CROWDSTRIKE | HEXADITE

CONTINUOUS BREACH PREVENTION

Automatically Detect, Investigate, and Remediate Threats with the Integrated Solution from CrowdStrike and Hexadite

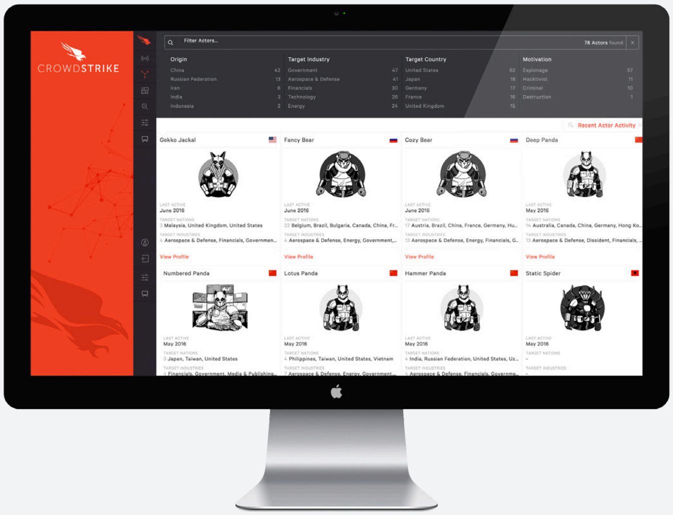
IMMEDIATE TIME-TO-VALUE:

- Detect potentially malicious activity on every endpoint
- Evaluate all threats with threat intel and endpoint correlation
- Take action automatically to resolve incidents before they spread

JOINT SOLUTION FEATURES:

- Real-time endpoint protection to identify threats
- Automatic enrichment and querying of host information
- Automated investigation and remediation of all threats

WITH REAL-TIME THREAT INTELLIGENCE AND CORRELATION FROM CROWDSTRIKE AND AUTOMATED ALERT INVESTIGATION AND ATTACK REMEDIATION FROM HEXADITE, CUSTOMERS CAN ACHIEVE CONTINUOUS THREAT DETECTION AND RESPONSE.



Filter Actors... 78 Actors found

Origin		Target Industry		Target Country		Motivation	
China	42	Government	47	United States	62	Espionage	57
Russian Federation	13	Aerospace & Defense	41	Japan	18	Hacktivist	11
Iran	6	Financials	30	Germany	17	Criminal	10
India	3	Technology	26	France	16	Destruction	1
Indonesia	2	Energy	24	United Kingdom	15		

Recent Actor Activity

Gekko Jackal
LAST ACTIVE June 2016
TARGET NATIONS 3 Malaysia, United Kingdom, United States
TARGET INDUSTRIES 4 Aerospace & Defense, Financials, Governmen...
View Profile

Fancy Bear
LAST ACTIVE June 2016
TARGET NATIONS 22 Belgium, Brazil, Bulgaria, Canada, China, Fr...
TARGET INDUSTRIES 4 Aerospace & Defense, Energy, Government,...
View Profile

Cozy Bear
LAST ACTIVE June 2016
TARGET NATIONS 17 Austria, Brazil, China, France, Germany, Hu...
TARGET INDUSTRIES 13 Aerospace & Defense, Energy, Financials, G...
View Profile

Deep Panda
LAST ACTIVE May 2016
TARGET NATIONS 14 Australia, Canada, China, Germany, Hong Ko...
TARGET INDUSTRIES 13 Aerospace & Defense, Dissident, Financials, ...
View Profile

Numbered Panda
LAST ACTIVE May 2016
TARGET NATIONS 3 Japan, Taiwan, United States
TARGET INDUSTRIES 4 Financials, Government, Media & Publishing...

Lotus Panda
LAST ACTIVE May 2016
TARGET NATIONS 4 Philippines, Taiwan, United States, Vietnam
TARGET INDUSTRIES 7 Aerospace & Defense, Energy, Government...

Hammer Panda
LAST ACTIVE May 2016
TARGET NATIONS 4 India, Russian Federation, United States, Uz...
TARGET INDUSTRIES 4 Aerospace & Defense, Financials, Governme...

Static Spider
LAST ACTIVE May 2016
TARGET NATIONS -
TARGET INDUSTRIES -

AUTOMATE INVESTIGATIONS

Leverage advanced threat intel and artificial intelligence to detect threats

STOP BREACHES

Prevent both malware and malware-free attacks

INCREASED PRODUCTIVITY

Lower costs and improve performance with 24/7 cloud delivery

DETECT, EVALUATE, AND RESPOND TO THREATS AUTOMATICALLY WITH **CROWDSTRIKE** AND **HEXADITE AIRS**

Falcon Host identifies and alerts on suspicious activity on a host that would be invisible to traditional malware-centric defenses.

Alerts from CrowdStrike automatically trigger **Hexadite Automated Incident Response Solution (AIRS)** to launch a full investigation.

Hexadite AIRS combines its own artificial intelligence with the real-time threat intel on the top threat actors, attack vectors and trends from **Falcon Intelligence** to determine whether an alert is benign or an attack.

Once a threat has been verified as malicious, Hedadite AIRS can automatically execute network remediation actions, such as quarantining files, killing processes, blocking IPs, and dozens of other actions, with or without human intervention

AUTOMATE THE DETECT-TO-RESPONSE LIFECYCLE

Challenge:
As attacks and subsequent alerts increase, security teams lack the resources to follow up on every lead.

Solution:
Endpoint events recognized by CrowdStrike automatically trigger Hexidate AIRS to launch an investigation and evaluate the threat, performing remediation actions when a threat is deemed malicious.

Customer Benefit:
Customers save time, money, and resources automating the detect-to-response lifecycle, strengthening their overall security.

COORDINATE PROACTIVE DEFENSE ACTIONS

Challenge:
Organizations need to proatively block attacks before a breach occurs. Stopping an attack requires both detection and response simultaneously.

Solution:
The integration between CrowdStrike and Hexadite allows joint customers to combine endpoint detection, threat evaluation, and remendation to expedite both detection and response.

Customer Benefit:
Customers are able to protect themselves against attacks by coordinating proactive defensive actions automatically

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 Hexadite

Modeled after the investigative and decision-making skills of top cyber analysts and driven by artificial intelligence, Hexadite Automated Incident Response Solution (AIRS™) remediates threats and compresses weeks of work into minutes. With analysts free to focus on the most advanced threats, Hexadite optimizes overtaxed security resources for increased productivity, reduced costs and stronger overall security.