Tide erkennt und behebt mit Splunk SOAR Bedrohungen 5-mal schneller

Zentrale Herausforderungen

Im Zuge des Wachstums seiner Plattform für Unternehmensfinanzen mussten Bedrohungserkennung und Incident Response bei dem britischen Fintech Tide agiler werden, um weiterhin ein hohes Sicherheitsniveau für seine mobile-affinen Kunden gewährleisten zu können.

Wichtige Ergebnisse

Gestützt auf Splunk Enterprise Security (SIEM) und Splunk SOAR konnte Tide Bedrohungsanalysen beschleunigen und bis zu 95 % der Incident Response automatisieren. Das Resultat: eine deutliche Steigerungen der Team-Effizienz und eine gleichermaßen sichere, wie auch komfortable UX für mehr als 470.000 Kunden.

Branche: Finanzdienstleister

Lösungen: Security

Mobile-first: Sicherer Kontozugriff in Kundenhand – immer und überall

Tide ist ein Fintech mit dem Anspruch, kleinen und mittleren Unternehmen zentrale, leicht handhabbare Finanzlösungen zu bieten – von der Kontoeröffnung und -verwaltung bis zum Cashflow-Management. Mobile-first natürlich, denn die Kunden wollen jederzeit und überall bereit für ihr Business sein. Doch da Finanzdaten höchst sensibel sind, ist Transaktionssicherheit unabdingbar für Bestands- wie Neukunden.

Umso mehr galt dies angesichts des rasanten Wachstums auf nun schon 470.000 Kunden. Um deren Daten weiterhin konsequent schützen zu können, war in puncto Bedrohungserkennung und Incident Response mehr Agilität gefragt.

Genau die erhält das verantwortliche Team jetzt mit Splunk SIEM und Splunk SOAR. Mit den Lösungen von Splunk deckt es verdächtige Aktivitäten nun deutlich schneller auf und kann direkt reagieren, um Kundendaten zu schützen. Außerdem profitiert das Unternehmen dank Splunk-Technologie jetzt von einer intelligenteren Datennutzung – ein wichtiger Faktor, um die Kundenzufriedenheit zu stärken und das Wachstum von Tide zu fördern.

Datengestützte Ergebnisse

Bis zu 95 %
der Incident Response automatisiert

Minuten
statt bislang mehrere Stunden zur Bedrohungsabwehr

5x
kürzere Reaktionszeiten mit SOAR

Geballte Team-Power für ein umfassendes Sicherheitsnetz

Den Schutz von Kunden- und Geschäftsdaten gewährleistet bei Tide das Team Threat Detection and Response (TDR) – gewissermaßen als schnelle Eingreiftruppe zur Untersuchung und Behebung von Security Incidents. Um sämtliche Bedrohungen abzuwehren, denen das Unternehmen anhaltend ausgesetzt ist, war es für das sechsköpfige Team wichtig, Informationen zur Systemsicherheit mit anderen technischen Funktionsbereichen austauschen zu können. Auch hier traf man mit Splunk ins Schwarze: „Mit Splunk SOAR vermitteln wir unseren Engineers mühelos wichtiges Security-Wissen und machen sie damit zum verlängerten Arm des TDR-Teams“, kommentiert Devyani Vij, Product Security Engineer bei Tide. „De facto vergrößern wir also den Kreis derer, die unsere Infrastruktur absichern. Entsprechend größer ist auch die Gewissheit, dass unsere Daten sicher sind.“

Entscheidend ist dabei die Fähigkeit, verdächtige Aktivitäten oder risikobehaftete Verhaltensweisen – ob mit böser Absicht oder nicht – aufzudecken, bevor sie sich zu handfesten Problemen auswachsen. „Splunk SOAR erleichtert unseren Engineering-Teams die Erkennung verschiedenster Arten von Bedrohungen und Schwachstellen, sodass wir allesamt schneller Klarheit haben und die Behebung punktgenau angehen können“, fügt Vij hinzu.

