Business white paper

5G/SOC: SOC Generations

HP ESP Security Intelligence and Operations Consulting Services

Table of contents

Since the inception of the Internet, there have been many advances and evolutions in security operations centers (SOC). The industry is currently defining the fifth generation, or 5G/SOC. This paper walks you through the generations of SOCs, their characteristics and goals, and what the future of security operations holds.

Executive summary

Security operations centers exist to monitor and protect the IT assets of an organization through standardized and repeatable processes. The first formal security operations centers existed in military and government entities where the first functional TCP/IP networks were installed and concepts of intelligence, risk management, and operations were well understood. As commercial and private entities became progressively more connected and IT dependent, the exploitation, and (necessary defense) of this infrastructure quickly emerged. Attackers were wildly successful with only social engineering and a variety of simple exploit methods as IT and network infrastructure adoption outpaced the creation and adoption of security controls. This led to the emergence of completely new markets for both the “good guy” defenders and the “bad guy” attackers in a highly dynamic threat landscape. Operations focused on addressing this threat landscape evolved out of corporate IT, Risk, or Compliance departments in various forms. These security operations teams live in the world between organizational silos, on the front lines of cyber defense.

A constant challenge for security operations organizations is to detect current and emerging threats and predict future attack methods. To do this we can look at the current cyber kill chain model, as originally defined by Lockheed Martin.[1] The current cyber kill chain consists of five steps that an attacker achieves during an attack. We see the attackers researching their targets, infiltrating the perimeter defenses and poking around an organization to discover what assets are available and most valuable. From here they capture the target's key systems and begin exfiltration of data. By understanding these threats, we can organize our security operations around each of these steps to verify each phase of the kill chain is addressed. Detection and disruption of activity at each and every stage of the kill chain is critical. If an attack is not detected early in the kill chain, the impact of that attack is amplified and later stage detection becomes critical.

Naming convention for security operations centers

The naming convention for security operations centers has also evolved. Organizations have toyed with different naming conventions to portray advanced capabilities and purpose or avoid political pitfalls and stigmas associated with the "operations" moniker in an organization. "Defense Centers" highlight the protective nature of the organization, "Intelligence Centers" show the advanced capabilities and high caliber of analysis. Adding the term "cyber" specifies an electronic focus as opposed to the physical security team. Inclusion of the term "threat" to reflect the risk based attributes of a monitoring team. Organizations have developed numerous creative names to represent a security monitoring function. For the purpose of this white paper, we will use "Security operations" and "SOC" in reference to the people, processes and technologies involved in providing situational awareness through the detection, containment, and remediation of IT threats.

[1] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Security operations capabilities to date can be grouped into five generations. The first generation of SOCs started as early as 1975. Early SOCs utilized emerging technologies but were often ad hoc and understaffed.

First-generation SOC: 1975-1995

Nuisance programs and minimally impacting malicious code era

The first-generation SOC was marked by the birth of the Internet. Most companies at this time had no network defense measures. Not long after adoption of the Internet, exploitation and abuse emerged. Early detections of abuse were the results of creative thinking and problem solving but were neither organized nor repeatable. By the mid-eighties, the cyber threat landscape was gaining public visibility in Hollywood movies, in books and publications, and in US Congress. The first security tools emerged in the form of antivirus and firewall software, followed by proxies and network intrusion detection systems. The first "Security Operations" were formalized to monitor and manage these products and respond to threats. Security operations was typically a single person, usually with a networking background, who was tapped to manage an organization's security devices. Functional Security Operations Centers begin to appear in government and military organizations during the latter half of this generation. The analysis done in these SOCs is largely unstructured, the bandwidth is low, and entrepreneurs begin to see the opportunity in being white hats or black hats.

