Santa Monica Networks

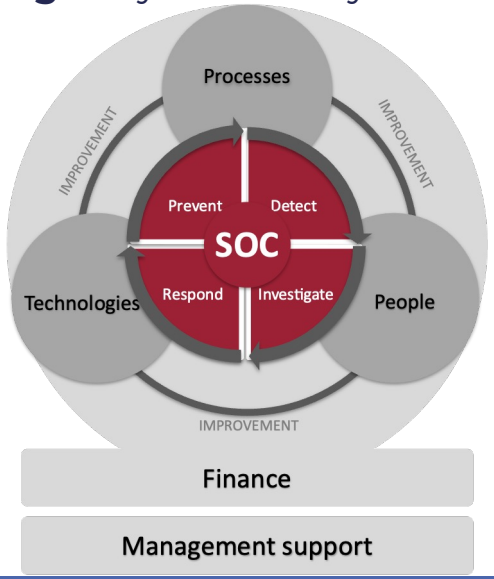
Simply SOC Managed Service

Arvydas Zvirblis

Definition

What is SOC?

- **SOC** - Security Operation Center is a structure within an organization or at a managed service provider employing **people**, **processes**, and **technology** to continuously **MONITOR** and improve an organization's security posture by **preventing**, **detecting**, **investigating**, and **responding** to cybersecurity threats.



The deification of the SOC

Perception

- SOC can solves all cybersecurity problems
- All problems can be solved within a few days
- Everything is done automatically by tools with minimal human intervention
- Security operations can be outsourced without knowing exactly what you want to outsource and how you intend to control the quality of service.
- You don't need to worry about cybersecurity yourself, the service provider will take care of it
- All responsibilities and duties can be transferred to a SOC service provider
- You don't need to be deeply familiar with your IT infrastructure, service provider will do.

- A service provider knows the company's risks and threats better and can identify them without deep dive in to the company IT infrastructure and business
- A service provider has a complete SOC service that is completely customized to the specifics of the company and can implemented in a few weeks
- A service provider has no problem hiring people
- A service provider has deep experience working with any IT solution used by company
- A service provider can provide all services without the support of company employees

72 Cybersecurity operations elements

Operationalization											Capabilities
Al Alerting	**In** Initial Research	**Th** Threat Hunting							**Ap** Application Monitoring	**Sm** Security Information & Event Management	**So** Security Orchestration Automation Response
St Severity Triage	**Ep** Escalation Process	**Ce** Content Engineering	**Sa** Security Automation					**Cl** Cloud Computing	**Ssl** SSL Decryption	**Em** Email Security	**Ips** Intrusion Prevention/ Detection Systems
Da Detailed Analysis	**Br** Breach Response	**Ti** Threat Intelligence Team	**Bl** Business Liaison	**Do** DevOps			**M** Mission	**Dl** Data Loss Prevention	**Url** URL Filtering	**Waf** Web Application Firewall	**Fw** Firewall
Mi Mitigation	**Pa** Preapproved Mitigation Scenarios	**Grc** Governance, Risk & Compliance	**Ft** Forensics & Telemetry	**Vm** Vulnerability Management Team	**Tt** Tabletop Exercises	**B** Budget	**P** Planning	**Cm** Case Management	**At** Analysis Tools	**Ept** Endpoint Security	**Ba** Behavioral Analytics
Ia Interface Agreements	**Cc** Change Control	**Rp** Red & Purple Teams	**Ea** Enterprise Architecture	**Se** SOC Engineering	**Eu** Employee Utilization	**Me** Metrics	**R** Reporting	**Nt** Network Traffic Capture	**Ed** Endpoint Data Capture	**Iam** Identity & Access Management	**Na** Network Access Control
Tu Tuning	**Pi** Process Improvement	**Hd** Help Desk	**It** Information Technology Operations	**Ot** Operational Technology Team	**Tr** Training	**S** Staffing	**F** Facility	**Th** Threat Intelligence Platform	**Vu** Vulnerability Management Tools	**Ms** Malware Sandbox	**Hp** Honey Pots & Deception
Ci Capability Improvement	**Qr** Quality Review	**Es** Endpoint Security Team	**Ns** Network Security Team	**Cs** Cloud Security Team	**Cp** Career Path Progression	**C** Collaboration	**G** Governance	**Am** Asset Management	**Km** Knowledge Management	**Mdm** Mobile Device Management	**Vpn** Virtual Private Networks
PROCESSES			INTERFACES		PEOPLE	BUSINESS		VISIBILITY		TECHNOLOGY	

