RadiantSecurity

Radiant Security AI-powered SOC Co-pilot

Solution Brief

Radiant Security AI-power SOC Co-pilot Overview

Tackling The Security Operations Challenge

Security Operations Centers (SOCs) have become the frontline defense for organizations seeking to protect their valuable data and infrastructure from would-be attackers. However, the mounting complexity of cyberattacks, expanding attack surfaces, and the well-documented shortage of security analysts needed to staff SOCs, have put immense pressure on SOCs, often leaving them understaffed and struggling to cope with the ever-growing workload.

Today's SOCs are trapped in a dire set of circumstances which put them in a precarious position because of their reliance on manual effort they are unable to hire. Virtually no SOCs are staffed such that they can triage and conduct proper, in-depth investigates for every alert they receive. If alerts are not addressed or investigations not performed, blindspots form which leave organizations potentially vulnerable to missed or only partially detected attacks. And, without visibility into the full scope of attacks, it's impossible to conduct proper remediation that can ensure incidents don't develop into breaches

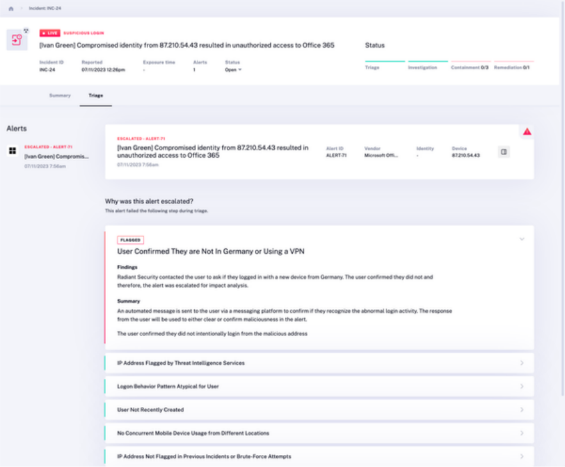
Ultimately, this model is fundamentally broken and SOCs need to rethink their entire approach if they wish to build effective programs that can adequately protect their organizations.

Key Benefits

- Boost SOC analyst productivity
- Detect more real attacks through in-depth investigation of alerts
- Respond more rapidly using intelligent automation

Key Use Cases

- Alert triage, investigation, & response for:
  - Phishing emails
  - Business email compromise
  - Endpoint alerts
  - Network security alerts
  - Suspicious logons
- SOC productivity improvement
- SOC automation



[Ivan Green] Compromised identity from 87.210.54.43 resulted in unauthorized access to Office 365

Incident ID: INC-24 | Reported: 07/11/2023 12:26pm | Exposure time: - | Alerts: 1 | Status: Open

[Ivan Green] Compromis...
07/11/2023 7:56am

[Ivan Green] Compromised identity from 87.210.54.43 resulted in unauthorized access to Office 365
07/11/2023 7:56am

Alert ID: ALERT-71 | Vendor: Microsoft Offi... | Identity: - | Device: 87.210.54.43

Why was this alert escalated?
This alert failed the following step during triage.

User Confirmed They are Not In Germany or Using a VPN

Findings
Radiant Security contacted the user to ask if they logged in with a new device from Germany. The user confirmed they did not and therefore, the alert was escalated for impact analysis.

Summary
An automated message is sent to the user via a messaging platform to confirm if they recognize the abnormal login activity. The response from the user will be used to either clear or confirm maliciousness in the alert.

The user confirmed they did not intentionally login from the malicious address

IP Address Flagged by Threat Intelligence Services
Logon Behavior Pattern Atypical for User
User Not Recently Created
No Concurrent Mobile Device Usage from Different Locations
IP Address Not Flagged in Previous Incidents or Brute-Force Attempts

Figure 1 - Radiant's co-pilot dynamically selects and perform dozens of test on every alert to determine maliciousness.

Take Control of Your SOC

Boost Analyst Productivity

SOCs don't have enough staff or hours in the day to triage and investigate every alert that comes their way. As a result, work is left undone and attacks can slip through the cracks. Radiant's AI-powered SOC co-pilot automates triage and investigation to free your team from tedious, time-consuming tasks.

