CyberRes

# Optimizing your SecOps Program

## …with our CyberRes Galaxy Portfolio

Markus Sell
Sr. Product Manager | CyberRes Galaxy
2022-04-27

# Agenda/Outline

## Why

… TI & Galaxy

## What

… can Galaxy do for you

## How

… do we do what we do

## Next Steps

# Why Threat Intelligence

# What is Threat Intelligence…

Information about Cyber Threats which help me making informed decisions.

---

Thus, enabling my Security Operations practice to be more
effective and efficient in protecting our business against threats that matter to me.

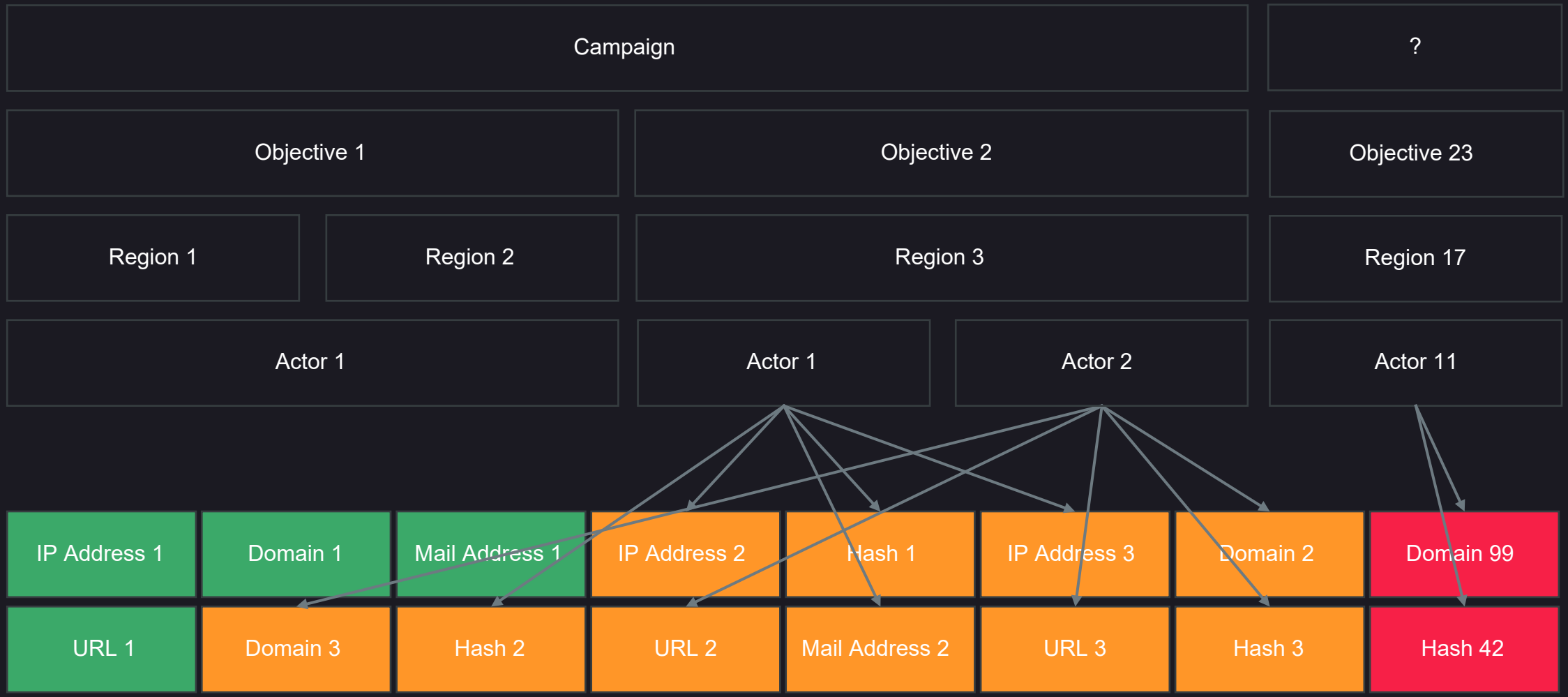
# What is Threat Intelligence…

## … and why should we want it?

- Indicator driven „Threat Intelligence“ lacks giving you answers to significant questions!
- Is the threat feed driving my activities…
  - …complete?
  - …reliable?
  - …accurate?
  - …generic or relevant?
- Where are my blind-spots?
- What else?