Notable events:

1970's	Phreaking takes advantage of telecommunications systems
1972	First full duplex modem introduced with 1,200 bps
1974	Ethernet developed
1979	Kevin Mitnick uses social engineering to gain access to DEC systems by getting a dial-in password reset
1980	Ethernet commercially introduced
1981	Hayes SmartModem (14.4 kbs) BBS's emerge (and remote connectivity connects living rooms and dorms around the world)
1983	"War Games" movie released
1984	"2600: Hacker Quarterly" magazine begins publication
1986	"The Cuckoo's Egg" is published—bringing IT security espionage to print
1986	Computer Fraud and Abuse Act and the Electronic Communications Privacy Act makes it a crime to break into computer systems
1987	Christmas Tree Exec, first widely disruptive self-replicating program
1987	tcpdump created
1987	McAfee Associates creates antivirus software
1988	November—Morris Worm, first worm to spread in the wild (BSD Unix variants)
1988	IRC protocol created by Jarkko Oikarinen
1989	SANS Institute formed
1991	Symantec creates Norton Antivirus software
1992	DEC SEAL, the first commercial firewall is shipped
1993	Windows 3.11 released with peer to peer network capability
1993	USAF creates 67th Air Intelligence Wing (AFCERT) based out of Lackland AFB (San Antonio, TX) to focus on Cyber Intelligence
1993	Bugtraq security mailing list created
1995	Wheelgroup launches first intrusion detection system: NetRanger
1995	"Concept" first macro virus

Intrusion detection systems played a huge role in second-generation SOCs. Organizations began formalizing some of their processes and procedures around intrusion response and vulnerability tracking. This generation was greatly improved over the first but remained mostly defensive and narrowly focused.

Second-generation SOC: 1996-2001

Malware outbreak and intrusion detection era

Second-generation Security Operations can be categorized as an era of malware outbreaks including widely impacting viruses and worms which wreaked havoc on corporate and government networks. This was the era which spawned vulnerability tracking and formalized system patching. SOCs were found in government and military organizations and began emerging in the largest commercial organizations. Companies began to commercialize security monitoring and management services and offer these services to paying customers, otherwise known as the Managed Security Service Provider model. There is an explosion of new technology products with varieties of firewalls, antivirus, proxies, vulnerability scanning, and intrusion detection systems. The big focus during this period was intrusion detection. Some government and military organizations had robust SNORT and tcpdump deployments; the private sector began to buy commercialized versions of IDS systems in droves during the later years of this era. Nation-states began cyber network exploitation, defense, and attack programs in the later years of this era, however none of these programs were yet known to the public. Security event analysis was largely performed through use of scripts, IDS consoles, and other homegrown tools. The concept of security information event monitoring (SIEM) was introduced at the end of this generation as a technology used to correlate disparate security events into a single system. However analysts would not rely on this single pane of glass in daily operations until the next generation.

Notable events:

1996	Managed Security Providers begin offering managed Firewall and IDS services (example Netrex)
1998	SNORT created
1999	MITRE creates the CVE repository/system
1999	SANS creates precursor to Internet Storm Center
1999	Packet Storm security mailing list debut
1999	"Happy99" virus affects Outlook Express and wishes users a happy new year, "Melissa" worm targets Microsoft Word
1999	GLBA introduced with privacy protection standards
2000	"ILOVEYOU" (Love Bug) virus
2001	"Sadmind" worm affects Sun Solaris, "Code Red" & "Code Red II" worm affects MS IIS, "Nimda" worm
2001	Wahoo Technologies is renamed "ArcSight" and "Security Information and Event Management" products are introduced to the market

By the mid-2000s, cyber threats had matured into financially-driven attacks organized in an underground marketplace. The number of attacks increased at a rapid rate and smaller organizations began feeling the impact of new threats. A new generation of security operations centers emerged to address these attacks and new technologies focused on prevention of attacks rather than just detection.

Third-generation SOC: 2002-2006

Botnets, cybercrime, intrusion prevention, and compliance era
The third-generation era was most noted for the expansion and organization of cybercrime syndicates which used Bots to steal identity and financial information for monetary gains. The third-generation was kicked off in 2003 with hugely impactful malware such as SQL Slammer and Blaster, which caused mass disruption of the Internet. That same year, the US-CERT was formed. As this generation continued, malware moved from disruptive worms to targeted attacks. Government, military, and managed service provider (MSSP) organizations had already developed mature security operations centers; large private sector companies within certain industries started to create formal security operations centers. The payment card industry formed the PCI council and required vendors to adhere to security and data protection standards. The cyber exploitation capabilities of nation-states such as China were first noticed during this period as the US military and various defense contractors were targeted by China as part of Operation Titan Rain. Computer Incident Response teams formalized crisis management procedures and a focus is placed on early detection capabilities. Adoption of security programs in the private sector increases and major data breaches began to be detected and reported to the public as a result of new breach notification laws.

