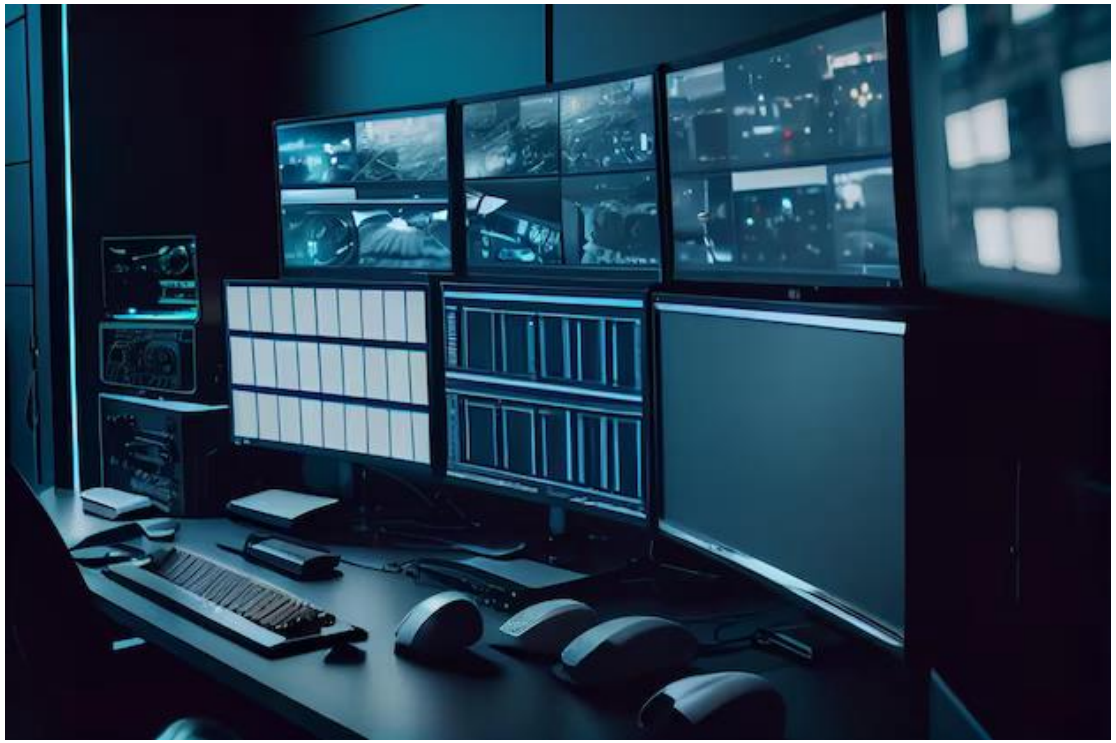
Santa Monica Networks

Uncertainty of Cyber Security: Human Role in SOC

dr. Dovilė Kėrienė

SOC – How we visualise it



- Automation of everything
- Lots of beautiful visuals
- AI based automation and decisions
- No human input
- Immediate response
- Magic

SOC is firstly people – with critical thinking, who knows where tools are wrong

What SOC really is

Key Impact:

- **End-Users** – carelessness, curiosity, greed, emotions
- **Managers** – rush, delegation of responsibility, “I pay you to do the job”
- **IT & admins** – simply “Know IT all”
- **Hackers/villains** – financial benefit, political statement, egocentricity, curiosity…

Up to 50% of organisations don’t have SOC in any format

- **NOC** – to provide full visibility to infrastructure and all its components and equipment
- **Physical security group** - protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise
- **SIEM** – compliance and log collection
- **CISO office** – regulatory compliance assurance and escalation to management, in case of non-compliance
- **MSSP** – takes care of various security duties on the company's behalf, enabling them to concentrate on their main business functions

Top incident types:

- Ransomware
- Malware
- Social engineering
- Data leak
- Availability threats
- Disinformation
- Supply chain attacks

Top threatened sectors:

- **Government (24% escalated incidents)**
- E-service providers (13%)
- Public sector (12%)
- Services (12%)
- Finance/banks (9%)
- Healthcare (7%)

Top Lithuanian of 2023:

- Government (25%)
- Security and defence infrastructure (13%)
- Business (7%)
- Finance institutions (5%)
- Energy infrastructure (5%)
- Telecommunications (5%)
- Transport (2%)
- Other (38%)

