Building your own SOCaaS

"The untold story of many sleepless nights"

whois

Bogdan Cazacu

Founder & CEO of SecretChip Consulting

Senior DevOps Engineer

...

dig -t all secretchip

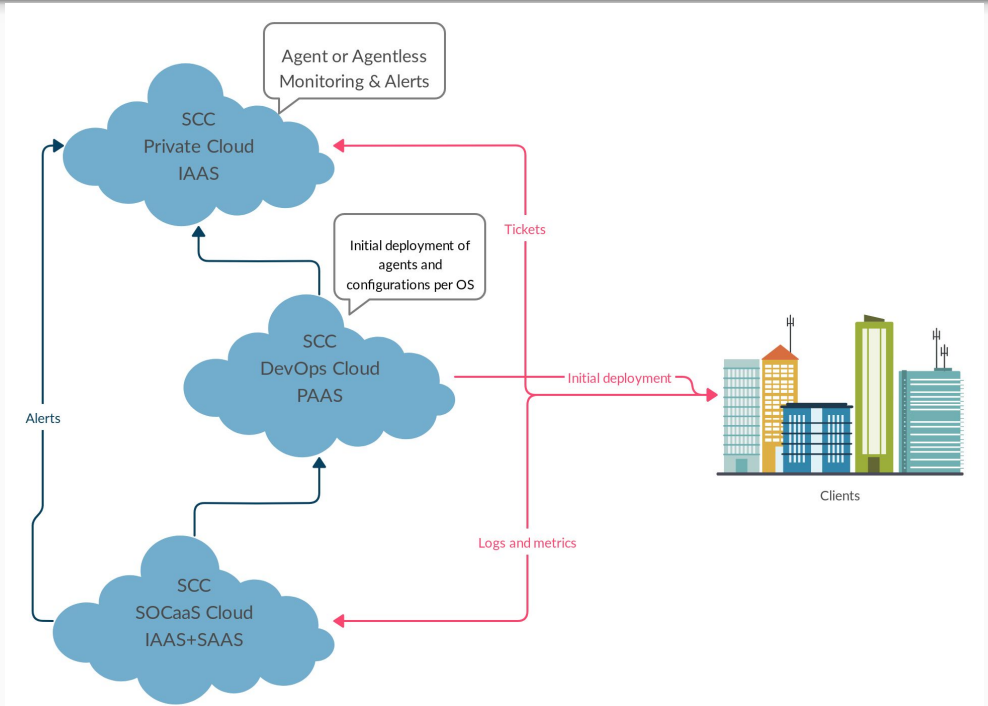
Small MSP based în Bucharest

Working with SOHO’s and SMB’s across Romania (none in Cluj...yet) în providing remote support and security services all in one package

Broad know-how in architecture, implementation and operation of complex IT infrastructures

Building the next generation public cloud capable of satisfying even the most picky of our partners

strace secretchip



select * from SOC.db where type = “SAAS” or type = “In-House”;

In house SOC

- Is a service offering that allows an MSP to have access to an exclusive, dedicated network of experienced security analysts to supplement or scale their existing teams.
- Who’s it suitable for? Dedicated SOCs are best suited for MSPs who have existing security products and teams but are struggling to cover 24/7 shifts, or for those who want to scale their existing security operations to meet customer demand. Dedicated teams are also the perfect option for MSPs who want to retain control and transparency over their security operations.
- Time to market: As Dedicated SOC teams operate within your existing framework, it can take 1-2 months to integrate and launch.