Notable events:

2002	Sarbanes Oxley Act dictates IT security controls and individual liability for executives
2003	“SQL Slammer” worm, “Blaster” worm, “Nachi” worm, “Sobig” worm, “Sober” worm
2003	HD Moore creates the Metasploit framework
2003	US-CERT created
2003	California state law SB 1386 requires notification to consumers if PII is disclosed to a third party. This is considered the first breach notification law.
2004	PCI council formed
2004	“Bagle” worm, “MyDoom” worm
2004	Rock phish attack first seen using wildcard DNS entries
2004	First mobile malware, Cabir, written for Symbian OS
2004	“Convention on Cybercrime” treaty goes into effect
2004	Operation Titan Rain (Chinese attack against US Military/Government systems)
2005	“Zotob” worm
2005	“Samy”, the first social media worm, spreads across MySpace
2005	BitTorrent created and peer to peer file sharing explodes
2006	Russian Business Network (RBN) registers domain name for website
2006	US ratifies the “Convention on Cybercrime” treaty
2006	WikiLeaks website launched by Julian Assange

Larger and more sophisticated attacks led to more government and mainstream media attention in the last few years. Attacks were larger and attack vectors had become more targeted to individuals. This led to a greater push for security controls and a new generation of security operations to handle more advanced threats.

Fourth-generation SOC: 2007-2012

Cyberwar, Hacktivism, APT, and exfiltration detection era
Fourth-generation Security Operations was marked by the publicity of a politically motivated cyber threat landscape. News headlines and detailed studies spotlighted nation-states attacking one another with the purpose of stealing intellectual property or sabotage. The first publicly known use of cyber-attacks in the context of an armed conflict changed the way warfare was viewed when Russia attacked Estonia in 2007. "Hacktivist" organizations gained widespread notoriety for their successful attacks against organizations and individuals with social media tools providing the means for coordination and information dissemination. Organizations began to realize that intrusions will happen regardless of the preventative security technologies in place and the focus shifts from intrusion detection and prevention to exfiltration detection and containment. During this time additional private sector organizations created security operations organizations for the purpose of detection, escalation, and remediation of security events.

Notable events:

2007	Zeus Trojan/Botnet
2007	TJX breach
2007	Russia attacks Estonia in first publicly known cyberwar
2007	Anonymous gains first media attention
2008	Conficker Worm/Botnet
2008	Hannaford Bros breach
2008-2009	Heartland Payment Systems breach
2010	SpyEye Trojan/Botnet
2009-2010	Operation Aurora—Chinese attacks on companies such as Google, Adobe Systems, Juniper Networks, Yahoo, Symantec, Northrop Grumman, Morgan Stanley, and Dow Chemical
2010-2011	WikiLeaks publishes Baghdad Air Strike video and Diplomatic Cables
2010	Stuxnet Trojan attacks Iranian SCADA systems
2011	SpyEye and Zeus Trojan code merged
2011	RSA breach
2011-2012	Anonymous attacks SONY, other DDOS and exploit campaigns release corporate documents via Twitter, paste sites like Pastebin.com, and Torrents
2012	Flame malware discovered, most complex malware seen to date

With cyber-attacks growing exponentially, organizations are rushing to find the best way to reduce their risk and limit the impact of a breach. Security operations have morphed from reactive to proactive programs. The fifth-generation SOCs are utilizing the complete visibility from a security devices and SIEM combined with big data analysis to find previously unknown attack vectors and indicators of long-undetected compromise. This security operations capability is currently growing critical mass in the most advanced SOCs around the world.

The 5G/SOC: 2013-?

Analytics and big data, intelligence-driven methodology, information sharing, human adversary approach

The fifth-generation (5G/SOC) of Security Operations is still evolving. The cyber threat landscape is evolving at an unprecedented pace and markets are demanding and providing increasingly advanced products. Threats have always been driven by human adversaries, yet most security products provide point solutions for signatures, faults and rogue viruses/worms–5G/SOCs recognize the change in threat landscape and are approaching the challenge holistically: training analysts in security counter-intelligence, surveillance, criminal psychology and analytical thinking to augment the technology investment. While standards and compliance efforts have improved the adoption of security products and practices, 5G/SOCs realize that security programs need to be active, engaged, and intelligent—and through that, compliance is achieved—not that compliance regulations will create better security.