New trend – **Hybrid attacks** – combined physical and cyber attacks (eg. Danish railways network attack, 2022 November)

Top vulnerabilities & vectors

Vulnerabilities:

- Server Security Misconfiguration 38%
- Cross-site scripting (XSS) – 13%
- Broken Access Control - 11%
- Sensitive data Exposure – 10%
- Authentication and Sessions– 8%

Vectors:

- **Employees / insider threats**
- Mobile devices and BYOD Policies
- Internet of Things (IoT)
- Misconfiguration

Conclussion – main attack vector is enendpoints

Threats Shortlist*

- Supply chain compromise of software dependencies

- Rise of digital surveilance authoritarianism/loss of privacy

- Targeted attacks enchanced by smart device data

- Rise of advanced hybrid threats

- Cross border ICT service providers as a single point of failure

Advanced disinformation campains

Human error and exploited legacy systems within cyber-physical ecosystem

Lack of analysis and control of spacebased infrastructure and objects

Skill shortage

Artificial Intelligence Abuse

*ENISA threats for 2030

- Threat actors - from cybercrime to hacktivists
- Motivation – from financial to political
- Type – from volumetric, volume & protocol based to app. layer and protocol-based attacks
- Volume (in 6 years):
  - from 6 DDoS attacks / 2 RDDoS to > 413 DDoS attacks
    - (51 claimed by hacktivists)*
- Lithuania (2022/2023) – from 43 to 98 DDoS attacks

Security - is a state of being free from danger or threat

Cyber Security – is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks

SOC function – to ensure cyber security by monitoring, preventing, detecting, investigating and responding to cyber threats around the clock

Technology?

- In itself, never makes mistakes
- Does, what people tell it to do

Processes?

- Do not act on their own
- Set of steps that people follow

PEOPLE:

- They are complex and make their own decissions
- Are those decissions always correct?

HUMAN?

Definetely – HUMAN:

- Recless uneducated employees (~40% hide incidents from security department)
- Insider threats, weak passwords, unauthorised data sharing, BYOD

Wrong attitude and lack of responsibility:

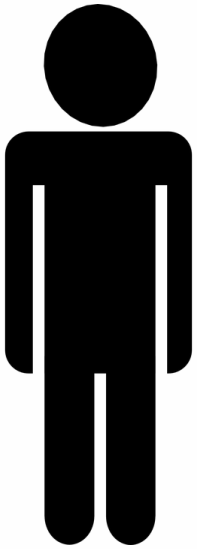
- I am / my company too small to be interesting – the OWNER
- That's too complicated to use – EMPLOYEES
- Why I cant use FB Messenger for business – even OWNERS / MANAGERS
- I have / pay people to think about it – especially OWNERS / MANAGERS

What is Human Role?

Humans, why?

- Trusty by nature
- Creatures of habbit and routine
- Too busy to pay attention to details
- Emotional

Convenience instead of security



Many roles who makes a difference:

- of organisational leaders
- of IT department
- of Help Desk
- of communication
- of employees

Many roles:

- of organisational leaders, of IT department, of Help Desk, of communication, of employees

Human element in cybersecurity is usually underestimated, but can be either the strongest defense or weakes link

SOC deals with uncertainty everyday:

- Unpredictability of the future events
- Obsolescence of hardware and software
- Innovative tactics of cyber criminals
- Even ”Act of God”

Uncertainty can become risk or reward:

- All depends on type and time of decissions made

90% of incidents starts from human error:

- Skill based errors
- Decission making errors

Unintentional actions – or lack of actions:

- Misdelivery, password problems, patching, physical security errors

Factors:

- Opportunity, environment, lack of awareness

Insider threats – most costly and difficult to eradicate

Business continuity management:

- Risk management plan
- Business continuity plan
- Disaster recovery plan
- Forensic readiness
- Contingency planning

Otherwise, usefull thing during crisis:

- Paper, pen, stapler…

- National legislation:
  - National Cyber Security Centre Cyber security incident management plan
  - Critical infrastructure regulations
  - National Cyber Security Law

- European legislation:
  - EU Cyber Security Strategy
  - GDPR
  - NIS2
  - AI (coming soon)