# What is Threat Intelligence…

## … and why should we want it?



# Why Galaxy

# *Why* did we build it

- Reshaping the Threat Intelligence space
- Business at the center of Threat Management
- Leveraging optimization potential
- Realign focus
- Not to replace, but to complement
- …

## WHY

Threat intelligence needs to be reshaped in that it needs more of an INTEL touch and less an INDICATOR touch.

Offerings available seem to be focusing on technical audiences and the shipping of indicators of compromise.

## HOW

By providing a complete set of capabilities which enable our customers to do research, prioritization, detection, triaging and response, supported by business relevant metrics .

# *Why* did we build it

- Reshaping the Threat Intelligence space
- Business at the center of Threat Management
- Leveraging optimization potential
- Realign focus
- Not to replace, but to complement
- …

## WHY

Threat management is a topic for business as it threatens the business, simply that. Furthermore, threat intelligence solutions in most cases today, still struggle providing proper prioritization capability, leaving Security Operation Centers alone still suffering from workload issues and false sense of security.

## HOW

We refocus threat intelligence from a bottom-up view to a top-down view. Coming from business metrics like financial impacts of threats, business operations impact or industry/regional relevance of threats. In addition, we offer additional views to make prioritization decisions.

# *Why* did we build it

- Reshaping the Threat Intelligence space
- Business at the center of Threat Management
- Leveraging optimization potential
- Realign focus
- Not to replace, but to complement
- …

## WHY

Because we believe, that current offerings are, in most cases, too practitioner focused. Focusing on potential issues “just because the TI feed told me to do” creates a lot of overhead and it might turn into creating more work than it helps.

Data quality in threat feeds is even more important then elsewhere, because we tend to trust it and rely on it.

## HOW

Providing business context drives confidence and offers another level of context to make right decisions quicker.

# *Why* did we build it

- Reshaping the Threat Intelligence space
- Business at the center of Threat Management
- Leveraging optimization potential
- Realign focus
- Not to replace, but to complement
- …

## WHY

The focus of existing TI platforms is, to provide customers with "intelligence" about what can happen, because someone saw this IP somewhen somewhere doing strange things.

This is good to have but does not provide a solution to the real problem which is: Knowing what has happened.

## HOW (late summer)

With Far Space analytics, based on Internet signaling, we can catch things while they are boiling, not only after they boiled over. And we can focus on things, relevant to the customer with "zero touch" integration.

# *Why* did we build it

- Reshaping the Threat Intelligence space
- Business at the center of Threat Management
- Leveraging optimization potential
- Realign focus
- Not to replace, but to complement
- …

## WHY

We believe, that multi vendor strategies make sense in many cases where confirmation of assumption leads to better decisions and more robust service delivery.

## HOW

We add business context and prioritization mechanisms. By making threat selections actionable in our detection technology stack, we also provide a way to combine multiple threat feeds information sources to increase robustness of decision, reliability of findings, reduction of false positives and increase efficiency of security operations resources.

# What can Galaxy do

# Our Mission

The CyberRes Galaxy brand combines an ecosystem of capabilities all sharing a single mission:

Helping our customers understand and act properly upon the IT threats they face.

To achieve this, we equip our customers with information and mechanisms to understand, prioritize, contextualize, operationalize and respond to threats they choose to focus on .

# The value of Galaxy – Today

1

## Business as Security Driver

Prioritization by business characteristics enables customers to set focus to the things that really matter. We enable security, to become more business aligned.

*Your SecOps program becomes business oriented.*

2

## We Buy You Time

The technical concepts behind Galaxy allow for early and focused detection of threats, sometimes, before they hit. It allows focusing on things, not on your radar in the first place.

*Galaxy widens your view on threats relevant to you.*

3

## Ensuring Growth

By supporting stakeholder language and needs in security operations, we help making growth easier for SecOps programs, thus enabling better protection of things that matters over time.

