Automated Cloud Security Incident Response with Cortex XSOAR and Microsoft Azure

Modern Day Security Challenges in a Cloud-First World

The accelerated enterprise movement to the cloud, coupled with a sudden increase in cloud adoption by employees and users due to remote work, has led to an expansion of the threat landscape and new types of cybersecurity attacks in a post pandemic world. Enterprises are now using a wider range of cloud services than ever before to enable their businesses to survive and thrive in a highly competitive world. Employees and users juggle between their business and personal devices to keep up with their work and daily routine beyond normal business hours. The increased complexity in the threat landscape has challenged the enterprise cloud security teams to urgently fix inefficiencies and gaps in collaboration to bring down the average mean time to respond to cloud security alerts.

The Cortex™ XSOAR security orchestration automation and response platform helps cloud security operation teams standardize incident response processes and automate repetitive actions across different cloud and on-prem environments with the help of task based playbooks. Cortex XSOAR integrates with a host of Microsoft Azure services and hundreds of security and IT operation products for more efficient security operations. Microsoft Azure integrations in Cortex XSOAR use Azure Active Directory applications to authenticate with Microsoft APIs. These integrations use OAuth 2.0 and OpenID Connect standard-compliant authentication services that use an application to sign-in or delegate authentication.

- Advanced case management
- Orchestrate cloud security response actions
- Unify security functions

Benefits

Orchestrate cloud security monitoring, enrichment, and response actions through playbooks.

Avoid credential management through seamless use of IAM roles for API integrations.

Reduce time to resolution by using one platform to collaborate, investigate, and document.

Integrations

Products: Cortex XSOAR, Azure Security Center, Azure Sentinel, Azure Log Analytics, Azure Feed, Azure Compute, Azure WAF, Microsoft Management Activity (0365 Azure events) API, Azure Network Security groups.

Platform: Platform Independent

Integration Features

- Collect and analyze data generated by the resources on the cloud and on-premise environments, and automate responses such as create, delete, execute and save searches on Azure log analytics.
- Create and manage Azure Virtual Machines (VM).
- Automate playbooks for unified security management and advanced threat protection across hybrid cloud workloads.
- Use the Azure Sentinel integration to get and manage incidents and get related entity information for incidents.
- Use the Microsoft Azure AD Connect Health Feed integration to get indicators from the feed.
- Integrate with Azure cloudIPs Feed.
- Integrate with Microsoft Management Activity API to subscribe or unsubscribe to different audits, receive their content, and fetch new content as incidents.
- Utilize Azure Network Security groups to filter network traffic to and from Azure resources in a Azure virtual network.
- Integrate with Azure WAF (Web Application Firewall) to centralize protection of your web applications from common exploits and vulnerabilities. It enables cloud and security teams to:
  - » Enforce policies that are configured in the Azure Firewall management platform
  - » Delete, or update policies
  - » Receive details of a specific policy or a list of policies.

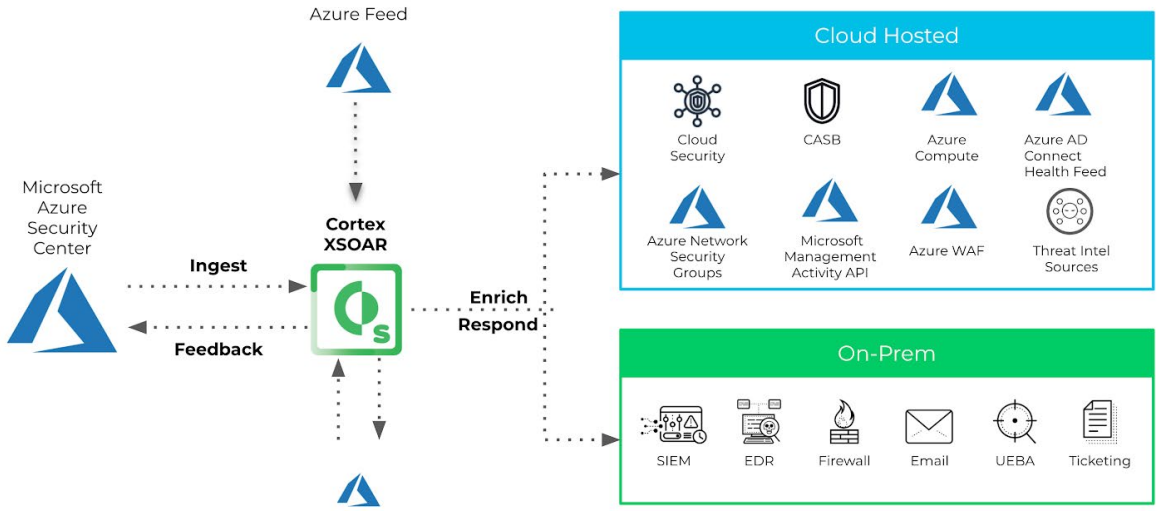

Figure 1: Cortex XSOAR orchestrates and automates incident response actions across different on-prem and cloud hosted products and services.

