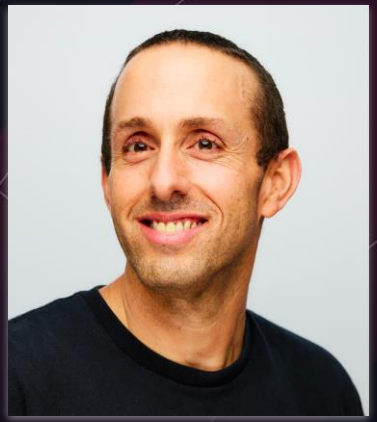
Agentic AI-Powered SOCs: Overcoming SOAR’s Unfulfilled Promises

RadiantSecurity

Speaker Bio



Shahar Ben-Hador

CEO & Co-founder of Radiant Security

I have nearly 2 decades in cybersecurity, both as a practitioner and a vendor

My past roles include:

- VP of Product at Exabeam
- CIO at Exabeam
- CISO at Imperva

Agenda

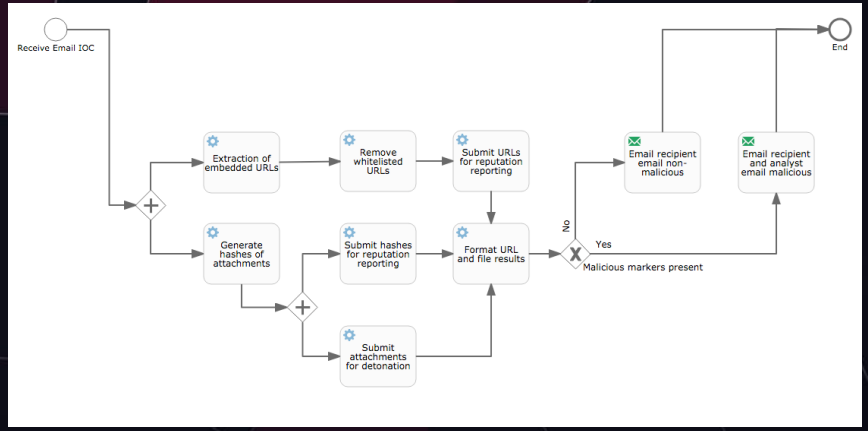
- A brief overview of SOAR and SOC Automation
- Why SOAR Didn’t Work
- How to Fix SOC Automation
- The Role of Agentic AI in SOC Automation
- Demo

What is SOAR?

SOAR stands for **Security Orchestration, Automation, and Response**

They perform automation using pre-defined logic (playbooks) to run actions over API connections to other tools.

SOARs were designed to automate security operations work like alert triage and incident response



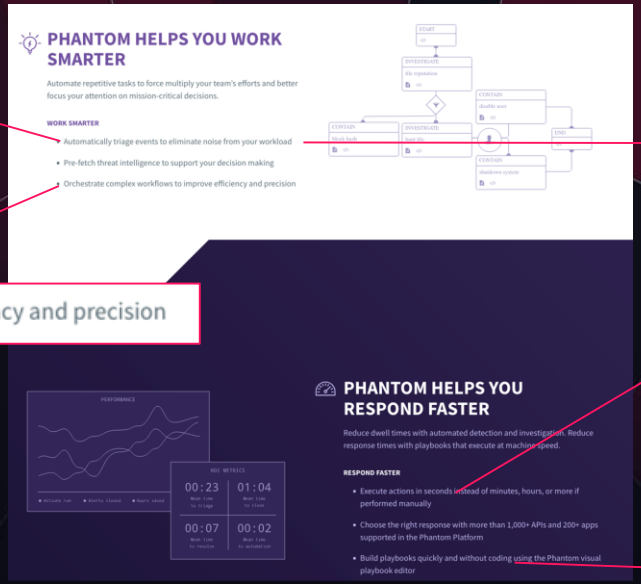
An example of a simple SOAR playbook for phishing

The Promise of SOAR

“Automate security operations tasks and workflows—to boost analyst productivity, find more attacks, and reduce response times.”

Automatically triage events

• Orchestrate complex workflows to improve efficiency and precision



eliminate noise from your workload

Execute actions in seconds instead of minutes

Build playbooks quickly and without coding

Phantom Cyber website, March 2018

The Evolution of SOAR

Gen 1

Mid 2010s

Static playbooks

Complex implementations

Huge maintenance

Simple security use cases

Gen 2

Late 2010s

Static Playbooks

Drag-n-drop editors

Playbook libraries

Moderate maintenance

Broader security use cases

Gen 3

Early 2020s to present

Static playbooks

Gen AI editors

Extensive playbook libraries

Moderate maintenance

IT & security use cases

Why didn’t SOAR work?