*Galaxy helps to grow the SecOps maturity.*

4

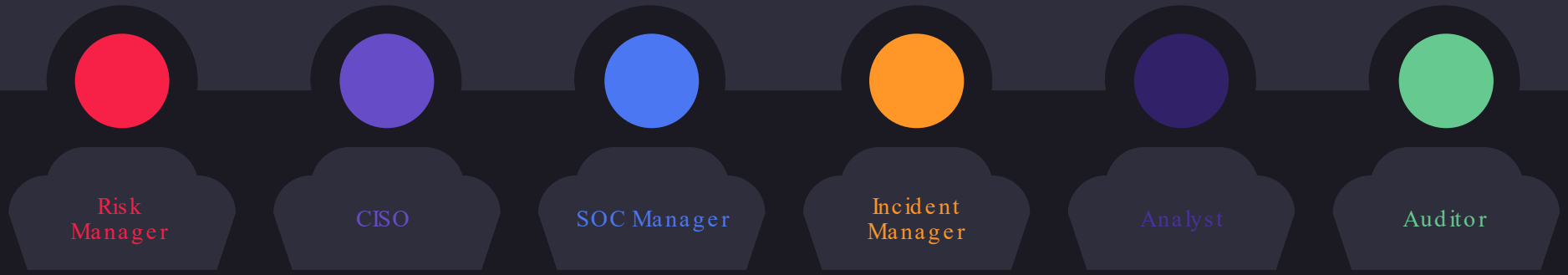
## Cost Optimization

Analysts focus their rare time on things that matters for the business. We remove friction from solely technical threat intelligence and help removing uncertainty and noise.

*Galaxy helps optimizing resource use.*

# Show Something

- How is Galaxy Online „Business oriented“
- How does Galaxy Online help prioritize?
- What can I learn from using Galaxy Online in general?



# How do we do what we do

# Galaxy Key Capabilities and Modules

## CyberRes Galaxy Online

Publicly accessible platform for Galaxy, providing a continuously updated view to threat research and allowing customers to integrate their ArcSight intelligence workflow with up-to-date threat context.

## CyberRes Galaxy GTAP Basic

GTAP is like the GTAP+ but is a community-based (OSINT2) intelligence feed that is available at no additional cost for all customers.

## CyberRes Galaxy GTAP Plus

GTAP+ is a continuous updated intelligence service for ArcSight that keeps threat models up to date with latest intelligence, indicators and tactics. GTAP+ includes intelligence from unique intelligence research, sources and methods.

## CyberRes Galaxy cyDNA Basic*

cyDNA Basic is a free content pack for ArcSight that provides a wide range of threat models, machine, pattern and anomaly detection, specifically designed to counter modern adversaries.

*) Content pack for future cyDNA service provided to let customers explore and reuse what they find helpful

# Galaxy Key Capabilities and Modules

**4** Cost Optimization

Analysts focus their rare time on things that matters for the business. We remove friction from solely technical threat intelligence and help removing uncertainty and noise.

*You can achieve more with less.*

**3** Ensuring Growth

By supporting stakeholder language and needs in security operations, we help making growth easier for SecOps programs, thus enabling better protection of things that matters over time.

*We help you to grow the SecOps maturity and growth.*

**2** We Buy You Time

The technical concepts behind Galaxy allow for early and focused detection of threats, sometimes, before they hit. It allows focusing on things, not on your radar in the first place.

*Galaxy widens your view on threats relevant to you.*

**1** Business as Security Driver

Prioritization by business characteristics enables customers to set focus to the things that really matter. We enable security, to become more business aligned.

*Your SecOps program becomes business oriented.*

**4** Cost Optimization

Analysts focus their rare time on things that matters for the business. We remove friction from solely technical threat intelligence and help removing uncertainty and noise.

*You can achieve more with less.*

**4** Cost Optimization

Analysts focus their rare time on things that matters for the business. We remove friction from solely technical threat intelligence and help removing uncertainty and noise.

*You can achieve more with less.*

**3** Ensuring Growth

By supporting stakeholder language and needs in security operations, we help making growth easier for SecOps programs, thus enabling better protection of things that matters over time.

*We help you to grow the SecOps maturity and growth.*

**2** We Buy You Time

The technical concepts behind Galaxy allow for early and focused detection of threats, sometimes, before they hit. It allows focusing on things, not on your radar in the first place.

*Galaxy widens your view on threats relevant to you.*

**4** Cost Optimization

Analysts focus their rare time on things that matters for the business. We remove friction from solely technical threat intelligence and help removing uncertainty and noise.

*You can achieve more with less.*

**2** We Buy You Time

The technical concepts behind Galaxy allow for early and focused detection of threats, sometimes, before they hit. It allows focusing on things, not on your radar in the first place.

*Galaxy widens your view on threats relevant to you.*

CyberRes Galaxy

Online

CyberRes Galaxy

GTAP Basic

CyberRes Galaxy

GTAP Plus

CyberRes Galaxy

cy DNA Basic*

# Key Takeaways

# The ~~3~~ 4 things you should remember from this session

## 1 Threat Intelligence is a Must

Threat Intelligence is more than “marketing” or “indicators”. It is the discipline which make you understand necessary details about threats, which enable you to understand a more complete picture of the landscape you are in.