Use Case No. 1: Streamline Cloud Security Case Management

Challenge

Too many different types of cloud alerts generated by a growing number of sources have challenged the enterprise cloud operations teams in successfully triaging cloud alerts. Also, the processes diverge depending on the analyst that handles the incident, leading to differing response quality. Not only is precious time lost but employee productivity also gets impacted.

Solution

Cortex XSOAR's advanced case management functionality automatically classifies ingested alerts from Microsoft Azure services and routes it to the appropriate stakeholders using the out of the box playbooks. CloudOps teams can view complete information on any alert on the incident summary page and take action.

Benefit

Security teams and CloudOps teams gain alert visibility with case management that unifies cloud alerts/data across sources, saving time with fast, efficient and accurate triage of cloud security alerts.

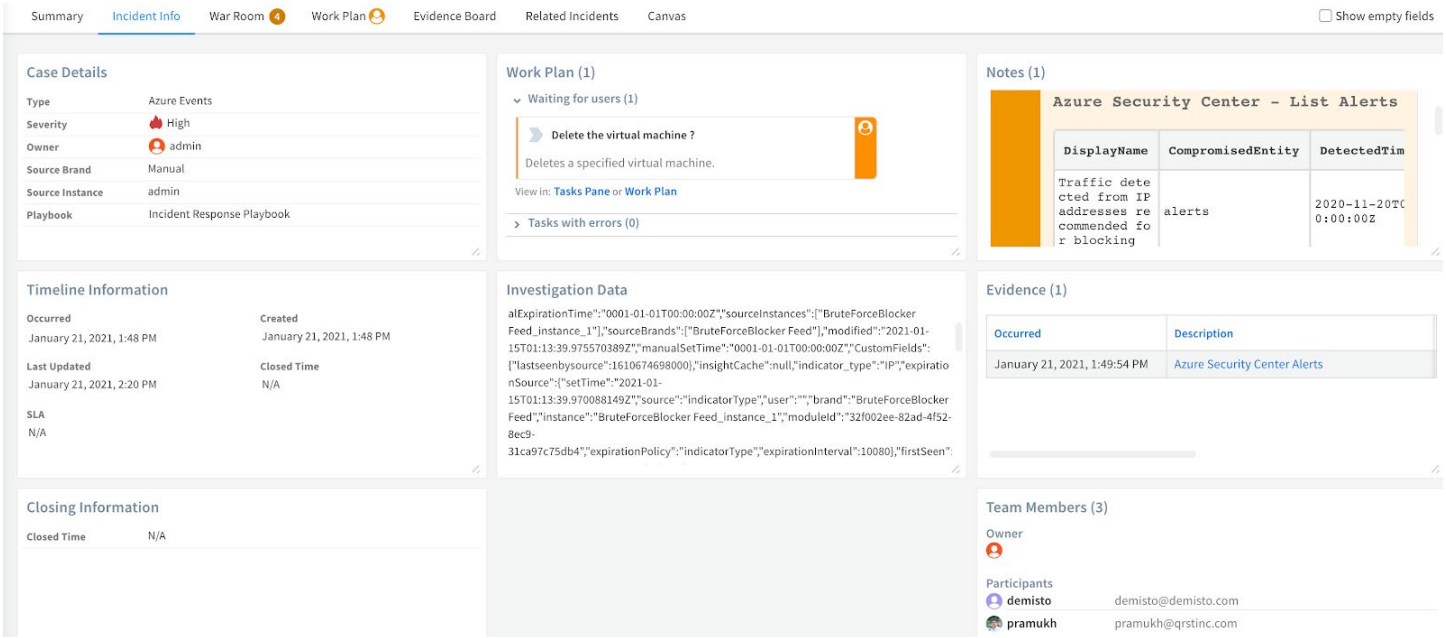

Figure 2: The advanced case management functionality structures incident information in a tailored manner to improve response clarity and speed. Users can create custom tabs and layouts for every incident type with full role-based access control.

Use Case No. 2: Automate cloud security alerts enrichment and response

Challenge

If cloud security consoles are isolated from other security functions such as EDR, malware analysis, and threat intelligence, it becomes time-consuming and repetitive for security analysts to cross-reference alerts from cloud security tools, get further context, and coordinate containment and response.

