access to the unsuspecting buyer's credit card number and can continue to steal and amass other credit card numbers using the same scheme.

Emerging or changing technologies to consider

User Behavior Monitoring

A current problem with how we manage security today is that it is implemented from the top down. Senior management will determine what is to be secured, network administrators will implement the required controls and users must abide by the company policy regarding security. Often the major failure in a company security posture is affected by the end user. Be it on purpose or an accident many security issues that occur on companies information systems are the result of the end user. User behavioral monitoring will allow for the quick identification of any misuse of company systems or information and allow management to quickly respond.

User behavior monitoring systems can examine specific actions of users as they leverage IT resources or compare user behavior against historic usage patterns. The basis behind user behavior monitoring is if the user is aware that they are being monitored, then they are more unlikely to offend against company policy.

Sandboxing

Cybercriminals are bypassing traditional antimalware solutions and inserting advanced persistent threats deep within networks. These attacks evade established signature-based detection by masking their malicious nature in many ways that include,

- compression,
- encryption,
- polymorphism, the list of techniques goes on.

A sandbox will attempt to execute suspicious code in a full virtual runtime environment. Once a malicious code is detected the results can be submitted for antimalware signature creation.

Sandboxing in the cloud is a service that advanced Managed Security Providers are now offering.

Security Information Event Management - SIEM

TechTarget defines SIEM as follows…

Security information and event management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security.

The underlying principle of a SIEM system is that relevant data about an enterprise's security is produced in multiple locations and being able to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary.

SIEM combines SIM (security information management) and SEM (security event management) functions into one security management system.

A SEM system centralizes the storage and interpretation of logs and allows near real-time analysis which enables security personnel to take defensive actions more quickly.

A SIM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralized reporting. By bringing these two functions together, SIEM systems provide quicker identification, analysis and recovery of security events. They also allow compliance managers to confirm they are fulfilling an organization's legal compliance requirements.

A SIEM system collects logs and other security-related documentation for analysis. Most SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-userdevices, servers, network equipment -- and even specialized security equipment like firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies. To allow the system to identify anomalous events, it's important that the SIEM administrator first creates a profile of the system under normal event conditions.At the most basic level, a SIEM system can be rules-based or employ a statistical correlation engine to establish relationships between event logentries. In some systems, pre-processing may happen at edge collectors, with only certain events being passed through to a centralized management node. In this way, the volume of

information being communicated and stored can be reduced. The danger of this approach, however, is that relevant events may be filtered out too soon.

SIEM systems are typically expensive to deploy and complex to operate and manage. While Payment Card Industry Data Security Standard (PCI DSS) compliance has traditionally driven SIEM adoption in large enterprises, concerns over advanced persistent threats (APTs) have led smaller organizations to look at the benefits a SIEM managed security service provider (MSSP) can offer such as Seccom Global.

Cybercrime

Cybercrime is criminal activity aimed at the online community with the motive for conducting this activity vast and varying. However while the activity may vary, the methodology for protecting your site against these threats remains alike.

- Educate yourself and users of the potential risks,
- Understand your responsibilities,
- Monitor and manage any potential incursions,
- Implement strong password and encryption technologies,
- Invest in Tier 1 security tools and systems to protect your site,
- Work with security focused service providers,
- Report any incursions promptly to the correct authorities.

A prominent form of cybercrime is identity theft, where criminals use a combination of social networking and online criminal activity to steal user personal information. Two of the most common ways this is done is through phishing and pharming. Both of these methods lure users to fake websites (that appear to be legitimate), where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers and bank account numbers. When operating online always check the URL or web address of a site to make sure it is legitimate before entering your personal information. We have heard it often, if it looks too good to be true, than more than likely this is the case. People don't give you a million dollars to get money out of a third world country!

Internet of Things

As Internet connectivity is becoming fast and more widely available, the cost to deliver this access continues to fall, this creates the perfect environment for the IoT to flourish.

