Governance of Security Operation Centers

Brencil Kaimba, Information Security Consultant, Serianu Limited.

About Me

Brencil Kaimba
ISO 27001/2013 Certified
SIEM deployment and analysis certified
Information Security Consultant at Serianu Limited

Email: brencil.kaimba@serianu.com

Agenda

- ❑ Disruptive Technology
- ❑ The impact of Disruptive Technology on organizations.
- ❑ Need for a Security Operations Center (SOC)
- ❑ Designing an effective SOC
- ❑ Operating a SOC
- ❑ Qualities of an Analyst
- ❑ Measuring the success of a SOC
- ❑ Sustainable Governance

Disruptive Technology

In recent years , the growth in technology and Innovation has been an engine of change, enabling people to do new things in ways that make old technology obsolete . This is what we call **disruptive technology**. Firms are in a race to match consumers to services and products. Customers are demanding more and more ease when it comes to engaging with businesses.

- An increasing tech-savvy population within the continent has seen a surge of more disruptive tech coming our way. Companies are pushed to craft new ways to incorporate technology or risk losing revenues. Simply put, Adapt or Lose business!

What This Means for Companies

These disruptive technologies include but are not limited to:

- IoT Internet of things
- Cloud Services
- Mobile money
- Introduction of 4G network capability

Consequently, businesses are under immense pressure to adopt these new technologies in order to maintain their competitive edge in the market. The result of this - these organisations are now more vulnerable to attacks.

Internet of Things (IoT)

- The biggest worry is how a company can consume all this information that is being generated by millions of IoTs to bring valuable insight.
- Due to insecure implementation, these Internet-connected embedded devices are routinely being hacked and used as weapons in cyber-attacks.

2016 AFRICA CACS AN ISACA EVENT

Cloud Services

- We are moving information from our premises to the cloud.
- From a security perspective, this presents two security issues.

1. **Traditional firewall protection won't help us** protect our systems and
2. we are **losing visibility of our security posture**.

- Managers sometimes forget that even though data is on the cloud, they are the ones who still **OWN** the data. When a cloud company is breached, it's your data that's being exfiltrated. You can delegate work but not **responsibility.**

The supply chain

- Third parties are usually considered the weakest link to an organization.
- Reported breaches that were related to Vendors - JP Morgan Breach, Target data breach

As we are looking at these, it's also about the **TRUST** within the supply chain. You need to ask yourself these:

1. What is it you are trusting with these 3rd party vendors with?
2. Is it Intellectual property? Brand and reputation? or Shared Control?
3. Do these companies have the capabilities to reduce that risk that they introduce to those they serve?

Sophistication of Attacks

As technology evolves, so does cybercrime. The criminal complexity is growing more sophisticated in software tools.

Cyber criminals have improved their tactics.

- Patching malware
- DDoS as a Service
- IoT Botnets
- Targeted Attacks

What's the Solution?

- We need a solution that can help us consume all the data we are receiving from these new technologies that we are embracing and provide **valuable insight** to Organizations.
- We need a platform to provide **enhanced visibility** on the security posture of organizations with regards to potential sources of attack.
- This solution is the SOC (Security Operation Center)
- As Serianu, our core business is to provide clients with valuable insight and enhanced visibility into information assets. As part of this, we help develop and manage an organization's SOC.

Benefits of a SOC

There is need for us to centralize collection, monitoring, detection and prevention of information.

1. **Correlation of different logs(Telling the Story)** -Single, isolated events often do not tell the whole story.
2. **Real time monitoring** of Security events.
3. **Forensics**- Even in cases where attacks are successful and data is stolen or systems compromised, an enterprise may be able to learn how to block future attacks through forensics.
4. **New Attack Vectors-** Because a firewall and IDS will not protect your mobile devices from hackers.

Designing a SOC

- Building a topnotch security operations center (SOC) takes a lot of time and no matter how much money you are prepared to spend, the task is generally considered more of a marathon than a sprint.
- Organizations should take a data-intensive approach called **“Intelligence-driven security”** to protecting critical information and business assets.
- Organizations need to converge and create collaboration among Information Security, Risk Management, Customer Security Management and Corporate Protection and Investigation groups to achieve a more compound view of risk throughout the whole organization.