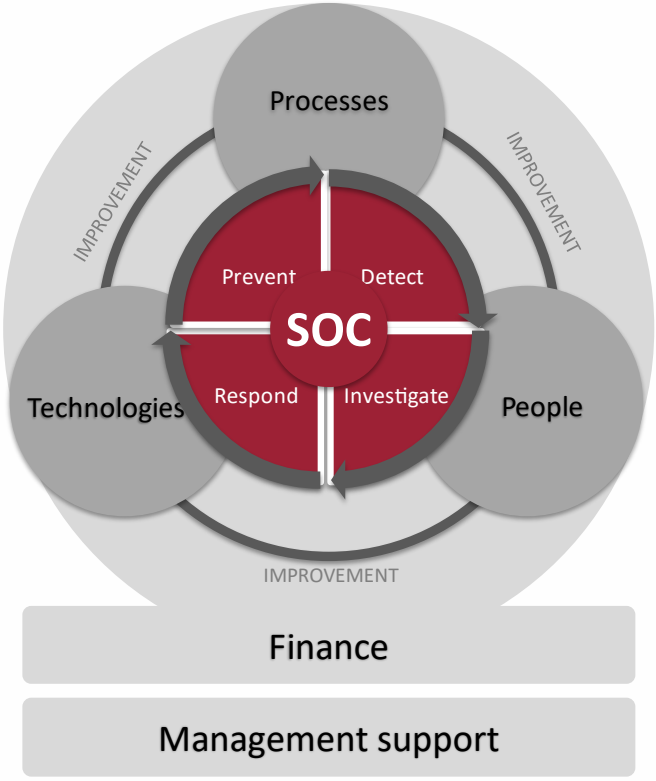
Cyber Security Insurance

- A way to mitigate cyber security risk to the third party
- Cyber security policies and procedures have to be in place and regularly updated
- If incident happens – insurance provider might take over incident handling
- What to include/consider:
  - Risks the organisations faces, triggers to activate policy, cost
  - Types of incidents, extend of coverage, first-party and third-party loses
- Lithuanian insurance companies does not provide such service

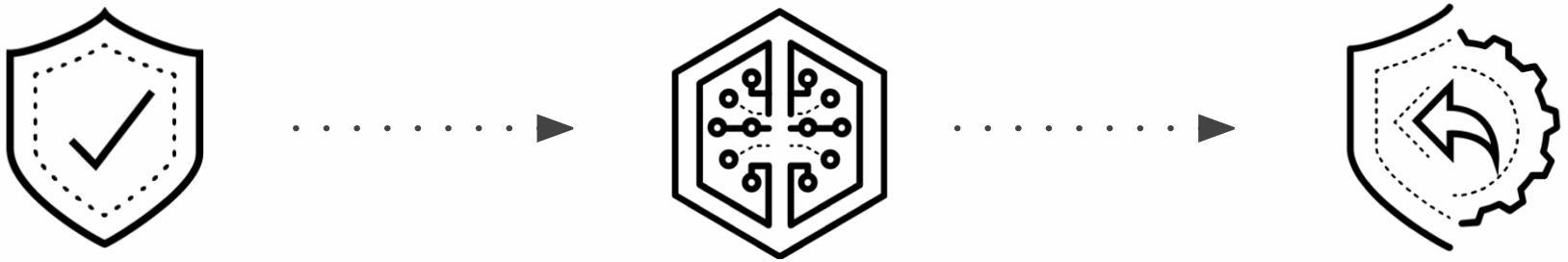
SMN SOC

How do we deliver SOC

- A structure within an organization or at a managed service provider employing
- People, Technology, Processes
- Continuous monitoring and
- Improvement of organizations security posture by:
  - Preventing
  - Detecting
  - Investigating
  - Responding to Threats