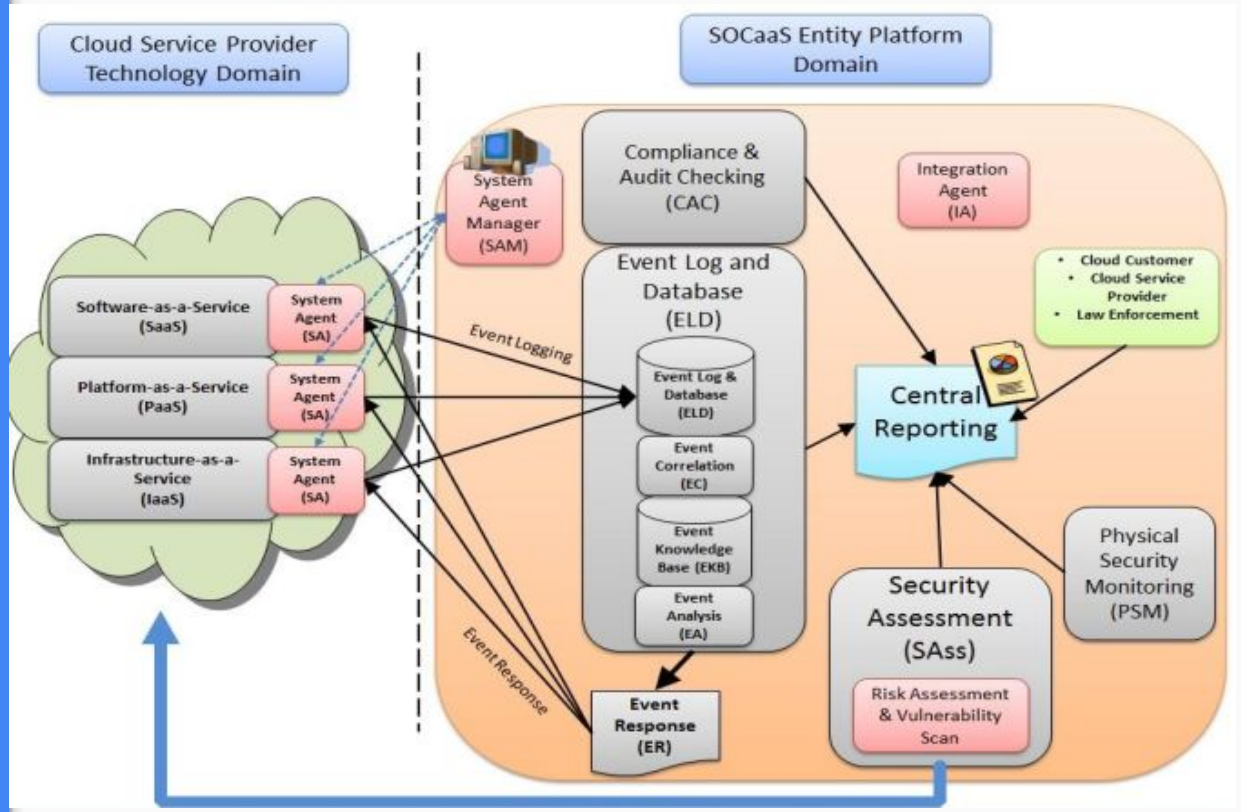
Managed SOC (aka SOCaas)

- Ideal if you’re an MSP whose customers are relying on you to monitor, detect, and respond to today’s cybersecurity threats and you currently don’t have an existing 24/7 SOC.
- Reduces time to market: Setting up a Managed SOC is usually fast, and can take anywhere from a few days to a few weeks. On top of this, it’s a service-based delivery model that is designed to scale with your growing security needs.
- Many SOCaaS providers have built their offer with little flexibility in mind. This often forces MSPs to stray from their desired delivery method or strategy in favor of quickly getting security solution to market

strace SOCaaS

Main advantage of a SOCaaS

Detection of malicious events that a single information security application or one layer of security devices may fail to recognize. Monitoring of all cloud services and processes through the collection of cloud security system events and logs enables efficient and effective event analysis and response on a 24/7 basis.