The Radiant co-pilot:

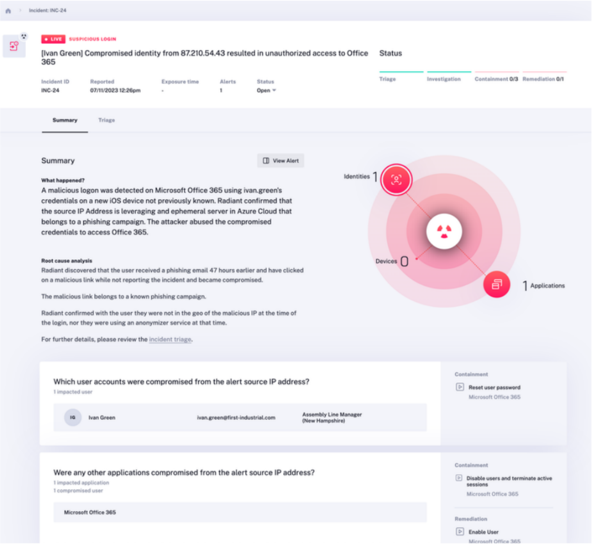
- Provides limitless triage capacity to ensure every alert is addressed.
- Dynamically selects & performs dozens of tests to determine an alert's maliciousness.
- Learns your organization's normal behavior and activity to boost accuracy.

Detect Real Attacks

SOCs have a detection problem — they detect too much, and most of it is just noise. This makes it nearly impossible for analysts to find the alerts that really matter. Radiant's AI-powered co-pilot finds real incidents by deeply investigating every last alert — and makes your security products better as a result.

Radiant finds real attacks by:

- Performing an in-depth investigation of every malicious alert.
- Determining the root cause & full scope of every incident.
- Stitching together data sources like email, endpoint, network, and identity to follow attacks wherever they go.



Incident: INC-24

LIVE SUSPICIOUS LOGIN

[Ivan Green] Compromised identity from 87.210.54.43 resulted in unauthorized access to Office 365

Incident ID	Reported	Exposure time	Alerts	Status
INC-24	07/11/2023 12:26pm	-	1	Open

Status: Triage · Investigation · Containment 0/3 · Remediation 0/1

Summary · Triage

Summary

View Alert

What happened?

A malicious logon was detected on Microsoft Office 365 using ivan.green's credentials on a new iOS device not previously known. Radiant confirmed that the source IP Address is leveraging and ephemeral server in Azure Cloud that belongs to a phishing campaign. The attacker abused the compromised credentials to access Office 365.

Root cause analysis

Radiant discovered that the user received a phishing email 47 hours earlier and have clicked on a malicious link while not reporting the incident and became compromised.

The malicious link belongs to a known phishing campaign.

Radiant confirmed with the user they were not in the geo of the malicious IP at the time of the login, nor they were using an anonymizer service at that time.

For further details, please review the incident triage.

Which user accounts were compromised from the alert source IP address?
1 impacted user

IG	Ivan Green	ivan.green@first-industrial.com	Assembly Line Manager (New Hampshire)

Containment
Reset user password
Microsoft Office 365

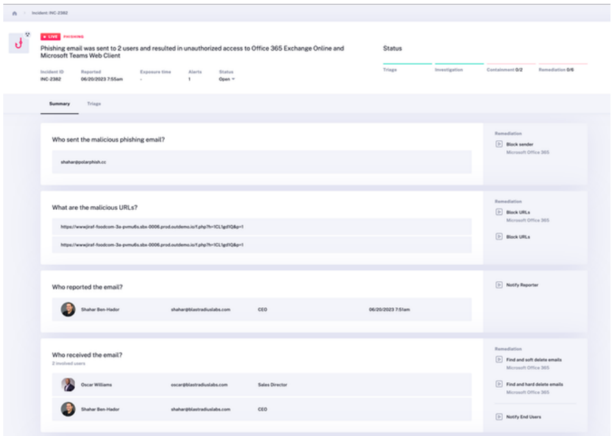
Were any other applications compromised from the alert source IP address?
1 impacted application
1 compromised user

Microsoft Office 365

Containment
Disable users and terminate active sessions
Microsoft Office 365

Remediation
Enable User
Microsoft Office 365

Figure 2 - Radiant determines root cause and incident scope for every malicious alert.