We use Pro-active strategy



Prevent

Prevent everything you can with in-line and endpoint security

Detect, Investigate

Detect sophisticated threats

Response

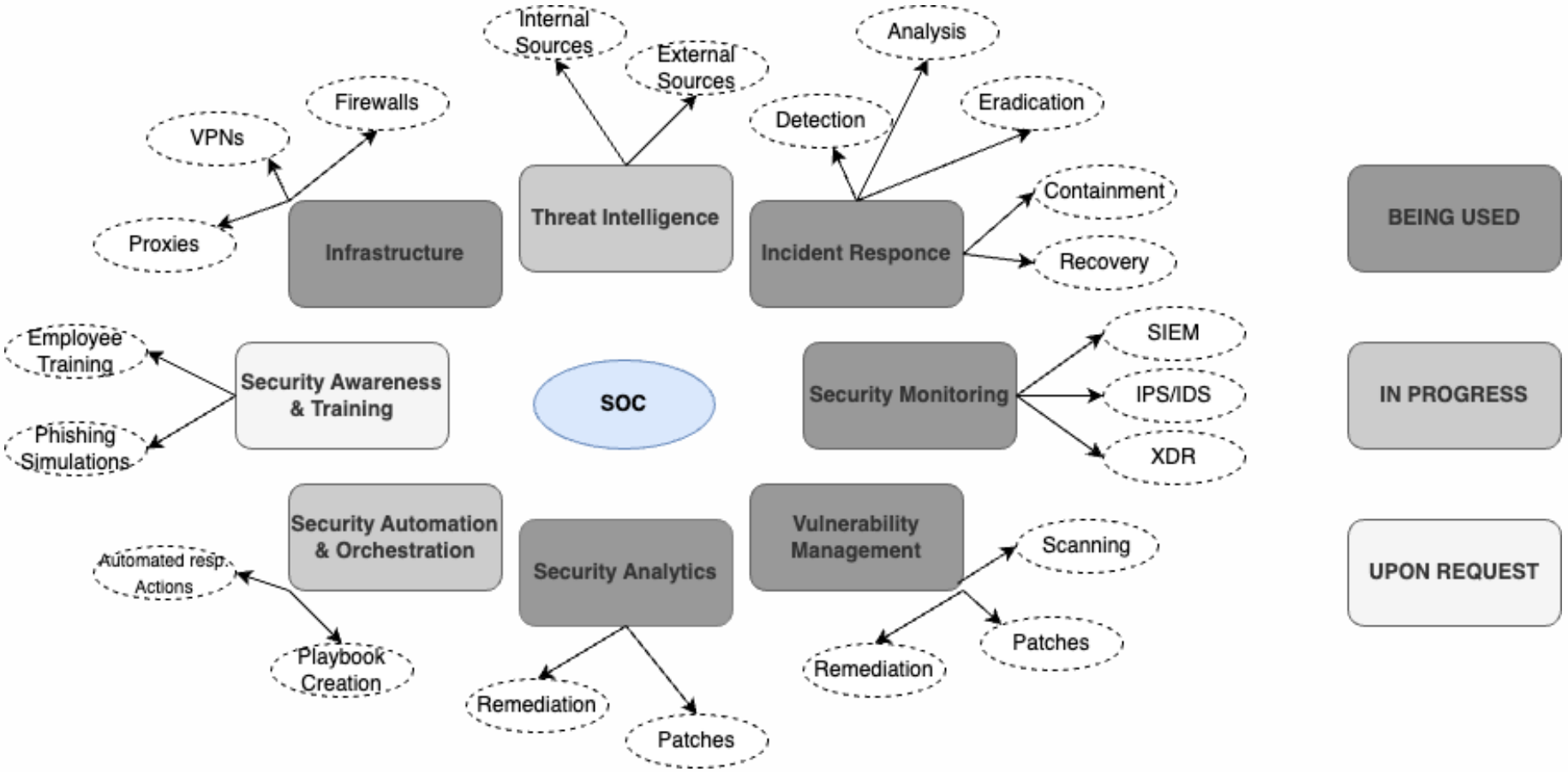
Response and learn from each incident

Santa Monica Networks

Threat prevention by monitoring:

- **Endpoints** – workplaces and servers, where OS is running (Windows, iOS, Linux)
  - Covered with agents
- **Network traffic analysis** – firewalls, IPS/IDS - PaloAlto, Fortinet Checkpoint
- **Integrations**:
  - MS infrastructure logs (cloud / on-prem)
  - Other third-party products
- Our used monitoring tools : **XDR or XSIAM**

Scope of SOC services



Santa Monica Networks SOC scope

- 24x7 or 8x5 monitoring

- Formal side: contract, SLA&KPI, reporting

- Pre-service evaluation of security maturity:
  - Policy and procedure readiness, inventory and infrastructure readiness
  - Security gaps identification
  - Required monitoring scope evaluation

- SOC process - prevention, protection, detection, response:
  - Endpoints, cloud, network, SOAR, threat management, forensic management, technology management and communication

- Incident management: (identification, triage, response, improvement)

- Our SOC technology support

- Other (behavioural analysis, user awareness improvement, licensing, …)

Proposed SLA

- When to choose 24x7 or 8x5 monitoring?
- Do you know your monitoring scope?
- What actual SLA your services requires?
- Do you have all policies and procedures and communication plans in place?