Vulnerability-centric vs Threat-centric defense

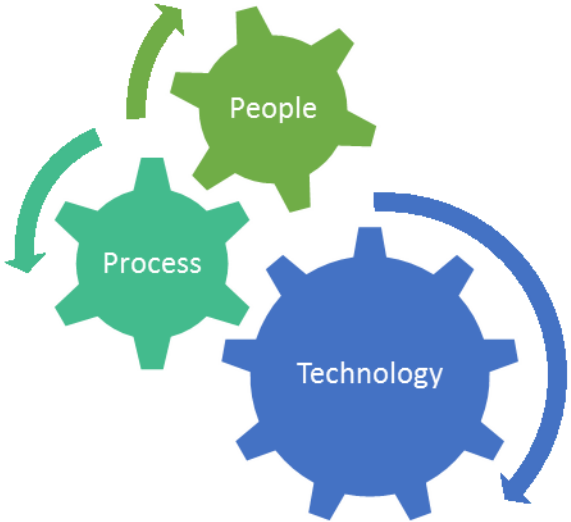
- Vulnerability-centric defense places focus on the **"how"** while threat centric defense focuses on the **"who"** and **"what".**
- Specifically, you must ask yourself **who would they be interested in when attacking your network**, and **what would they stand to gain from such an action**?
- Threat-centric defense is much harder to perform than its predecessor. This is because it requires two things: **extensive visibility** into your network, and the ability to collect and **analyze intelligence** related to the intent and capability of attackers.

Define Threats- (Threat-centric security)

- When it comes to defining threats, ask the question - "**What is the worst scenario that relates to the survivability of the organization?"**
- The answer must come straight from the Top Management.
- With the identification of these threats, the security team should then dig deeper and narrow down to the underlying technologies.
- You need to understand the infrastructure within the network by asking the right questions to the primary stakeholders involved.

Roadmap

- As Serianu, we use the following fundamental building blocks when designing our client's SOC;



Roadmap

- **People:**

While analyzing the people aspect in an organization, it's important to look at the level of formal training, experience, level of expertise and Security awareness. It's easy for top management to feel confident that their employees are well prepared to handle any security issue. Far too often, this is not the case. You find that these staff are too busy or are not equipped with the right skills and experience to maintain a far-reaching security strategy, and they react to problems rather than proactively managing layered security.

Roadmap

- **Processes**

Existing processes within an organization need to be defined and where necessary documented. When it comes to SOC, defining repeatable incident triage and investigation processes standardizes the actions a SOC analyst takes and ensures no important tasks fall through the cracks.

- **Technology**

Understanding the underlying technology of an organization is key. This understanding will help determine the kind of attacks/exploits to expect, vulnerabilities and ways to mitigate.

Acquiring a SOC

- What type of SOC to acquire?

A company can either outsource a SOC or operate one In-house.

- An **in-house SOC** has the advantage that the staff know the environment better and have most potential to be most efficient. However, there is higher pressure to show ROI quickly and higher potential for collusion between analyst and attacker.
- An **outsourced SOC** has less potential for collusion between monitoring team and attacker and the staff are unbiased. The biggest risk with this however is the risk of external data mishandling.

Fundamental Questions

When Outsourcing a SOC:

- About the company- Its reputation, customers and duration in business.
- Stability of the company- How many systems can they monitor?
- Staffing of the Company- What is the experience of its staff?
- Sizing and costs
- Contents of the SLA
- Knowledge transfer

In-house SOC

- What tasks will the SOC perform?
- Who will own and Manage it? What qualifications will they need?
- Who will use the data collected and analysed?

Role of the Vendor

- As a vendor, my role and that of every analyst is to share our unique visibility of the information security field. Our clients are in a battle field without weapons defending themselves against an attacker who is armed with weapons. It's up to us to ensure that we are not the point of weakness for the organizations we aim to protect.

What are the Cost implications of Outsourcing(MSSP) verses operating a SOC In-house?

Cost Breakdown	SIEM Solution	MSSP	Savings	%
Tools (Product Cost) SOC Infrastructure (to support product purchase)	$400,000			
MSSP Fees/Initial Charges	$100,000	$30,600		
Total – Initial	$500,000	$30,600	$469,400	94%
Annual/Ongoing Expenses				
Resources (2FTE)	$212,500			
Management Costs	$106,250			
Security Engineering Costs	$78,750			
Training	$11,250			
Tools, Maintenance	$90,000			
SOC Operating Expense	$9,200			
Depreciation and Amortization	$166,667			
Consulting Services Ongoing	$12,500			
Network IDS/IPS	$10,000			
MSSP Fees/Charges		$511,240		
Total - Recurring	$697,117	$511,240	$185,877	27%

The Business Case for Managed Security Services Managed Security Services Providers vs. SIEM Product Solutions
http://www.solutionary.com/dms/solutionary/Files/whitepapers/MSSP_vs_SIEM.pdf

Operating a SOC

- Defining Expectations and Scope
- Defining Normal through Baselining
- Threat Intelligence
- Incident Handling

Expectations and Scope

- Before starting any operations in the SOC, its paramount that the Executives and the SOC team meet up and clearly define the scope and expectations.