Incident: INC-2382

LIVE PHISHING

Phishing email was sent to 2 users and resulted in unauthorized access to Office 365 Exchange Online and Microsoft Teams Web Client

Incident ID	Reported	Exposure time	Alerts	Status
INC-2382	06/20/2023 7:55am	-	1	Open

Status: Triage · Investigation · Containment 0/2 · Remediation 0/6

Summary · Triage

Who sent the malicious phishing email?

shahar@polarphish.cc

Remediation
Block sender
Microsoft Office 365

What are the malicious URLs?

https://wwwjiraf-foodcom-3a-pvmu6s.sbx-0006.prod.outdemo.io/1.php?h=1CL1gd1Q&p=1

https://wwwjiraf-foodcom-3a-pvmu6s.sbx-0006.prod.outdemo.io/1.php?h=1CL1gd1Q&p=1

Remediation
Block URLs
Microsoft Office 365
Block URLs

Who reported the email?

Shahar Ben-Hador	shahar@blastradiuslabs.com	CEO	06/20/2023 7:51am

Notify Reporter

Who received the email?
2 involved users

Oscar Williams	oscar@blastradiuslabs.com	Sales Director
Shahar Ben-Hador	shahar@blastradiuslabs.com	CEO

Remediation
Find and soft delete emails
Microsoft Office 365
Find and hard delete emails
Microsoft Office 365
Notify End Users

Figure 3 - A customized response plan organizes response tasks and can launch one-click remediation.

Reduce Response Times

Incident response is complex, time-consuming work. This plus the scarcity of analyst cycles leads to long dwell and response times. Radiant slashes response times by streamlining and automating triage, investigation, and response of detected issues.

Radiant's co-pilot:

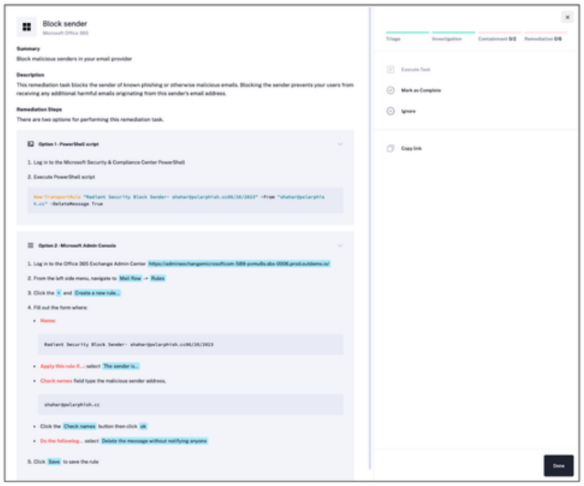
- Dynamically builds a response plan based on the specific needs of the uncovered security issues.
- Provides analysts with step-by-step remediation guidance on how to respond to incidents.
- Offers flexible response automation, including manual, one-click,, or fully automated response.

Enable Junior Analysts

There is a well known shortage of cybersecurity talent. Luckily with the help of Radiant as a co-pilot, SOCs can still thrive using junior, hire-able talent.

Radiant lets you:

- Increase the security knowledge of fresh-out-of-school team members so they can quickly become valuable contributors.
- Obtain step-by-step guidance for analysts on how to handle incidents using your toolset to help analysts learn best practices.
- Boost the efficiency and output or junior analysts with the help of automated triage and investigation.



Block sender
Microsoft Office 365

Summary
Block malicious senders in your email provider

Description
This remediation task blocks the sender of known phishing or otherwise malicious emails. Blocking the sender prevents your users from receiving any additional harmful emails originating from this sender's email address.

Remediation Steps
There are two options for performing this remediation task.

Option 1 - PowerShell script

1. Log in to the Microsoft Security & Compliance Center PowerShell
2. Execute PowerShell script

```
New-TransportRule "Radiant Security Block Sender- shahar@polarphish.cc06/20/2023" -From "shahar@polarphis
h.cc" -DeleteMessage True
```

Option 2 - Microsoft Admin Console

1. Log in to the Office 365 Exchange Admin Center https://adminexchangemicrosoftcom-589-pvmu6s.sbx-0006.prod.outdemo.io/
2. From the left side menu, navigate to Mail flow → Rules
3. Click the + and Create a new rule...
4. Fill out the form where:
   - Name:

```
Radiant Security Block Sender- shahar@polarphish.cc06/20/2023
```

