Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on May 21, 2024 and its most recent report on Form 10-K filed on September 7, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

splunk> .conf24

Building a SOC from Scratch with Splunk® Enterprise Security

SEC1345C

.conf24

splunk>

Bring on the future.

Breaking Out Session

Combining our strengths,
protecting tomorrow

Speakers

Maxime Massant

SOC Engineer
COVEA

Julien Vallee

Cybersecurity Expert
COVEA

splunk> .conf24

Who is COVEA ?

Combining our strengths, protecting tomorrow

Our brands

Since 1951

MAAF

Since 1828

MMA

Since 1934

GMF

Since 1993

PartnerRe

Our values

- Solidarity
- Responsibility
- Innovation

Covea is the leader in goods insurance in France

10,8 millions
Insured vehicles

8 millions
Insured homes

Property and liabilities

COVEA in Numbers

12,000

Servers

With up to 1,500 applications

6

Main sites

2,400 Sales Point

40,000

Workstations

32,000

Users

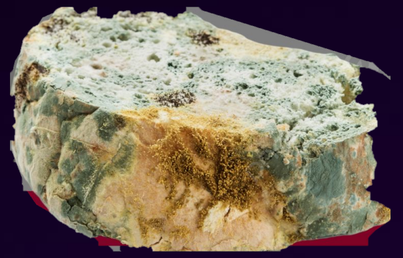
COVEA's Learning in Cybersecurity?

In July 2020 COVEA was victim of a Ramsomware.

Following this Major Cyber Incident Covea decided to launch a strategic project in order to strengthen its cybersecurity.

The first step was to audit the operation of its security tools.

Old Proprietary SIEM System.



Log Loss

Many uncontrolled log losses, making the detection system defective.

30% True Positive

The vast majority of alerts are unqualified and random.

56 Rules

Few rules and very limited customization of whitelists and blacklists.

Nothing to keep.

Remind our Strategy.

More flexible, more accuracy.

SIEM is the cornerstone of security alert detection and incident investigation for the SOC COVEA.
We must have quick « GO to Market »

- Flexibility
  - Agile build method
  - Agile partners
- Accuracy
  - Focused on result
  - Keep under control

Why did COVEA choose Splunk?

Two main reasons

Time To Market

- Ability to get up and running quickly
- Interoperability with our source log
- An extensive catalog of detection rules
- Focused on product strategy

Maintainability

- MSSP's ability to operate the solution
- Availability of human resources
- Scalability
- Long term Experience
- Learning and Certification

THE Plan.

Keep under control the transformation to SPLUNK SIEM

Remind Security Strategy

- Which perimeter
- Which Legals logs (NIS1, NIS2 , DORA, HADS/HIPAA …)
- Which sources
- Which Logs types (Sourcetype)
- Which evolution and goals