Expectations

Defining scope helps prevent unrealistic expectations from both sides.

Reality

Defining Normal through Baselining

- A SOC consolidates a lot of information from different sources and it's the ability to differentiate what's normal from what is abnormal that will contribute to the general success of the SOC.
- Start by **understanding the network** and **processes** of the Organization.
- Clearly state the problem to be solved by the SIEM tool/SOC
- **Review the functionality** of different components of the SOC i.e. SIEM tool/ Vulnerability management tools (rules, algorithms, reports and dashboards) that is needed to solve the problem.
- Develop Use cases.

Threat Intelligence

- What is Threat Intelligence?- The ability of a SOC to identify and update specific types of threat information that will help in detecting attacks.
  - Continuous monitoring to ensure that all the rules are working
  - Fine tuning the rule with time
  - Visualization on the dashboard
  - Drilling down on particular incidents
  - Reporting.

Incident Handling

Prevention Eventually fails

- **Identification:** This phase deals with the detection and determination of whether a deviation from normal operations within an organization is an incident and its scope assuming that the deviation is indeed an incident.
- **Containment**-Involve management at this point in time.
- **Eradication-** Understand the attack vector and remove it permanently as well as cleanup any remnants from the attack.
- **Recovery-** This is where you put systems back into production.
- **Lessons Learned-** What are the main learning points derived.

Qualities of a SOC Analyst

A good SOC analyst should possess (but not limited to) the following skills:

- Offensive and Defensive Tactics- Penetration testing and security assessments.
- Systems Administration - An adept understanding of Windows and Linux
- Malware Analysis- Performing both dynamic and static analysis.
- Host-Based Forensics- This knowledge is used to generate new indicators of compromise

Measuring The Success of a SIEM

- Organizations should not measure the effectiveness of SIEM by whether a compromise occurs, but rather, **how effectively it is detected, analyzed, and escalated**. Ultimately, instead of asking "**why did this happen**?", the questions leadership should be asking your SOC team after a compromise are, "**how quickly were we able to detect it,** how quickly were we able to escalate it to response, and **how we can adjust our SOC posture to be better prepared next time**?"

Attitude Change

- **Embracing Security**- Gartner projects that by 2020, 60% of budgets will be allocated to rapid detection and response approaches.
- **Paradigm of Fear:** There are far much bigger risk that far outstrip the ones we're focused on, risks that need to be dealt with in a more focused way. We need a change of an epical nature.
- **Fragmentation of the solution**.
- **Change behavior-** Intellectually we know that antivirus, malware sandboxes, firewalls and next generation firewalls won't protect us but it's still not translating into change behavior fast enough.

Sustainable Governance

To run a successful SOC, the following governance principles should be applied:

- **Invest in People**: “Adversaries are not beating us because they have more technology, it’s because they’re more creative, patient, single minded and they explore limitless pathways”- *RSA president Amit Yoran.*
- **Emphasize Teamwork:** cohesiveness helps promote a learning culture.

Sustainable Governance

- **Provide Formalized Opportunities for Professional Growth**
- **Reward Success-** Acknowledge the efforts of those who contribute to the success of the SOC as this can be a monumental morale booster.
- **Exercise Servant Leadership-** Give precedence to the needs of others by helping them achieve their mission for the prosperity of the organization.

Conclusion

- Acquiring and maintaining a SOC takes a lot of money and it's the company's responsibility to ensure that value is gotten from these Centers.
- Running a successful SOC is not a time affair. It takes time and correction of a lot of errors along the way. Mistakes will be made.
- Finding and maintaining good analysts is also difficult.
- Prevention eventually fails- you will be hacked.
- Information Security is not a one person affair and as such, companies in the same industry need to collaborate, share information that will enable improved detection and prevention of attacks.

References and Further Reading

- Bejtlich, R. (2013). The practice of network security monitoring: understanding incident detection and response. No Starch Press.
- Ben rothke. (2016). Rsaconferencecom. Retrieved 18 July, 2016, from https://www.rsaconference.com/writable/presentations/file_upload/tech-203.pdf
- Sanders, C., & Smith, J. (2013). Applied network security monitoring: collection, detection, and analysis. Elsevier.
- Torres alissa, T.A. (2016). Sansorg. Retrieved 18 July, 2016, from https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907
- RSA Technical Brief, February 2013
- Troels Oerting, CISO Barclays Bank-RSA Conference 2016
- Amit Yoran, President RSA- RSA Conference 2016
- Samir Kapuria, GM Cyber Security Services, Symantec-RSA Conference 2016

Thank You!