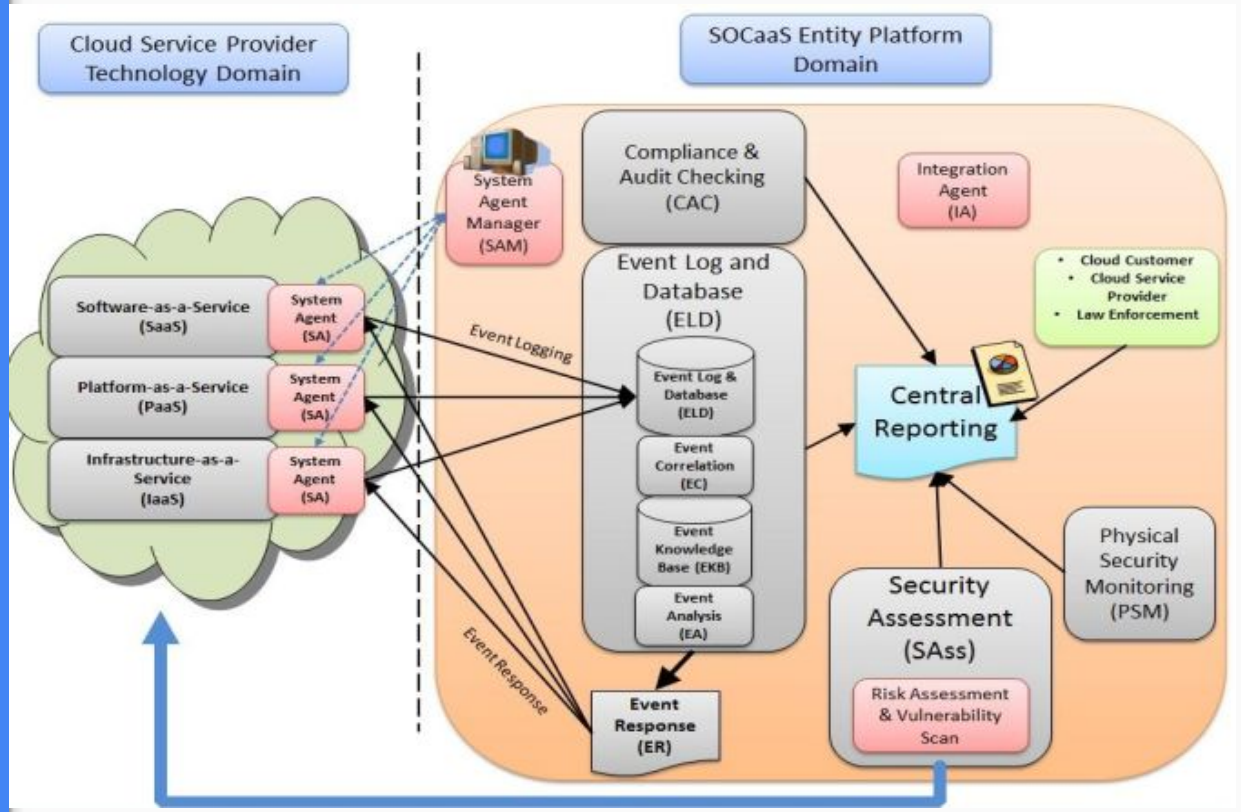
strace SOCaaS

Another important advantage is reduce cost to market (if you know what you're doing)...

Costs can range from $ to $$$ per month depending on your hosting provider mainly.

Also the open source community has some nice tools to help you get started with log management, databases, SIEMs, vulnerability scanners, etc.

Ask me about some of the tools after the talk :)



What tools do we use?

Alienvault (SIEM)

Checkmk (Network Monitoring)

Snort (IDS/IPS)

OSSEC (HIDS)

Nessus (Vuln Analisys)

Ansible (automation)

ELK (Logging)

Faraday (Networks Security Assessments)

MISP (Malware Information Sharing Platform)

Alienvault OTX (Threat Intelligence)

OpenVAS (Vulnerability Scanning)

What tools we want

Ghidra (Reverse Engineering)

Cuckoo (Sandboxing)

Questions?

Follow me @cazacub

Email me @ MayDay2019@secretchip.ro