*You are half -blind without it.*

## 2 Business should care

Business orientation in Security Operations in general, and Threat Management in particular, is a necessity, not only for a self-purpose, but for achieving effectiveness and efficiency in Cyber Security operations.

*Business orientation is not an option.*

## 3 Go play and let us know

Galaxy Online and other offerings are available for free use or try-out. Give it a try and let us know what you think. More exciting things are about to come. Remember, this is just the beginning of Galaxy.

*Its waiting for you and just couple clicks away.*

## 4 Less is better, more is better

We are not here to compare or replace, we are here to complement and help you becoming more effective in what you are doing. For this, we further invest in even our non-commercial capability to make it a more useful experience for your day-jobs.

*Multi-vendor, slim feeds, relevant intelligence*

# Next Steps

# Get your hands dirty with “ *Galaxy Online* ”

Register to Galaxy Online with your business e -mail address and start exploring how Threat Intelligence can help you focus with business relevant intelligence.

Go to Portal

# Check out some “ *live in action* ” examples


See how our ArcSight platform leverages Threat Intelligence information to help analysts making better decisions quicker.

Go to video

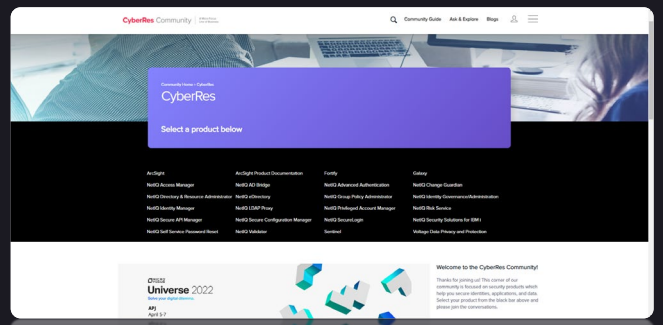
# Start your free trial with “ *Galaxy TAP Plus* ”

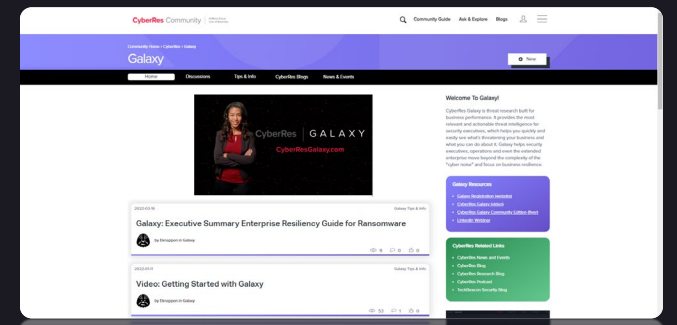
Register for a non -web trial and get access to our premium “Threat Intelligence” IoC feed to uplevel your real-time detection and response experience…

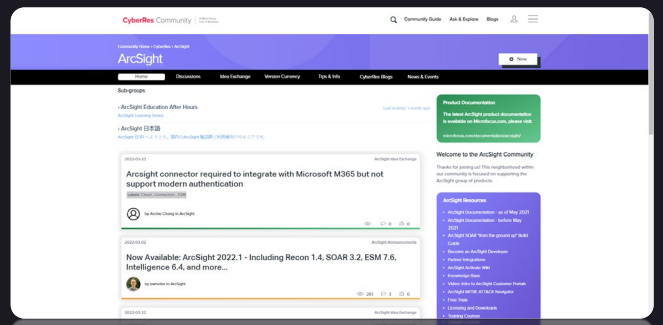
[Contact your sales representative to open a non -web trial for GTAP Plus.]

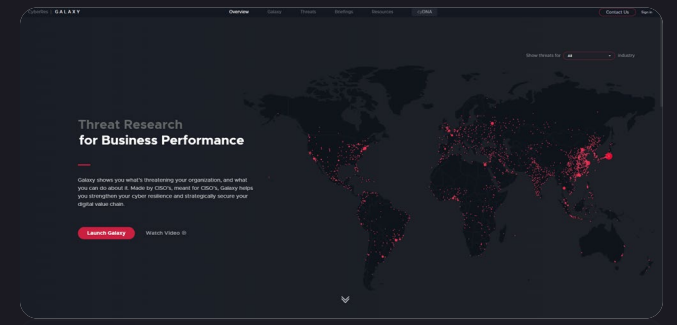
# Resources

# Galaxy Resources you should know



CyberRes