splunk>

CASE STUDY

Tide Detects and Responds to Threats 5x Faster With Splunk SOAR

Key Challenges

As it grew, UK business financial platform Tide needed to expedite threat detection and incident response so it could maintain a high level of security for its mobile-first customers.

Key Results

With Splunk Enterprise Security (SIEM) and Splunk SOAR, Tide sped up security threat investigations and automated up to 95% of incident responses — increasing team efficiency and creating a safe, convenient experience for its more than 470,000 customers.

Industry: Financial Services

Solutions: Security

Products: Splunk SOAR, Splunk Enterprise Security, Splunk Cloud Platform

Mobile-first model puts secure account access where it belongs — anywhere the customer is.

Tide provides small and medium-sized businesses with a simple, centralized way to open accounts, access funds and manage cash flow. Thanks to Tide's mobile-first model, customers can access their accounts from anywhere so they can "get back to doing what they love." Given the sensitive nature of the financial data that the company handles, securing transactions is paramount to winning and keeping customers.

As it grew fast to over 470,000 customers (and counting), Tide needed a way to help its threat detection and response team expedite incident response to keep customer data safe.

Now with Splunk SIEM and Splunk SOAR, the team quickly spots any suspicious activity and immediately takes action to safeguard customer data. Splunk technology also supports smarter use of data throughout the organization, ensuring high levels of customer satisfaction and supporting Tide's rapid growth.

Outcomes

Up to 95%
of incident responses automated

Mins
to respond to security threats, compared to hours previously

5x
faster response times with SOAR

Enlisting allies to cast a wide safety net

Tide's threat detection and response (TDR) team protects customer and business data by swiftly investigating and remedying any security incidents. To keep up with the company's steady stream of threats, the team of six people needed to be able to share information about system security with other technical teams — a goal now achieved with Splunk. "With Splunk SOAR, it's easy to educate our engineers and enlist them as allies to the TDR team," says Devyani Vij, product security engineer at Tide. "That means we're effectively expanding the number of people safeguarding our infrastructure and providing higher levels of assurance that our data is safe."

For Tide, it's essential to recognize any suspicious activity or risky behavior — whether intentional or not — before it causes issues. "Splunk SOAR helps our engineers identify different kinds of threats and vulnerabilities, so we can all spot them as quickly as possible and focus on how to mitigate them," Vij says.

Automating the busy work strengthens Tide's security posture

With Splunk SOAR, the TDR team can now easily identify possible incidents and, in many cases, automate the response. Thanks to Splunk, Tide is well on its way to automating up to 95% of alerts so humans can focus on the most complex, sophisticated threats.

Insights derived from Splunk are also used to create dashboards for management that support smarter decision-making. "We now have visibility into all of our tools and resources, whether they're homegrown or third-party applications," says Ojasvi Chauhan, threat detection engineer at Tide. "That information raises security consciousness and supports the actions we take across the business."

> Instead of spending hours looking into an incident, it can often be handled in just minutes."
>
> **Ojasvi Chauhan,** Threat Detection Engineer, Tide

Incident response takes minutes, not hours

Migrating Splunk to the cloud relieved Tide of maintaining on-premises systems. "With Splunk Cloud Platform, our team doesn't have to manage updates and other issues, and we can request any features we need," says Chauhan. "That means we have more time for core tasks like investigating and responding to incidents."

> Splunk SOAR makes it easy to educate our engineers and enlist them as allies to the TDR team. That means we're effectively expanding the number of people safeguarding our infrastructure and providing higher levels of assurance that our data is safe."
>
> **Devyani Vij,** Product Security Engineer, Tide

Using Splunk SOAR, the team is more efficient and able to resolve incidents in a shorter amount of time. Before Splunk SOAR, the TDR team had to manually investigate alerts for potential incidents. One incident might take several hours to look into and require a team member to use multiple tools before clearing false alerts and taking action.

That's all changed with Splunk. "It's easy to send alerts directly from Splunk Enterprise Security to Splunk SOAR," says Chuahan. "Instead of spending hours looking into an incident, it can often be handled in just minutes."

Everybody's all in on security — and on Splunk

With Splunk, Tide's TDR team is always there to support the business and safeguard data. It's also increased security awareness across the organization in a matter of months. "Our people now think more about the security perspective," says Vij. "When they're developing new products or services, they consider the security implications, so protection is built-in."

As Tide grows, the security threats it faces will inevitably increase. With insights from Splunk, teams can expand their capabilities to meet those challenges and ensure resilience every step of the way.

24-543931-Splunk-Tide-CS-102