Post-detection SOC Work Has Two Types of Tasks

Triage & Investigation

What is this?
Is this a false positive?
What happened?
What caused it?
What should I do about this?
Could it lead to anything else?
How do I keep it from happening again?
Etc.

“Thinking Tasks”

Response

Taking corrective actions
Notifying affected people
Updating stakeholders
etc.

“Doing Tasks”

SOARs Struggle at Performing Investigative Tasks

Investigations are too complex & diverse

Static playbooks can’t learn, think, or adapt

SOAR requires predictable inputs to function

SOARs Alone Can’t Produce Low MTTRs

Detection

Automated by point products (Fast)

Investigation

Manually done by humans (Slow)

Response

Automated via **SOAR** (Fast)

Fixing SOC Automation Requires

1. **Understanding complex problems**
2. **Handling unexpected inputs**
3. **Learning environment norms**
4. **Utilizing security expertise and knowledge**
5. **Providing results without lots of customization and maintenance**
6. **Removing the manual bottleneck of investigation**

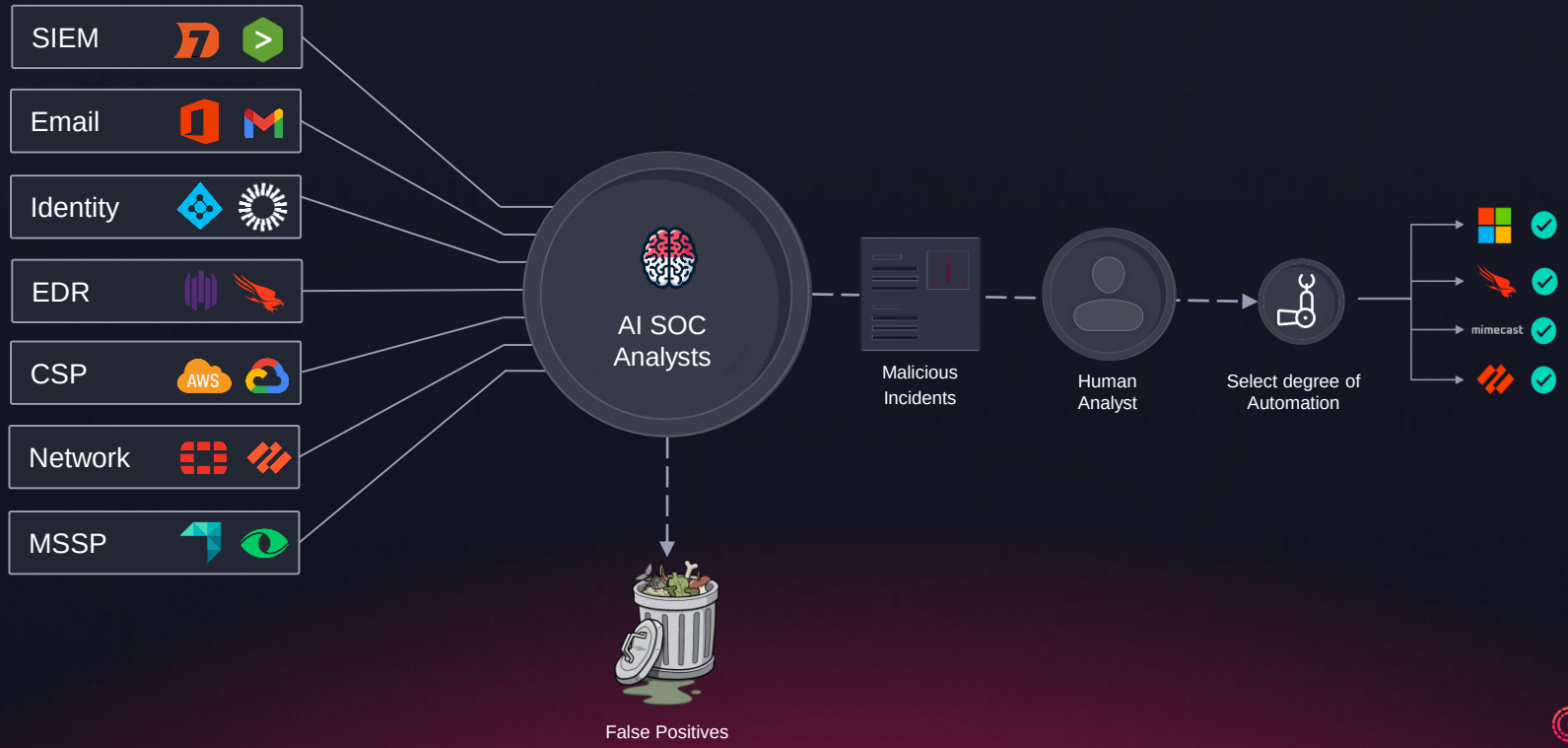
Most AI Tools in the SOC Don’t Address The SOC’s Issues