Create Adaptative SIEM

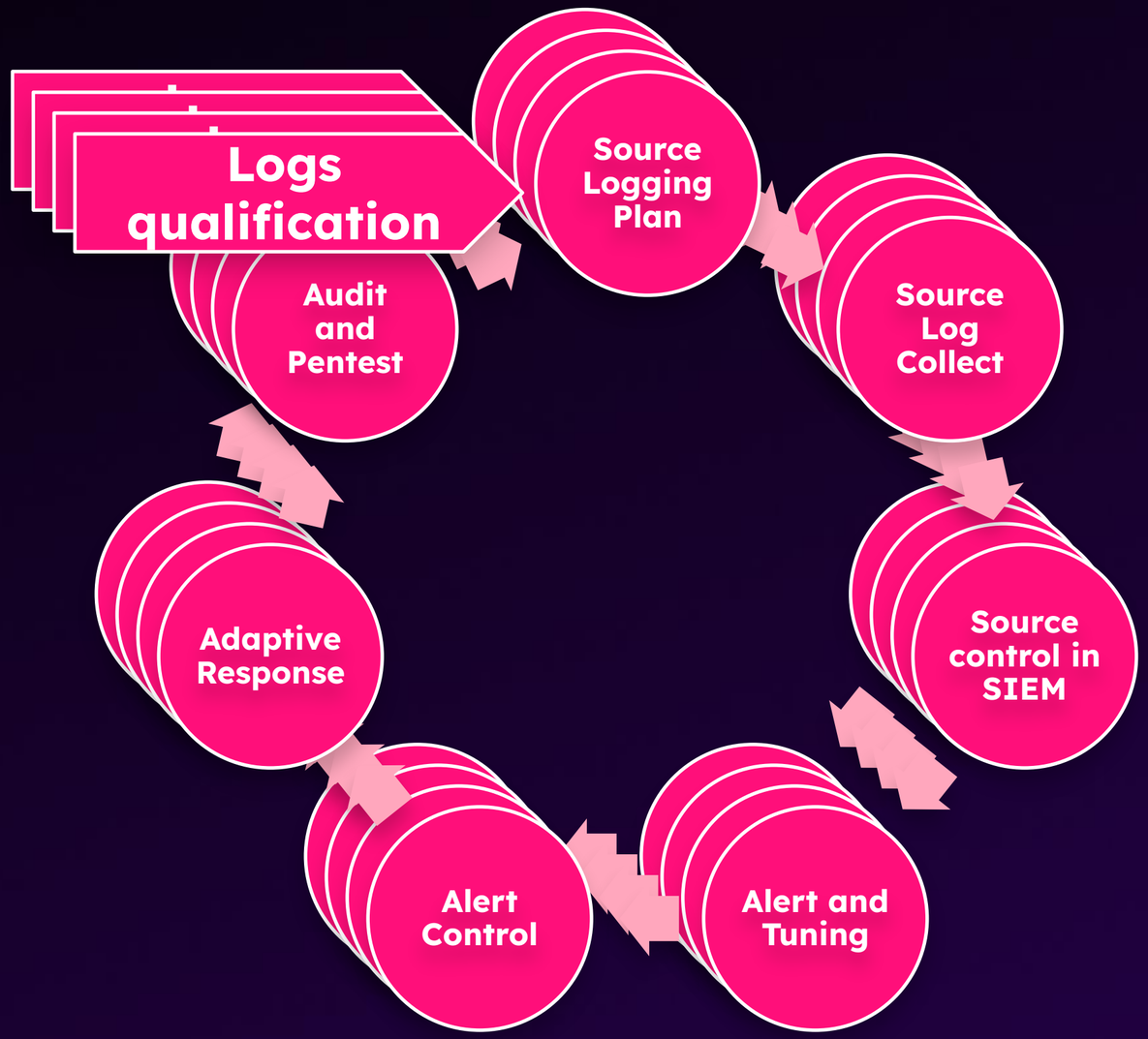
- Scalability
- Redundancy
- Accuracy
- Flexibility
- Interoperability

SOC Operation

- Alert associated with an incident response
- Easy maintenance in operational condition
- Customization of rules for production

THE Method.

Agile circle progress.



Result After 6 Months.

Keep under control the transformation to SPLUNK SIEM

Remind Security Strategy

- Spread over 3 data centers and Cloud infrastructure
- 750 hosts sending logs
- 45 different sourcetypes
- 2 To logs per day
- Coverage of Legals logs
- All qualified Logs

Create Adaptative SIEM

- Scalability of 12 appliances and Splunk Cloud
- Redundancy behind Load Balancer
- Accuracy with CIM model
- Flexibility of lookup update
- Interoperability with XSOAR for alerts treatment
- Connection to API Cloud

SOC Operation

- 110 Alerts associated with a response (290 alerts comparing to old system)
- 20 datamodels acceleration
- Automation SOAR for alerts treatment (playbooks)
- Customization of 20 rules protecting business activity
- 46 users of Splunk
- 57 TTP MITRE ATT&CK covered

New SPLUNK SIEM System.

No Log Loss

Under control log losses, making the detection system efficient.

80% True Positive

All alerts are qualified , treated and responded.

286 Rules

Custom rules and very flexible customization of whitelists and blacklists.

What’s Next.

- RBA implementation (identity and assets management)
- IA integration
- Specific applicative detection rules
- Spread SIEM to SUBSIDIARIES.

Thank you