   - Apply this rule if...: select The sender is...
   - Check names field type the malicious sender address.

```
shahar@polarphish.cc
```

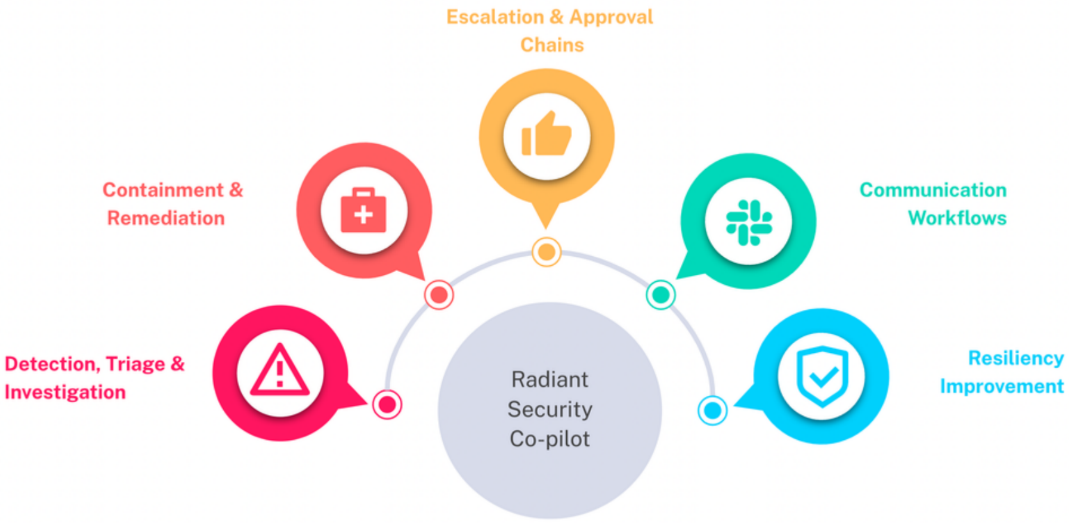
   - Click the Check names button then click ok
   - Do the following... select Delete the message without notifying anyone
5. Click Save to save the rule

Triage · Investigation · Containment 0/2 · Remediation 0/6

Figure 4- Step-by-step guidance for analysts on exactly how to respond to a security issue using your tooling.

How it works

With the Radiant AI-powered SOC co-pilot, your team can get more done, find more attacks, & respond more rapidly.


Escalation & Approval Chains
Containment & Remediation
Communication Workflows
Detection, Triage & Investigation
Radiant Security Co-pilot
Resiliency Improvement

Automated Detection, Triage, & Investigation

- **Automated Triage** – Automatically inspect all elements of suspicious alerts using AI to determine if an alert is malicious.
- **Impact Analysis** – Analyze all malicious alerts to understand detected issues' root cause and complete incident scope.
- **Data Stitching** – Stitch together data sources like email, endpoint, network, and identity to follow attacks wherever they go,

Rapid Containment & Remediation

- **Incident specific response** – Radiant dynamically builds a response plan for analysts based on the specific containment and remediation needs of the security issues uncovered during incident impact analysis.
- **Automated response** – Analysts can automate or manually perform the corrective actions to address each security issue for rapid, effective response.

Escalation & Approval Chains

Taking corrective actions to address an incident often involves tasks which require approval. Radiant can automate your existing escalation chains and approval processes to efficiently obtain permission.

Communication Workflows

Automatically keep affected users and stakeholders informed by leveraging your existing productivity tools (e.g., Slack, Teams, Email, etc.) for seamless communication. This ensures rapid response and uninterrupted workflows.

Resiliency Improvement

After an incident has been handled, it's important to improve your security posture. As part of each incident's custom response plan, Radiant automatically recommends actions that can be taken to enhance your environment's resiliency against similar threats, reducing the likelihood of future incidents of the same nature.

About Radiant Security

Radiant Security is an AI-powered security co-pilot for the SOC. Radiant enables SOCs to harness the power of AI to boost analyst productivity, detect real attacks through unlimited in-depth investigation, and rapidly respond to incidents. Deployed in minutes via API, Radiant Security provides rapid time to value and immediately reduces analyst workloads by as much as 95%.