Cybersecurity operations pillars

Prevent

Prevent everything you can with in-line and endpoint security

Detect, Investigate

Detect sophisticated threats

Response

Response and learn from each incident

Key SOC team roles

- **SOC manager** – Supervise activities of the SOC team. Hire and train workforce, measure relevant metrics and generate reports for external stakeholders, create and execute strategic plans for the SOC.
- **Tier 1 analyst** - responsible for looking into the alerts received daily to triage, classify and prioritize them. Open tickets for relevant alerts and forward to tier 2/3 tier analysts
- **Tier 2 analyst** – responsible for detail investigation to identify source of attack, methodologies used end etc. Collects data across tools, such as asset data, logs, and threat intel, to execute response efforts (Incident Responder).
- **Tier 3 analyst** – more proactive and focused on hunting threats. Review asset, vulnerability, low fidelity alerts, and complex threat intel data to identify shortcomings and capture stealthy threats before they affect the organization.
- **Forensic Investigator** – analyses incident data for evidence and behavioural information. They can work with law enforcement post incident.

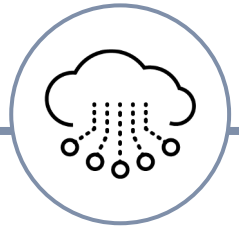
Key SOC team roles

- **Threat intelligence** - identifies potential risks to the organization that have not yet been observed in the infrastructure. Responsible for validating threats and then work with the security operations team to provide IOCs for the analysts and to update controls. Additionally, the deliver threat landscape reports.
- **Security Engineer** – Implement and maintain SOC tools

SOC Generations

- **I generation**
  - Building operation around a SIEM
  - Ingesting logs from big number different systems/solutions
  - Relies on a large amount of analytics who manually triage incidents, drowning in data lakes of security events that sooner or later become swamps, trying to find dependencies and meaning in an inordinate amount of logs.
  - A strong focus on network data in transit analysis
  - The belief that the collected logs can later be used for forensic analysis
  - In most case operation is reactive rather than proactive
  - …

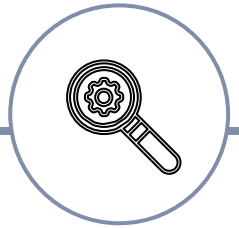
Improvement of security areas



Network

Perimeter

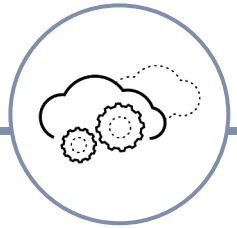
Zero Trust SASE



Data in transit

Unencrypted

Encrypted



Infrastructure

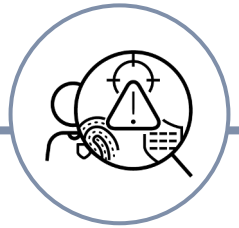
Data Center

Cloud

Endpoint

AV

EDR/ XDR



SOC

SIEM

???

SIEM expectations and reality

SIEM

✓ Log Analysis	Real Time Alert ?
✓ Log Collection	User Monitoring ?
? Log Correlation	Dashboards ✓
? Log Forensics	Reporting ✓
✓ IT Compliance	File Integrity ?
? App Monitoring	System & Device Monitoring ?
? Object Access Audit	Objects Access Audit ?