Mehr Sicherheit durch Automatisierung arbeitsintensiver Aufgaben

Die jetzt deutlich leichtere Erkennung potenzieller Sicherheitsvorfälle ist das eine. Splunk SOAR ermöglicht es dem TDR-Team aber auch, die Reaktion darauf zu großen Teilen zu automatisieren – dies für bald 95 % der Warnmeldungen. So kann sich das Team voll darauf konzentrieren, besonders komplexe und perfide Bedrohungsszenarien zu entschärfen.

Hinzu kommt, dass die mit Splunk gewonnenen Dateneinblicke in Dashboards für das Management visualisiert werden, was zu fundierteren, smarteren Entscheidungsprozessen führt. „Das verschafft uns absolute Transparenz zu all unseren Tools und Ressourcen – unternehmenseigenen ebenso wie solchen von Drittanbietern", so Ojasvi Chauhan, Threat Detection Engineer bei Tide. „In puncto Sicherheit sind damit alle besser im Bilde, sodass wir als Unternehmen insgesamt informierter agieren."

> Wo wir früher stundenlang an einem Incident saßen, haben wir heute oft schon nach Minuten alles gelöst."
>
> **Ojasvi Chauhan,** Threat Detection Engineer, Tide

Incident Response in Minuten, nicht erst nach Stunden

Auch ging Tide mit Splunk den Weg in die Cloud und ersparte sich dadurch den Verwaltungsaufwand rund um On-Premises-Systeme. „Durch die Splunk Cloud Platform muss sich unser Team nicht mehr mit Updates und ähnlichen Belangen befassen. Und wenn wir neue Features benötigen, fordern wir sie einfach an", sagt Chauhan. „Auch das bedeutet wieder Zeitersparnis, dank derer wir unseren Fokus stärker auf die Untersuchung und Behebung von Incidents richten können."

Dabei agiert das Team mit Splunk SOAR insgesamt effizienter und behebt Vorfälle schneller: Zuvor musste es bei jeder Warnmeldung manuell überprüfen, ob tatsächlich etwas im Argen liegt. So zogen sich Untersuchungen bisweilen über mehrere Stunden hin, nicht zuletzt wegen der diversen Tools, die zum Unterscheiden zwischen echten und Fehlalarmen sowie zur entsprechenden Reaktion benötigt wurden.

> Mit Splunk SOAR vermitteln wir unseren Engineers mühelos wichtiges Security-Wissen – und machen sie damit zum verlängerten Arm des TDR-Teams. De facto vergrößen wir also den Kreis derer, die unsere Infrastruktur absichern. Entsprechend größer ist auch die Gewissheit, dass unsere Daten sicher sind."
>
> **Devyani Vij,** Product Security Engineer, Tide

Mit Splunk ist das alles nun passé. „Warnmeldungen lassen sich einfach und direkt von Splunk Enterprise Security an Splunk SOAR übermitteln", freut sich Chauhan. „Wo wir früher stundenlang an einem Incident saßen, haben wir heute oft schon nach Minuten alles gelöst."

Voller Fokus auf Sicherheit – und auf Splunk

Dank Splunk ist das TDR-Team stets zur Stelle, wenn es um die Stärkung der Geschäftsprozesse und Datensicherheit bei Tide geht. So hat binnen weniger Wochen auch unternehmensweit ein deutlich stärkeres Bewusstsein für Sicherheitsthemen Einzug gehalten. „Alle betrachten ihre Arbeit jetzt stärker unter dem Aspekt der Sicherheit", stellt Vij fest. „Das beginnt bereits bei der Entwicklung neuer Produkte oder Services. Schutzmaßnahmen sind nun also schon direkt integriert."

Gleichwohl wird mit seinem weiteren Wachstum unweigerlich auch die Bedrohungsdynamik für das Unternehmen zunehmen. Doch mit den Einblicken und Erkenntnissen, die Splunk den Teams bei Tide liefert, lassen sich auch kommende Herausforderungen gezielter adressieren. Somit ist zu jedem Zeitpunkt die nötige Resilienz sichergestellt.

22-26576-Splunk-Tide-A4-CS-101-451498-DE