5G/SOCs are efficient. They automate the activities that most fourth-generation SOC Analysts performed manually, including incident containment and response—human cycles are applied to advanced analytics and subtle event detection.

5G/SOCs are analysis-focused. They are storing enormous amounts of structured and unstructured data from inside and outside of their organization and using advanced analytical tools to derive intelligence and make predictions based on newly discovered patterns. 5G/SOC's merge business intelligence and security intelligence tools to create contextual understanding of enterprise and its risks. 5G/SOC analysts include mathematicians, statisticians, theorists and big data scientists to achieve their goals.

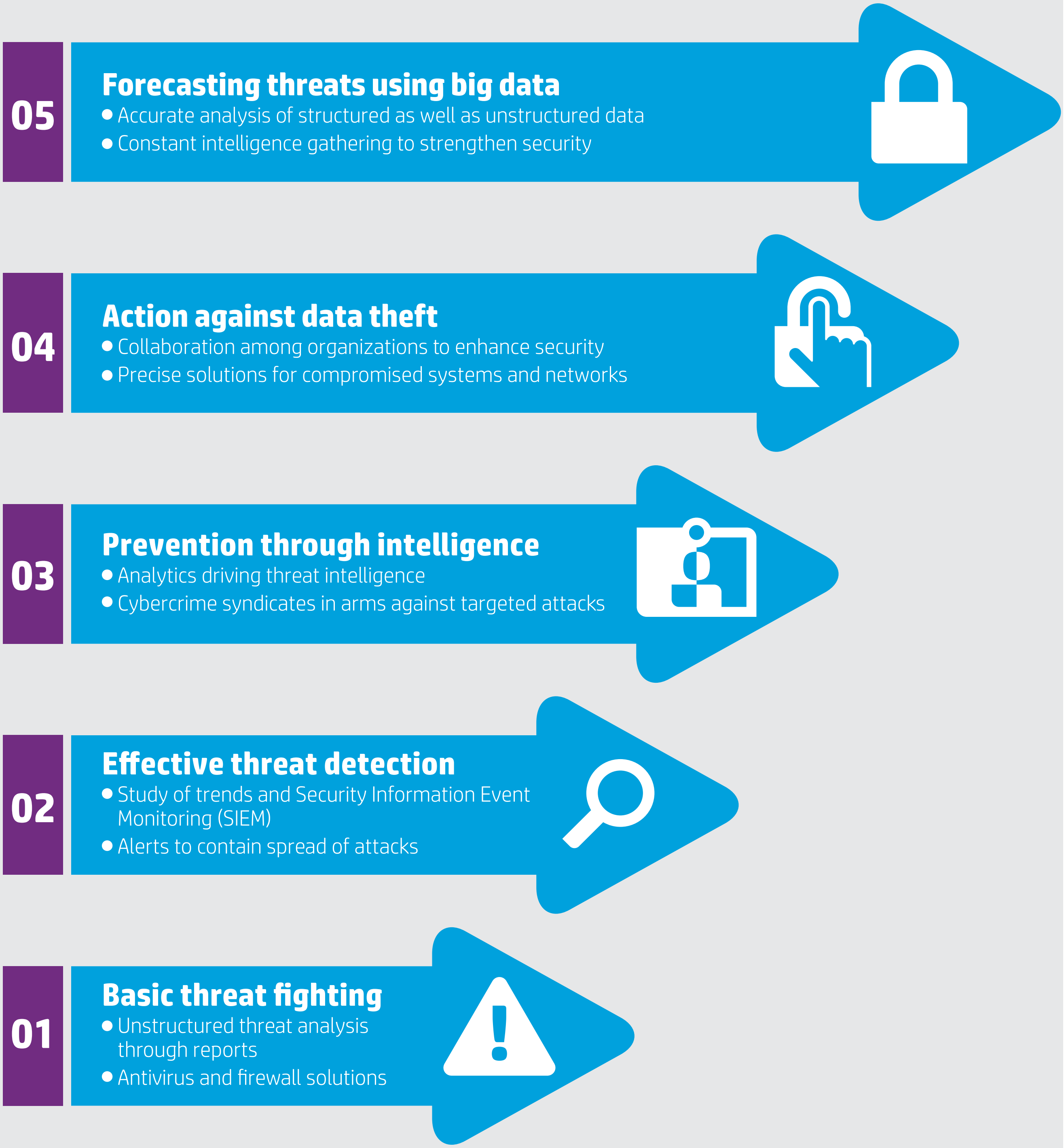
5G/SOCs are not alone. The functions of the 5G/SOC have the same goals of previous generations; the main goal being to reduce the risk to an organization by detecting threats before they cause undo damage. To meet this goal, the 5G/SOC must collaborate with others at least as well as attackers are collaborating. No single organization has all the information needed to detect all threats, "Threat Intelligence" services are not broad enough alone, and formal consortiums still have guarded participation. 5G SOC leaders are forming active information sharing groups and direct relationships within their industry/vertical and leverage each other's expertise to match wits with the adversary.