	AI/ML Analytics	Co-Pilots	Agentic AI
Pre/Post Detection	Pre	Post	Post
Output	Detections	Answers to Questions	Completed Work
Productivity improvement	N/A	Incremental	Exponential
Why they aren’t the answer	It creates more work for the SOC	SOC analysts are still doing the work	AI does the work, humans review it

RadiantSecurity

Agentic AI Offers a New Approach for the SOC Automation

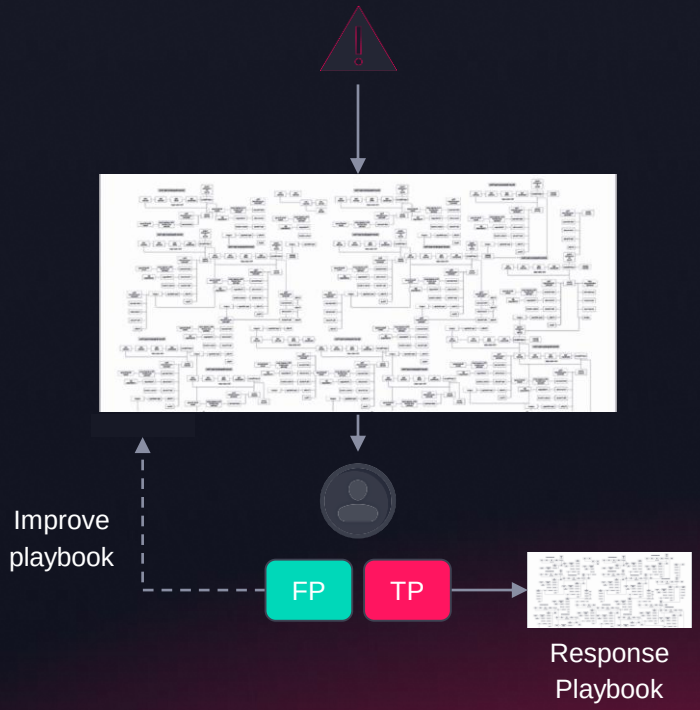
AI Analysts **emulate human techniques & decision-making**
to autonomously perform 80 to 90% of tier 1 work



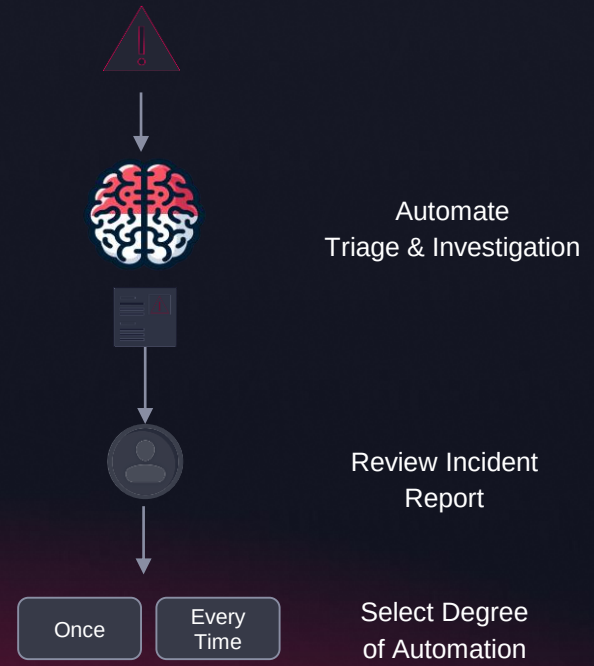
RadiantSecurity

SOC Automation with SOAR vs Agentic AI

Automation with SOAR

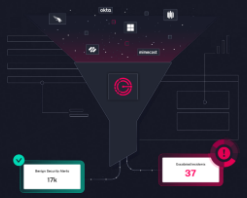


Automation with Agentic AI



Turbocharge Productivity with AI Analysts

1



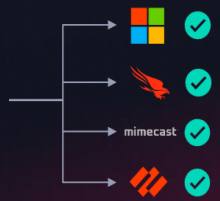
Autonomously triage & investigate **every** alert
to ensure work is completed and attacks aren't missed