Solution

Analysts can use the Azure Security Center, Azure Sentinel, or other integrations to ingest alert data, create incidents in Cortex XSOAR, and trigger standardized, automated cloud security incident response playbooks for responding to those incidents. These playbooks can enrich the alert with more event details from Azure Network Security groups, Azure log info from Azure log analytics, and access information from other integrations and services. Playbooks can also coordinate across hundreds of other products to extract wider context without the need for screen switching and manual repetition.

Benefit

Using this solution, security analysts will be able to aggregate Azure data across products and execute actions from a central console to save screen switching time. Cortex XSOAR orchestrates other product actions in the same window and can also help analysts coordinate across security functions for richer and more comprehensive incident context. Cortex XSOAR playbooks can automate extraction of IOCs before pushing those IOCs to blocklists across both cloud and on-prem environments. As an example, a playbook handles the tagging of Azure indicators. Users can specify the tag to apply to the indicators in the playbook inputs. If no inputs are specified, the indicators will be auto-tagged for manual review. The user can specify whether a manual review incident is required.

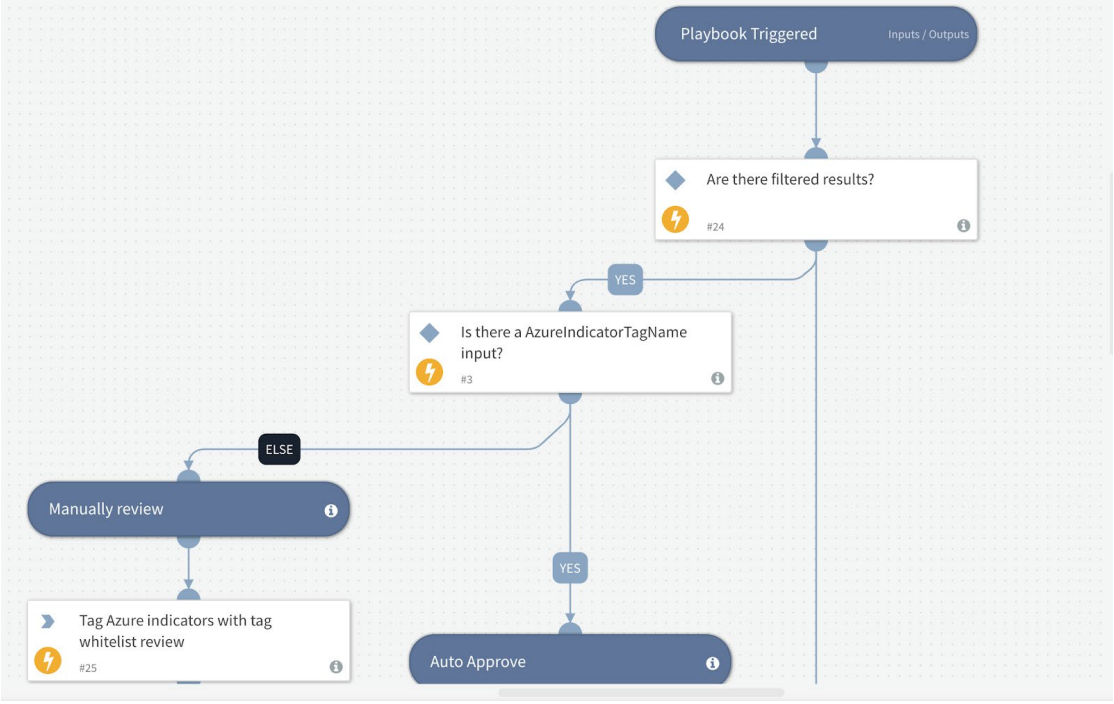

Figure 3: Playbooks are at the heart of Cortex XSOAR. Automated playbooks unify alerts and indicator feed ingestion, enrichment and incident management workflows, bringing machine speed to cloud security operations.

Use Case No. 3: Interactive Cloud Security Investigation and Digital Forensics

Use Cortex XSOAR's built-in command line utility that also doubles up as chatOps functionality for real time cross team collaboration with auto documentation.

Challenge

Disparate enterprise security infrastructure (private cloud, hybrid, multi-cloud, on-prem etc.) has created team silos that hamper active collaboration between CloudOps, SecOps, DevOps, and DevSecOps. The lack of well defined cloud security response processes has further resulted in a need for ad hoc investigations that require manual invoking of commands with several different teams involved in remediation.

