CROWDSTRIKE | DEMISTO

CONTINUOUS BREACH PREVENTION

Stop breaches and gain threat knowledge with an integrated solution from CrowdStrike and Demisto

IMMEDIATE TIME-TO-VALUE:

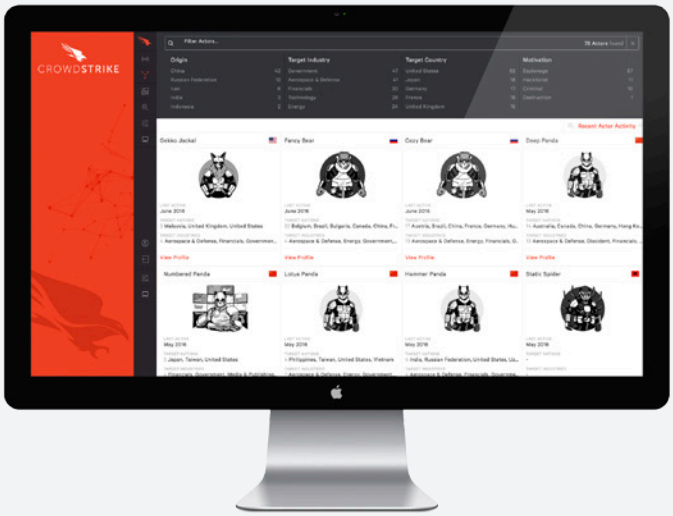
- Automatic enrichment of all investigation data with Falcon Intelligence via Demisto Playbooks
- Faster resolution of incidents using Demisto collaborative war-rooms and information collected from Falcon Host
- Automatic security investigation and data enrichment based on IOC search

JOINT SOLUTION FEATURES:

- Bi-directional integrations enable automatic data collection for a more robust investigation and response strategy
- Automating enrichment of querying of host information files landed, malware samples, running process and more from Falcon Host
- Streamlining remediation and response via Demisto's Playbooks and automation scripts by updating CrowdStrike policy

RESPOND TO ATTACKS FASTER:

CrowdStrike and Demisto have partnered to combine the rich endpoint data and threat intelligence from Falcon Connect with the automation capabilities of Demisto Enterprise to enable customers to respond faster and with better accuracy to incidents allowing them to save precious time and resources.



STOP BREACHES - Prevent both malware and malware-free attacks

5-SECOND VISIBILITY - To discover and investigate current and historic endpoint activity

CLOUD POWERED - Lower cost and effective performance with cloud delivery 24/7

COMBAT ADVANCED ATTACKS WITH CROWDSTRIKE AND DEMISTO

AUTOMATE HUNTING, INVESTIGATIONS AND RESPONSE TO MITIGATE RISK

Falcon Intelligence provides actionable insights into the top threat actors, attack vectors, and threat intelligence trends

Demisto Enterprise integrates with CrowdStrike Falcon Host and Falcon Intelligence to enrich threat detection and attack remediation

Falcon Host automatically ingests Indicators of Compromise (IOCS) from Demisto to block attacks from executing on the endpoint

AUTOMATED SEARCHING OF IOCS

Challenge:
When an organization is under attack time is of the essence. A key component to understanding the attack's progress is knowing how the attack is spreading and being able to search for across your environment. For example, where malware files have landed and at what time, etc.

Solution:
When an attack is investigated in Demisto, automation scripts and playbooks can automatically query CrowdStrike in order to hunt for IOCs on endpoints. For example an analyst can query CrowdStrike to find out if a certain process running on suspect endpoints. Furthermore, once IOCs are discovered during the investigation, automation scripts can query CrowdStrike for the presence of these IOCs such as specific binaries on the endpoints.

Customer Benefit:
The power of automating these steps within Demisto and the accurate immediate data from CrowdStrike can save hours and sometimes days of carrying out the same steps manually.

AUTOMATED RESPONSE TO CYBER ATTACKS AND ENFORCEMENT ON ENDPOINTS

Challenge:
Even when the attack method becomes clear, it often takes days and sometimes months to clean the network from malicious components and implement remediation efforts to ensure future attacks are mitigated.

Solution:
Whenever a new IOC is discovered, whether through analysis of Crowdstrike data or through a dynamic malware analysis solution, Demisto can automatically send information about the IOC to Falcon Host and block the IOC across the environment.

Customer Benefit:
With CrowdStrike and Demisto working together, attack mitigation efforts can be improved and shortened, enabling security analysts to reduce response time from hours and sometimes days to minutes.

About CrowdStrike

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. The CrowdStrike Falcon platform stops breaches by preventing and responding to all attacks type – both malware and malware-free. Only Crowdstrike unifies next-generation antivirus with EDR (endpoint detection and response), backed by 24/7 proactive threat hunting – all delivered via the cloud.

About Dimesto

Demisto helps Security Operations Centers scale their human resources, improve incident response times, and capture evidence while working to solve problems collaboratively. Demisto Enterprise is the first comprehensive, Bot-powered Security ChatOps Platform to combine intelligent automation with collaboration. Demisto's intelligent automation is powered by DBot which works with teams to automate playbooks, correlate artifacts, enable information sharing and auto document the entire incident lifecycle.

crowdstrike.com | 1.888.512.8906 | sales@crowdstrike.com | 15440 Laguna Canyon Road, Suite 250, Irvine, California 92618