2

Automatically generate decision-ready results within <3 minutes

1. Investigation summary
2. Root cause analysis
3. Incident-specific, response plan

3

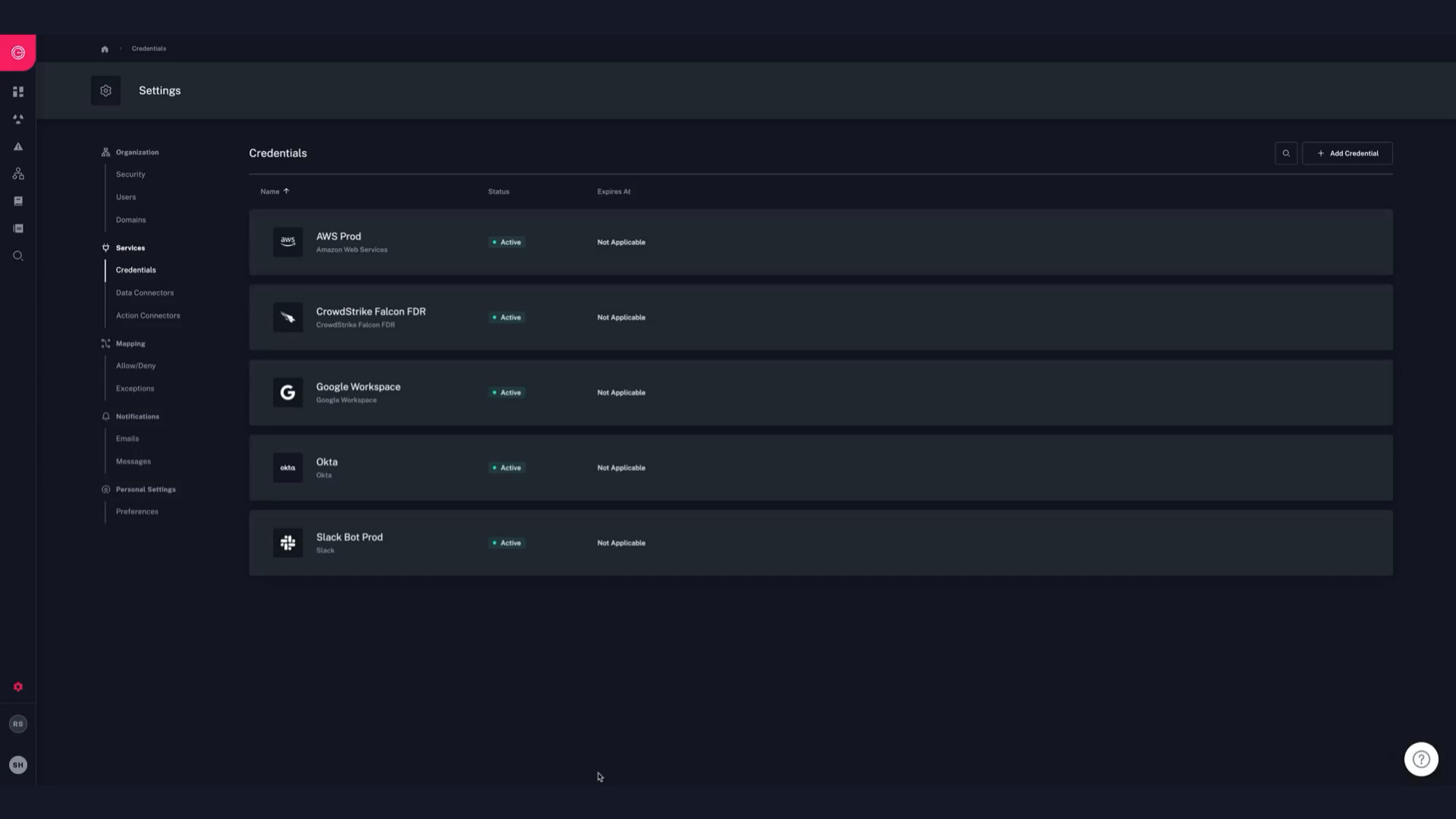


Automate response with the 3 options for lower MTTR:

1. Step-by-step instructions for manual response
2. Single-click response for semi-automation
3. Fully automated task execution

RadiantSecurity

Demo


Credentials
Settings
Organization
Security
Users
Domains
Services
Credentials
Data Connectors
Action Connectors
Mapping
Allow/Deny
Exceptions
Notifications
Emails
Messages
Personal Settings
Preferences
Credentials
Add Credential
Name
Status
Expires At
AWS Prod
Amazon Web Services
Active
Not Applicable
CrowdStrike Falcon FDR
CrowdStrike Falcon FDR
Active
Not Applicable
Google Workspace
Google Workspace
Active
Not Applicable
Okta
Okta
Active
Not Applicable
Slack Bot Prod
Slack
Active
Not Applicable

Questions?

Want to learn more?

Visit us at radiantsecurity.ai