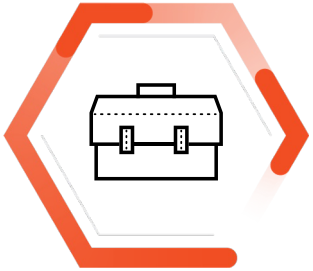
- **SIEM** was originally designed more as a compliance tool, log “searcher”

Enemies of the SOC

Too Many Low Fidelity Alerts

Investigations are Time-consuming

Repetitive Manual Tasks



Too many products to piece together an incident

Shortage of staff and skills

Alert Fatigue

SOC IMPACT:

Important threats are missed

90%+ Analyst time spent responding to alerts

Long response to real incidents

Tired, demotivated team

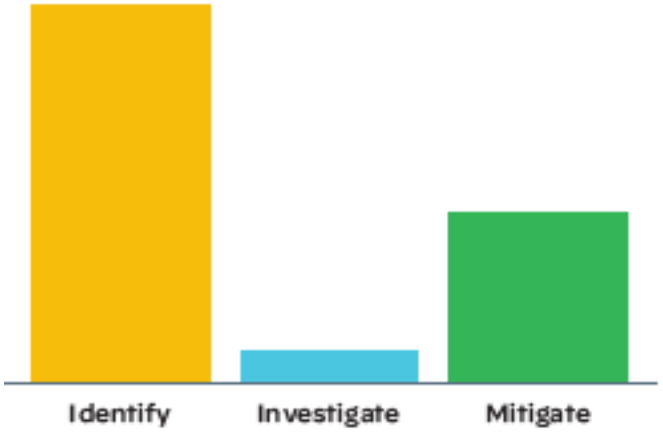
High staff turnover

Continuous Firefighting

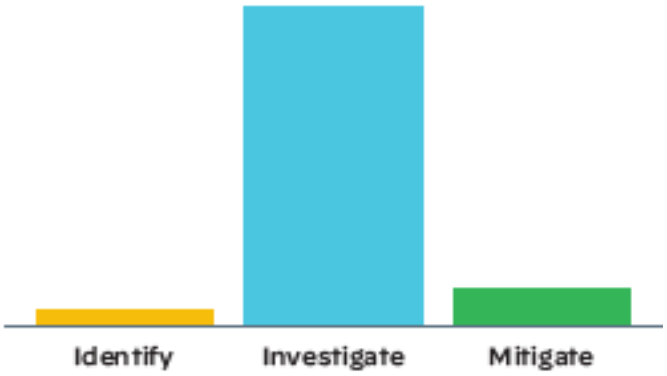
Large SOC Teams

High Analyst Turnover

Time consumption



Traditional analyst time allocation

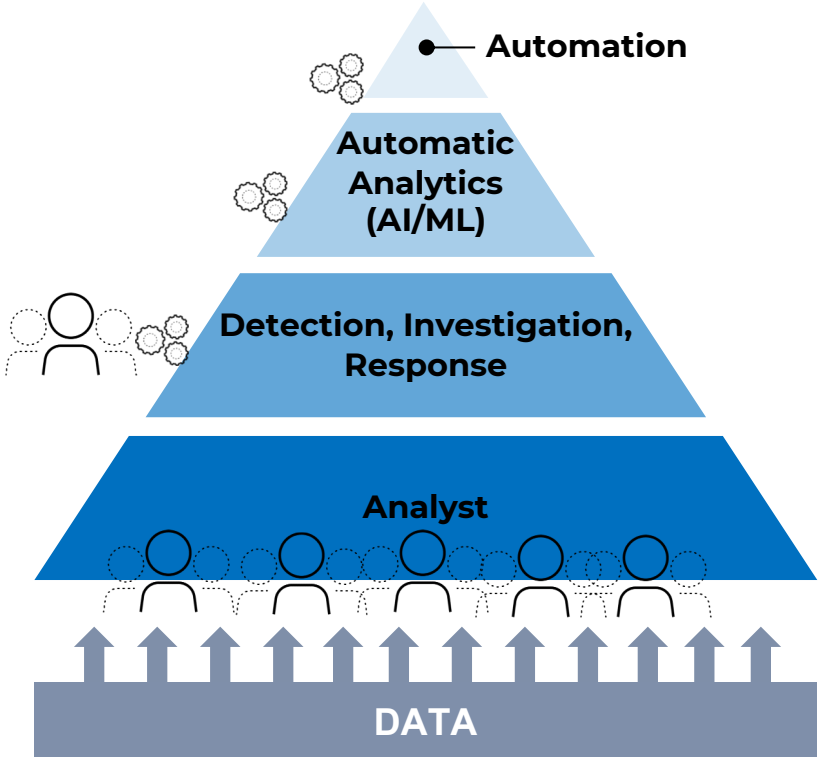


Ideal analyst time allocation

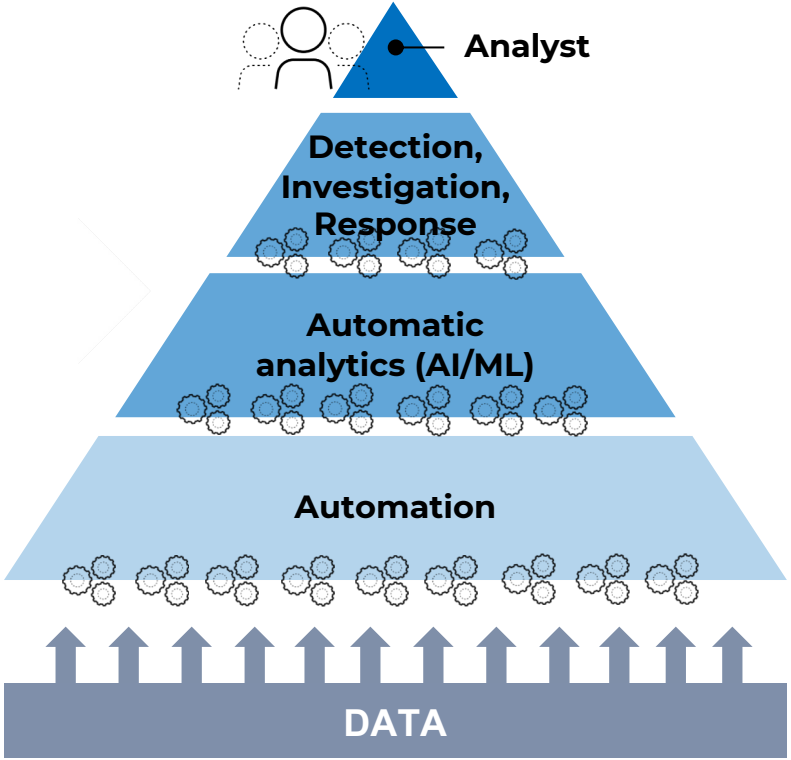
The purpose of security operations is to identify, investigate, and mitigate threats.

SOC generations

I generation



II generation



SOC Generations

- **II generation**
  - Automation-first, not human-first approach - automatic data analysis, triage, stitching, correlation, response, protection, detection.
  - Proactive operation
  - Integrated threat intelligence in the SOC tools.
  - Ingesting logs only from sources having value for monitoring, analysis, response, prevention
  - …

II generation SOC approach

- **Prevention First** - prevent as many threats as you can before they breach your environment, reduce the number of alerts going to the SOC.
- **Detect and Investigate** - detect and investigate the threats that can't be prevented such as a zero day attacks. Better visibility and insight into detecting stealthy attacks from deep, detail data triaged from multiple sources including the network, endpoint, and cloud. Security events from multiple sources stitching to alert.
- **Response** - automatic or manuall response thouth the inline firewalls, agent on the enpoints etc.
- **Vendor intelligence** – continuous improvement of prevention, detection, investigation and response using the intelligence of the leading vendor.

I generation vs II generation

I generation SOC	II generation SOC
Valuable results within 6-12 months	Valuable results within 2-4 weeks
Monitoring	Monitoring
Reactive	Proactive
	Prevention
	Detection
	Response
	Integrated intelligence

Open questions to consider

customer tools

or

service provider tools

Open questions to consider

24x7 or 8x5

Open questions to consider

SOC for common IT infrastructure

vs

SOC for custom applications

Santa Monica Networks

Thank you