	INCIDENT MANAGEMENT				CHANGE / REQUESTS MNG
	Critical	High	Medium	Low	Low
REACTION TIME	30 min	1 hr	1 hr	1 day	1 day
RESPONSE TIME	2 hr	4 hr	8 hr	2 days	1 day

- REACTION TIME – duration of time, incident noticed, acknowledged and assigned
- RESPONSE TIME – duration of time, from incident recording to first containment

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 – is automated role using our selected tools

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

Additional SOC team responsibilities

Forensic Investigator – analyses incident data for evidence and behavioral information. They can work with law enforcement post incident

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

Lawyer support – legal help during crisis

Client representatives – responsibilities defined in communication plan and Service procedures

Weekly (on-demand):

- Summary of incidents and their management during the week

Monthly/quaterly report:

- Analysis of incidents during reportng period and their tendencies in time (critical/high incident separately)
- Communication with third parties, if such
- Services and security improvement suggestions
- Client threats monitoring and vulnerabilities elimination recommendations

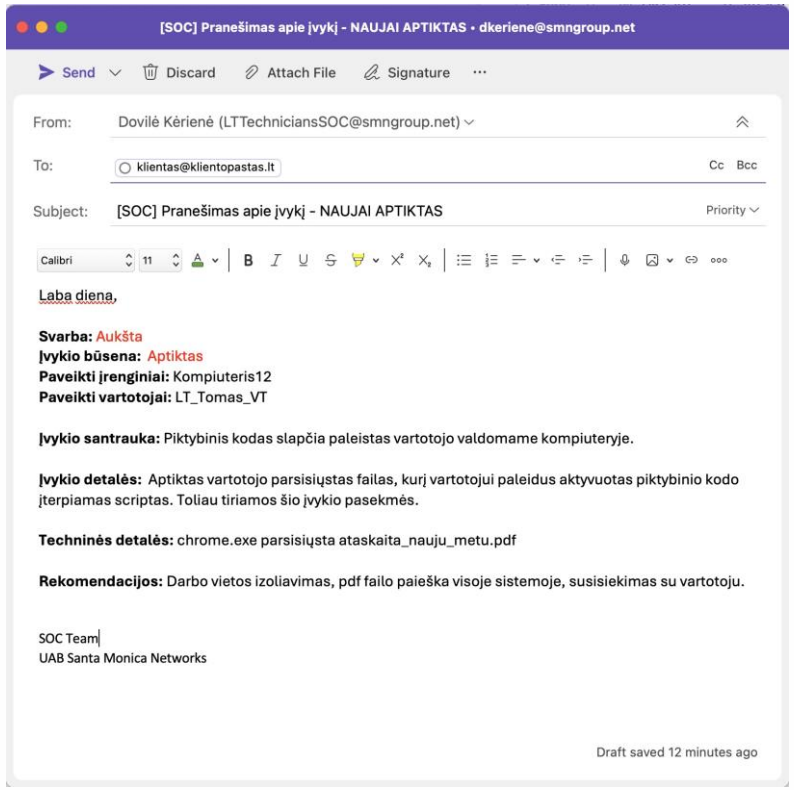
Meetings:

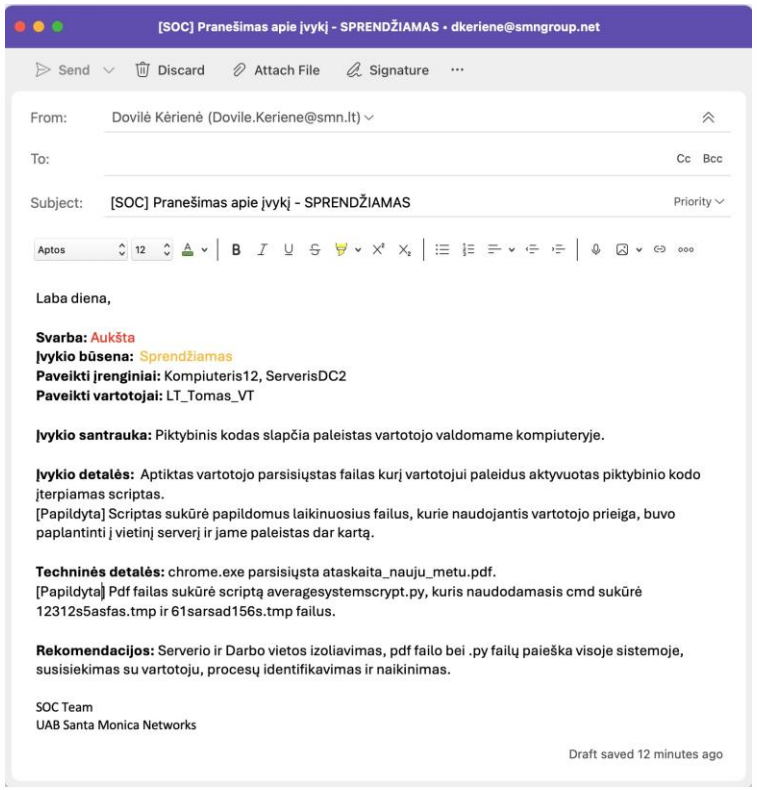
- On-demand – critical / high incidents management and escaltion
- Regular – for service level and quality overview

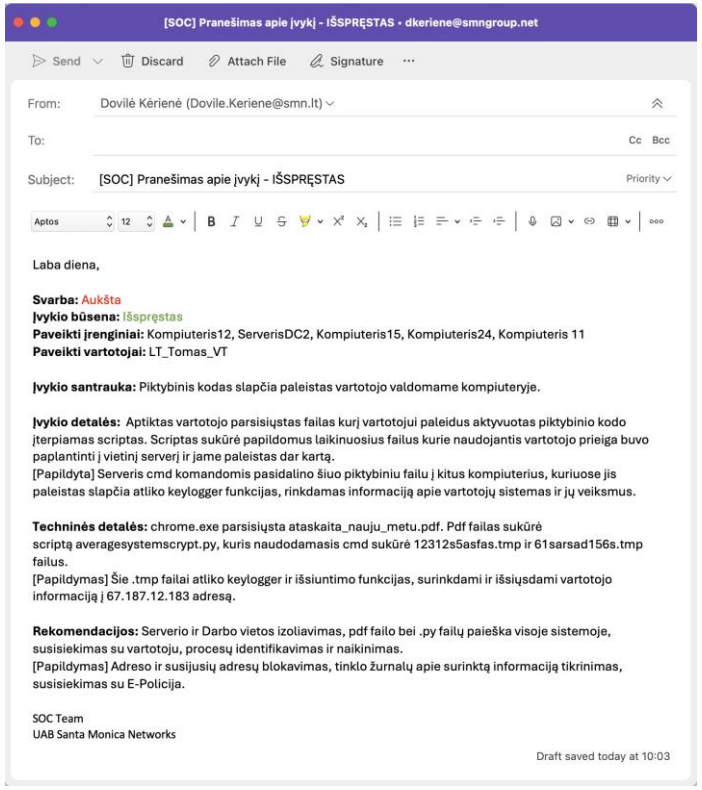
Communication:

- Email / phone – incidents, their management, progress reporting
- Third parties – on critical / high incidents, including govermental bodies

Communication during incident







Data security and privacy assurance:

- Cloud based technologies used
- Data storage only in EU area servers, which comply with reguired security standards

Data archival:

- Full data archival - month
- Incident data – half a year
- Or – as agreed with client

Data can be exported to client infrastructure any time

Service delivery complying ISO 27k

- Technology based input
- Vendor based databases
- MITRE ATT&CK, MISP
- Our own threat research
- Incident notifications from constituents
- OSINT?

Prevention First - prevent as many threats as you can before they breach your environment, reduce the number of alerts going to the SOC.

