DATA SHEET

# Use Managed Security Services to Increase Accuracy, Reduce Toil

## Stay Focused on Adding Value to Your Business—Not on Diving Deep into Security Logs

Ensuring that your applications and cloud native infrastructure are protected from attackers and internal threats is challenging enough. And then there's the matter of finding and hiring talent to help monitor it all on an ongoing basis.

The F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, Managed Security Services reduces the time and resources needed to identify and respond to security incidents and risky behavior.

With Distributed Cloud AIP Managed Security Services, our Security Operations Center (SOC) monitors your cloud continuously on a 24/7/365 basis, prioritizing alerts based on in-depth analysis and validation of suspicious activity within the context of your unique environment. To ensure that you can take action as quickly as possible when a threat is detected, our SOC analysts work around the clock to review Severity 1 alerts. Our SOC analysts investigate on your behalf, and provide actionable recommendations for remediation.

## What You Get

- Active alert monitoring and escalation
- Incident investigation
- Remediation recommendations and guidance
- Continuous Severity 1 alert review
- 24/7/365 coverage

## See the SOC in Action

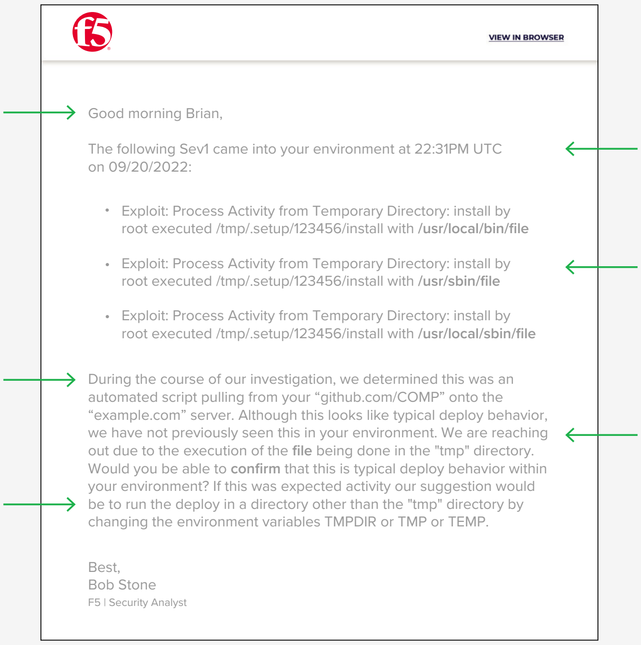
The Distributed Cloud AIP Managed Security Services' SOC regularly catches real, live threats—and we have shared a few with the world in our blog. There, you can read about the new strain of malware we found, a breach that spanned the cloud management console and hosts, and a Docker cryptojacking exploit.

## How It Works

1. Distributed Cloud AIP Managed Security Services produces a Severity 1 alert
2. Your SOC analyst jumps into action—researching what happened
3. The analyst creates an email report to brief you if the incident requires attention

## Inside a Threat Notification

When a threat is detected and validated, a member of the Distributed Cloud AIP Managed Security Services SOC team will email you with the findings, context, and recommendations you need to immediately remediate. Here is a sample email report:



VIEW IN BROWSER

Good morning Brian,

The following Sev1 came into your environment at 22:31PM UTC on 09/20/2022:

- Exploit: Process Activity from Temporary Directory: install by root executed /tmp/.setup/123456/install with **/usr/local/bin/file**
- Exploit: Process Activity from Temporary Directory: install by root executed /tmp/.setup/123456/install with **/usr/sbin/file**
- Exploit: Process Activity from Temporary Directory: install by root executed /tmp/.setup/123456/install with **/usr/local/sbin/file**

During the course of our investigation, we determined this was an automated script pulling from your "github.com/COMP" onto the "example.com" server. Although this looks like typical deploy behavior, we have not previously seen this in your environment. We are reaching out due to the execution of the **file** being done in the "tmp" directory. Would you be able to **confirm** that this is typical deploy behavior within your environment? If this was expected activity our suggestion would be to run the deploy in a directory other than the "tmp" directory by changing the environment variables TMPDIR or TMP or TEMP.

Best,
Bob Stone
F5 | Security Analyst

You **get notified only when there is real risk**, so you can focus on growing your business, not chasing false leads.

**THE RESEARCH**
Your analyst **gives you the context you need** to understand the nature of this specific incident.

**THE RECOMMENDATION**
You'll get suggestions for remediation from your cloud security expert.

**Timely updates**, so you know exactly when the incident occurred.

**THE INCIDENT**
You get the **essential information** you need to know what happened.

**THE CHECK-IN**
Your analyst will see if you're aware of the incident or the behavior that triggered the alert.

## Threat Stack: Now Part of F5

Threat Stack is now F5 Distributed Cloud App Infrastructure Protection (AIP). If you'd like to learn more about this solution, the company's Security Operations Center (including Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights), and more, feel free to contact our cloud security and compliance experts.

**Let our experts take your cloud security worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, visit our website today.**