5G/SOCs are adaptive. They leverage and invest in the expertise of people. Much like it takes a human pilot to fly an aircraft (even an unmanned aircraft), it takes seasoned information security professionals to provide effective threat detection. Better technology advances one's capabilities, but without the human brainpower behind the technology even the best technology will crash on the pad.

5G/SOCs push the envelope. Organizational structure and operational tactics used by 5G/SOCs will change the nature of the game. Organizations are exploring counter-attack capabilities, investing heavily in intelligence gathering teams, and formalizing hunt teams that track malicious groups and individuals both inside and outside. Governments and large organizations already maintain Red Teams to continually test their Blue Teams. Red Teams attack while Blue Teams defend. Smaller organizations are realizing the value of Red Teaming to support a better defensive posture. In a 5G/SOC, the constant attack and defend exercises are making the enterprise safer against real-world threats. In addition, intelligence teams are collaborating with other organizations to share details about adversary methods, techniques, and tools. Hunt teams take a step back from the triage of alerts and utilize the big data stores to search for previously unknown and unseen attacks. This data analytics driven hunt team will be able to search farther back into the past than has been previously possible to show how long a threat has been active in the environment once its presence is detected.

Evolution of tackling security breaches

Security breaches to the IT network not only affect infrastructure, but can have a direct impact on the business and in several instances, can tarnish your competitive advantage in the market. Take a look at how the world has been tackling security breaches over the years, improving and redefining security at every step.



05

Forecasting threats using big data

- Accurate analysis of structured as well as unstructured data
- Constant intelligence gathering to strengthen security

04

Action against data theft

- Collaboration among organizations to enhance security
- Precise solutions for compromised systems and networks

03

Prevention through intelligence

- Analytics driving threat intelligence
- Cybercrime syndicates in arms against targeted attacks

02

Effective threat detection

- Study of trends and Security Information Event Monitoring (SIEM)
- Alerts to contain spread of attacks

01

Basic threat fighting

- Unstructured threat analysis through reports
- Antivirus and firewall solutions

Conclusion

Every 5G/SOC must build on the history and capabilities of all previous generations of SOCs. 5G/SOC must cover perimeter security, vulnerability tracking, malware detection, and incident response. 5G/SOCs must detect insider threats and advanced persistent threats. They must monitor users and their activity for data exfiltration and must effectively utilize threat intelligence and big data tools to find previously unknown attacks. New tactics and techniques must be utilized, new technologies must be implemented, and existing processes must be automated. Highly trained and motivated staff must collaborate to reduce the risk to the enterprise. It is no longer just about securing infrastructure. The 5G/SOC is not only defending the network but is also defending the business and its competitive advantage in the market.

Industry leading SOC technologies by HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Expert services to mature your SOC

HP ESP Global Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results and demonstrate ROI. Our proven, use-case driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people.

HP Enterprise Security has been building SOCs for enterprises for the last 10 years. We can help you build or mature your security operations.

Learn more at
hp.com/go/sioc

Sign up for updates
hp.com/go/getupdated

Rate this document