Solution

SecOps and incident response teams can refer to Cortex XSOAR's automation browser and execute commands on an ad-hoc basis to manually orchestrate security actions using Azure services commands from the central CLI. Stakeholders from different teams can actively collaborate and exchange raw data and information during investigation. For example, analysts can run the !azure-nsg-security-groups-list command from the CLI to list all network security groups, or run the !azure-nsg-security-rule-update command to

update a security rule. If command does not exist, it will be created. The results can then be added to the evidence board and will be available for future reference. As another example, the CloudOps teams can interact with SecOps and DevOps using the chatOps functionality and exchange critical data and information in real time.

Benefit

Real time collaboration between different teams with the help of ChatOps capability helps in quick exchange of security artifacts of interest during complex investigations. This functionality also auto-documents all chats, artifacts and playbook action output for easy retrospective analysis of past investigations, identification of gaps, learning, and new team member onboarding.

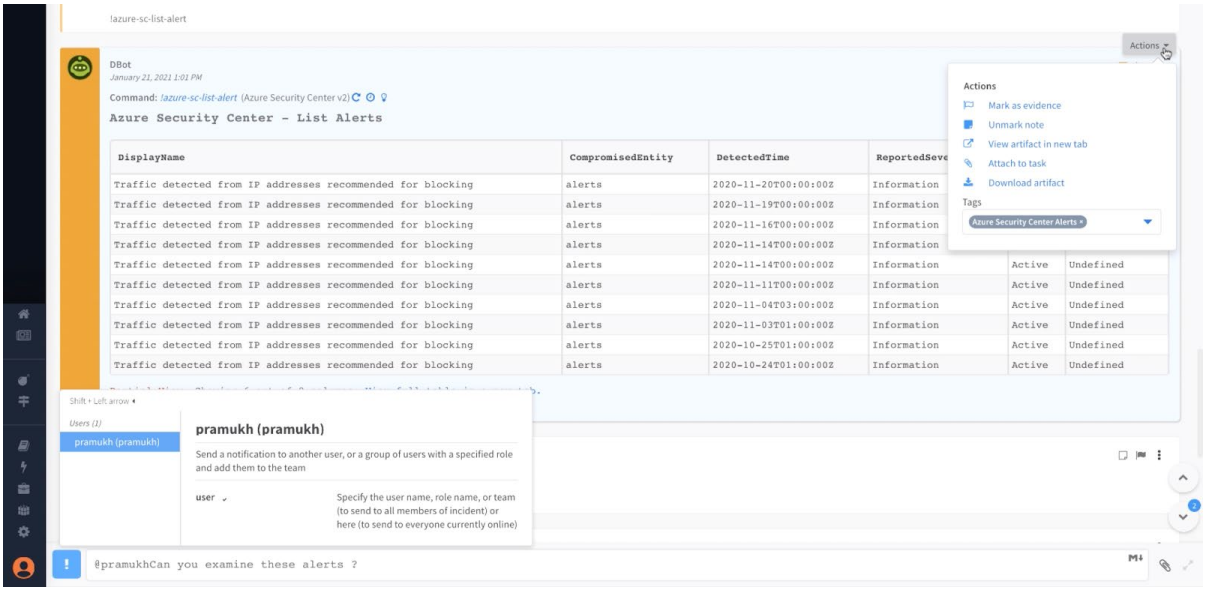

Figure 4: Investigate new threats in real time with collaboration, remote execution of third-party commands and auto-documentation from the Cortex XSOAR virtual War Room.

About Cortex XSOAR

Palo Alto Networks Cortex™ XSOAR, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit https://www.paloaltonetworks.com/cortex/cloud-security-orchestration or go to the Cortex XSOAR listing on Microsoft Azure marketplace here https://azuremarketplace.microsoft.com/en-us/marketplace/apps/paloaltonetworks.cortex_xsoar.

About Microsoft Azure™

Microsoft Azure™ is one of the most comprehensive cloud platforms available. It offers companies a full range of services that are easy to access and user-friendly, whether you want to set up a website, create a database, maintain and administer projects, or even develop, deploy and support your own applications. The Azure cloud platform is more than 200 products and cloud services designed to help you bring new solutions to life—to solve today's challenges and create the future. Build, run, and manage applications across multiple clouds, on-premises, and at the edge, with the tools and frameworks of your choice. For additional information, please visit https://azure.microsoft.com/en-us/overview/

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies. cortex_azure_automated-cloud-security_270121

Microsoft Azure

© 2021 Microsoft Azure™ is a registered trademark of Microsoft. A list of our trademarks can be found at https://www.https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/EN-US.aspx. All rights reserved. This data sheet is for informational purposes only. Microsoft makes no warranties, express or implied, with respect to the information presented here.