ADAPTIVE SHIELD

Identity Threat Detection & Response

Prevent, detect and respond to SaaS threats.

Adaptive Shield's ITDR is designed based on the comprehensive understanding of SaaS characteristics and Identity Security within this dynamic landscape. With the widest coverage of over 140 SaaS apps, Adaptive Shield's prevention capabilities establish the robust security layer in the Identity Fabric, while the threat detection and response engines offer a proactive approach to the security challenges.

ITDR Capabilities

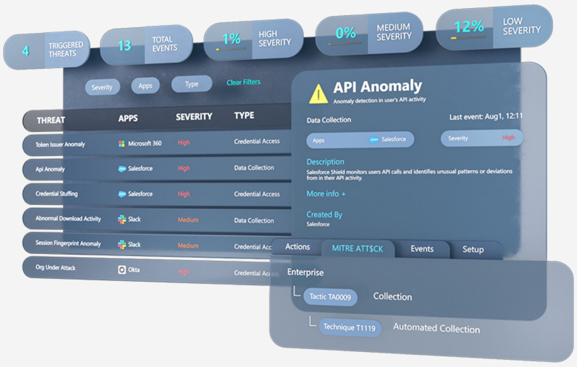
Adaptive Shield's ITDR capabilities provide extensive coverage in detecting Tactics, Techniques, and Procedures (TTPs). By understanding these TTPs, Adaptive Shield's ITDR improves incident response capabilities through:

Indicator of Compromise (IOC) Detection

Gather evidence indicating that the organization's SaaS apps have been compromised. IOCs can include data from IP addresses, domain names, URLs, etc.

User and Entity Behavior Analytics (UEBA)

Detect behavioral anomalies and identify threat actors as they navigate through the the organization's applications, offering proactive threat detection.



THREAT	APPS	SEVERITY	TYPE
Token Issuer Anomaly	Microsoft 360	High	Credential Access
Api Anomaly	Salesforce	High	Data Collection
Credential Stuffing	Salesforce	High	Credential Access
Abnormal Download Activity	Slack	Medium	Data Collection
Session Fingerprint Anomaly	Slack	Medium	Credential Acc
Org Under Attack	Okta	High	Credential Acc

API Anomaly

Anomaly detection in user's API activity

Data Collection

Last event: Aug1, 12:11

Apps: Salesforce

Severity: High

Description

Salesforce Shield monitors users API calls and identifies unusual patterns or deviations from in their API activity.

More info +

Created By

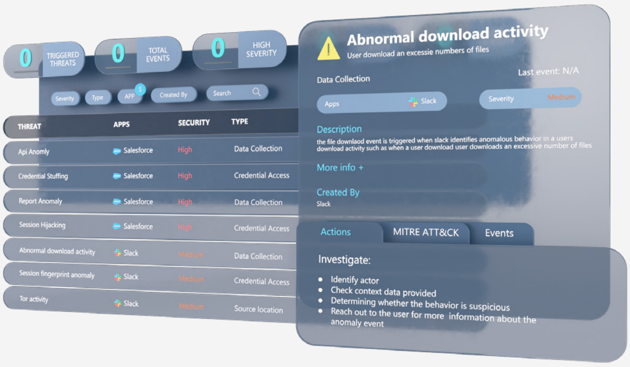
Salesforce

Enterprise

Tactic TA0009 Collection

Technique T1119 Automated Collection

Monitor showing threats by time with MITRE ATT&CK mapping



THREAT	APPS	SECURITY	TYPE
Api Anomly	Salesforce	High	Data Collection
Credential Stuffing	Salesforce	High	Credential Access
Report Anomaly	Salesforce	High	Data Collection
Session Hijacking	Salesforce	High	Credential Access
Abnormal download activity	Slack	Medium	Data Collection
Session fingerprint anomaly	Slack	Medium	Credential Access
Tor activity	Slack	Medium	Source location

Abnormal download activity

User download an excessie numbers of files

Data Collection

Last event: N/A

Apps: Slack

Severity: Medium

Description

the file downlaod event is triggered when slack identifies anomalous behavior in a users download activity such as when a user download user downloads an excessive number of files

More info +

Created By

Slack

Investigate:

- Identify actor
- Check context data provided
- Determining whether the behavior is suspicious
- Reach out to the user for more information about the anomaly event

Threat center showing all monitored events

ADAPTIVE SHIELD

Features & Key Capabilities

MITRE ATT&CK Mapping

Enhance incident response capabilities and improve threat detection and mitigation by aligning observed or potential attack techniques with the MITRE ATT&CK framework.

Alerts & Notifications

Get alerts in multiple channels such as email, Slack, or Teams, indicating potential security incidents or suspicious activities that require immediate investigation or response.

SIEM & SOAR Integrations

Seamlessly integrate with your existing Security Operations Center (SOC) and Security Orchestration, Automation, and Response (SOAR) tools, improving threat correlation and incident response efficiency.

Remediation Guidance

Get actionable recommendations and step-by-step guidance to address and mitigate vulnerabilities, weaknesses, or compromises in the event of a security incident.

GitHub	docebo	GitLab	DATADOG	G Suite		salesforce
Lucidchart	jumpcloud	Looker	bob	OneDrive	Confluence	PingOne
snowflake	UiPath	Trello	MuleSoft	DocuSign	HubSpot	CROWDSTRIKE
	ATLASSIAN	EGNYTE	Jira Software		Dropbox	bambooHR
	N	SAP SuccessFactors	vidyard		zendesk	box
Apollo.io	DUO	workato	jamf	New Relic		zscaler
workday	sumo logic		asana	PagerDuty	servicenow	TWILIO SendGrid
cisco Meraki	S	monday.com	slack	webex by cisco	onelogin	
ArcGIS ESRI	tenable	okta	smartsheet	Wrike	Bitbucket	zoom

View all supported 140+ integrations

ADAPTIVE SHIELD

Adaptive Shield enables security teams to start securing their entire SaaS ecosystem's security by strengthening the organization's SaaS posture, and detecting and responding to SaaS threats. Founded by Maor Bin and Jony Shlomoff, Adaptive Shield works with many Fortune 500 enterprises and has been named Gartner® Cool Vendor™ 2022.

With Adaptive Shield, you can secure your SaaS stack with:

- Misconfiguration Management
- SaaS-to-SaaS Access Discovery and Control
- Identity and Access Governance
- Device-to-SaaS Risk Management
- Identity Threat Detection and Response (ITDR)

www.adaptive-shield.com

Follow us on LinkedIn

REQUEST A DEMO