Imagine a world where everything is connected! Where cell phones are used to drive cars, where a golf ball could have a sensor imbedded that connects back to an app on your phone - meaning you never lose a ball again, where a medical device imbedded in a patient will be able to feedback information to their doctor? Well this world is here, but the potential that the IoT will bring, what can be connected and how it will be used is still a matter for the imagination. The ability to connect, communicate with and manage an almost incalculable number of devices creates opportunity for both the entrepreneur and also those with more sinister motives.

Given the pace of innovation, it is expected that an entirely new security solution will emerge that is uniquely designed to protect IoT systems. The truth is the solution will more likely be a combination of established security measures that we adapt to meet the constraints of the imbedded devices that we will find within the IoT.

The primary difference between the IoT and established enterprise networks is that we generally have an understanding of where the security boundaries exist. Although this is rapidly changing the areas of the network we tend to deal with are;

- Internal networks (business or home) – trusted.
- Externally or public networks – untrusted.
- Business partner networks - partly trusted.
- Cloud provider networks - trusted but with little visibility.
- Remote user access – trusted once authenticated.
- Public WiFi networks – often trusted but very risky.

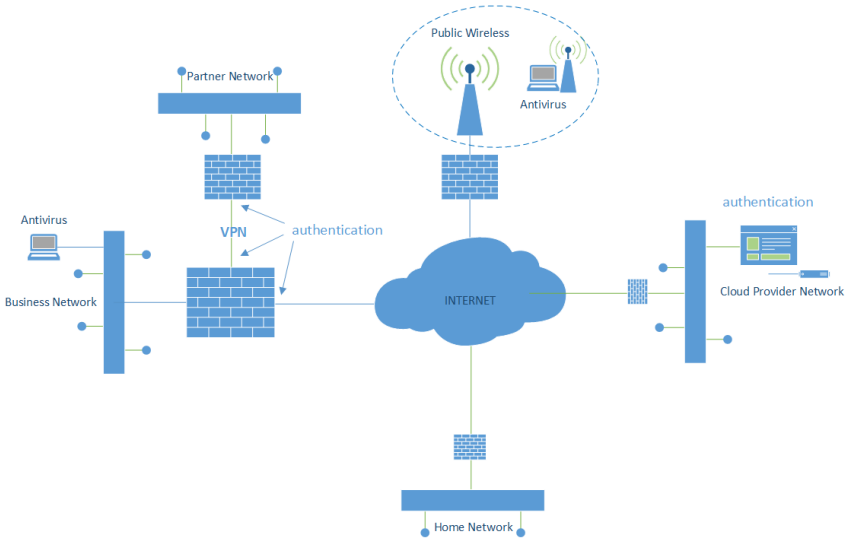


Figure 1.0 - Traditional methods of implementing security

In a corporate network understanding the zones between the trusted and untrusted areas of the network and implementing the security controls to protect the systems and information within these zones traditionally is the responsibility of the network administrator. Establishing policy of what is allowed and what is not allowed on the corporate network more traditional will be the responsibility of more senior level management. In an IoT world where embedded devices exist these areas of control will become more blurred and it is these areas where challenges will be faced.

Embedded devices are generally designed for low power consumption, with small silicon form factor, these often have limitations on storage, connectivity, and processing that most likely they will operate independently of user intervention. The variety of what these embedded devices may be used for is what will create the security challenges to be faced. For example just some of the devices we currently see or will see in the not too distant future include;

- Programmable Logic Controllers (PLC's) currently used to control robotic systems will become even more integrated with the IT systems of an organisation.

- Control systems for energy resources, smart cities and homes will be connected to the public network to allow for more granular integration between the user and supplier of the service.
- Smart cars will be connected to mobile applications that will sense when you're about to exit the office, shops, or home. The technology will allow you to summons the car and it will drive independently up to you with heated seats and music playing, to pick you up.

What is a 5G network?

With speeds of up to 100 gigabits per second, 5G will be as much as 1,000 times faster than 4G, the latest iteration of mobile data technology. Huawei, the Chinese telecoms giant that is a driving force behind 5G research, says 5G will allow for any mobile app and any mobile service to connect to anything at any time. 5G will allow for billions of sensors to be built into appliances, security systems, health monitors, door locks, cars and wearables. Analyst firm Gartner predicts 25 billion devices networked in 2020 up from 5 billion in 2015.