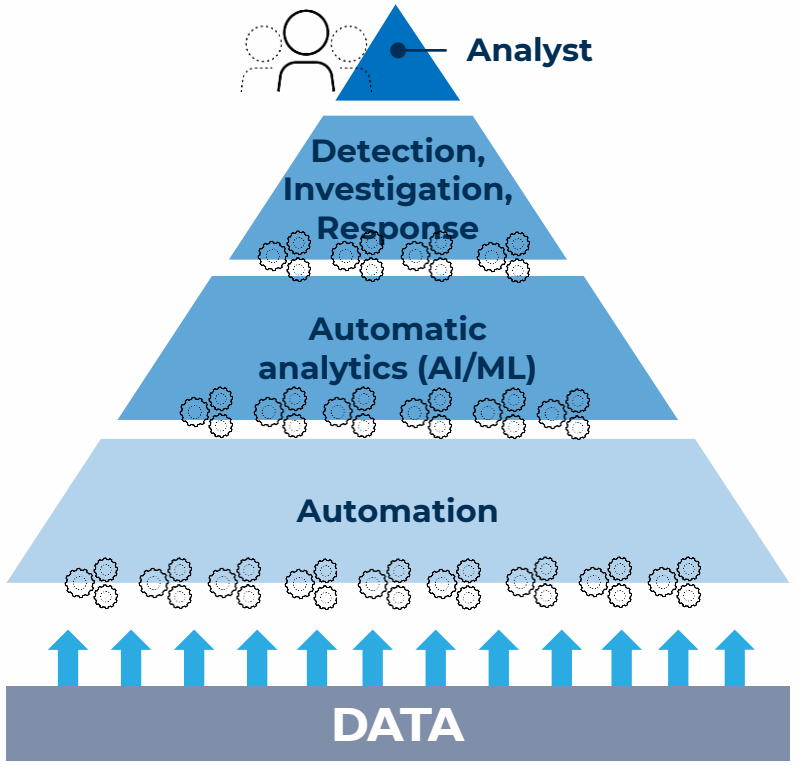
Detect and Investigate - detect and investigate the threats that can't be prevented such as a zero-day attacks. Better visibility and insight into detecting stealthy attacks from deep, detail data triaged from multiple sources including the network, endpoint, and cloud.

Response - automatic or manual response though the inline firewalls, agent on the endpoints etc.

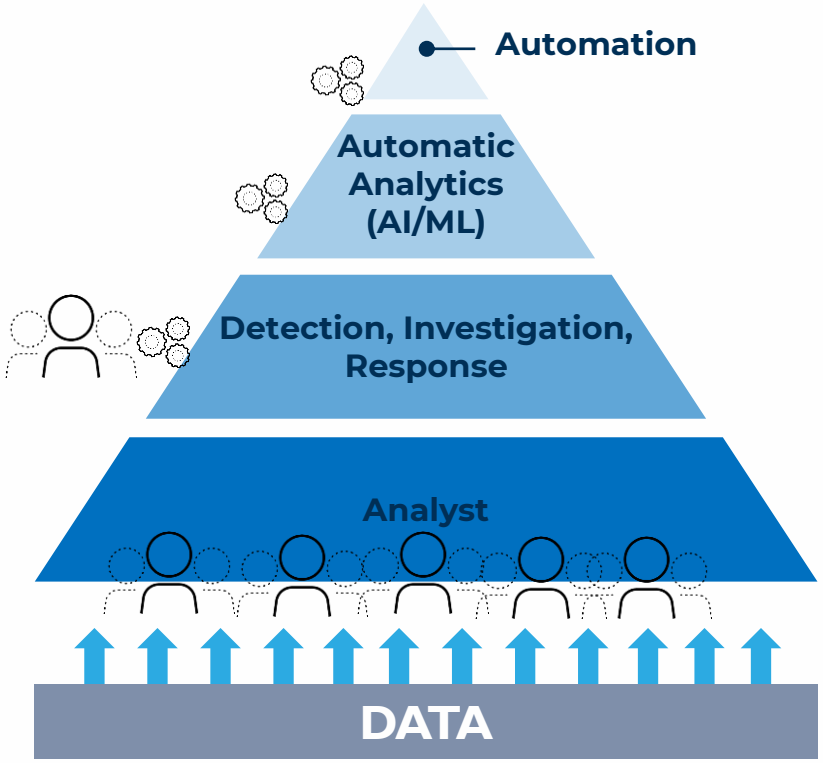
Vendor intelligence – continuous improvement of prevention, detection, investigation and response using the intelligence of the leading vendor.

SOC Generations

SMN SOC



Other SOC



Key Take Aways

- Raise user security awareness:
  - from CEOs, to analysts, end-users
  - make understand the price
- Educate user to detect and report incidents
- Think as an attacker
- Go to next level thinking:
  - forget - ”we have spent money, and nothing happened”
- You get what you give yourself
- Invest in resilience ~ 80% if budget
- Feedback, feedback, feedback