CrowdStrike Cybersecurity Conference
10.2020
falconexperience.crowdstrike.com
Cautionary Statement Regarding Forward-Looking Statements

This presentation includes express and implied “forward-looking statements”, including forward-looking statement within the meaning of the Private Securities Litigation Reform Act of 1995. Forward-looking statements include all statements that are not historical facts, and in some cases, can be identified by terms such as “anticipate,” “believe,” “estimate,” “expect,” “intend,” “may,” “might,” “plan,” “project,” “will,” “would,” “should,” “could,” “can,” “predict,” “potential,” “continue,” or the negative of these terms, and similar expressions that concern our expectations, strategy, plans or intentions. Forward-looking statements contained in this presentation include, but are not limited to, statements concerning the performance and benefits of our platform, products and services; our strategic plans or objectives; our growth prospects; and our future financial and operational performance. By their nature, these statements are subject to numerous risks and uncertainties, including factors beyond our control, that could cause actual results, performance or achievement to differ materially and adversely from those anticipated or implied in the statements. These and other risk factors are described in the “Risk Factors” section of our most recent Form 10-Q and/or Form 10-K filed with the Securities and Exchange Commission. You should not rely upon forward-looking statements as predictions of future events. Although our management believes that the expectations reflected in our statements are reasonable, we cannot guarantee that the future results, levels of activity, performance or events and circumstances described in the forward-looking statements will be achieved or occur. Recipients are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date such statements are made and should not be construed as statements of fact. Except to the extent required by federal securities laws, we undertake no obligation to update these forward-looking statements to reflect events or circumstances after the date hereof, or to reflect the occurrence of unanticipated events.
See More, Know More, Do More With Cloud Security Posture Management

Anand Visvanathan, Directory of Product Management, CrowdStrike
Arlene Watson, Director of Engineering, CrowdStrike
Agenda

- Limitations in Today’s CSPM Approach
- CrowdStrike’s Approach to Securing our Cloud
- CrowdStrike CSPM
Anand Visvanathan
Director of Product Management

- Product management leader at CrowdStrike for CSPM, Spotlight & Discover
- 20+ years of experience in the Cybersecurity, Vulnerability and GRC
Arlene Watson
Director of Engineering

- Engineering leader at CrowdStrike for CSPM and Discover for Cloud.
- Extensive experience driving cloud and Data technologies in Threat Intelligence, SIR, Vulnerability and GRC.
Some Recent Cloud Breaches

**Docker Hub**
- 190,000 accounts
- Chtrbox
- Lack of passwords, MFA, anomaly awareness

**Capital One**
- 80,000 bank accounts
- Misconfigured firewall
- Configuration, anomaly detection

**AutoClerk**
- 179 GB of data
- Unsecured Elasticsearch database on AWS
- Permission proliferation
Security Issues With Cloud Infrastructure

**Human Mistakes**
- Misconfiguration, e.g., S3
- Open ports
- Use of insecure APIs

**Runtime Threats**
- Adversaries
- APTs / Zero Day
- Vulnerabilities

**Shadow IT**
- Lack of Visibility
- Unauthorized usage
- Unsecured assets

**Lack of Knowledge**
Limitation of Today’s CSPM Approach

“What you need” vs. “What the current tool can provide”

Limited to data plane/control plane vs Unified with workload & application

Standard best practices vs. Adversarial threat hunting
CrowdStrike Approach
CrowdStrike Cloud Security Approach

**Know**
Your Adversary

**Reduce**
Your Risk of Exposure

**Monitor**
Your Attack Surface
Protecting One of The Biggest Cloud Environments in the World

- 470 BILLION EVENTS/DAY
- 14 PETABYTES OF DATA
- 1000s of MICROSERVICES ACROSS MULTIPLE HYBRID CLOUDS

**Protect Data**

**PRACTICAL ACTIONS**

- Falcon Linux Sensor
- Cloud Logs & Config
- Streaming Correlation Engine
- Proactive Hunting
- Cloud Specific IOAs
Increase Visibility of Attack Surface

**VISIBILITY**
- Cloud Configs
- Cloud Services, API

**LOG ANALYSIS**
- Log Aggregation
- Cloud, Instances, Flow

**HUNTING**
- Cloud-Specific
- Console & Email Alert Notification

**RUNTIME SECURITY**
- Falcon Platform
- 24 X 7 OverWatch

©2020 CROWDSTRIKE
Single View of Configuration Security Intelligence

- Most critical security risks
- Security risk ranking by service
- Region based security risks
- Account based security risks
- Scan History & Trend of security risks by service
Multidimensional Scan Report

Analyze your cloud security risks by:
- severity
- accounts
- services
- regions
- policies
- with drilldowns at a single click.

Perform historical scan analysis with easy to navigate on-screen drop-downs.
Insecure Cloud Resource Detail Discovery and Remediation

Remediation steps with single click access to the best practice documentations.
Details findings of misconfigurations and associated security risks.
On-screen resource detail panel for in-dept investigations within Falcon.
### Flexible Cloud Configuration Policy Management

#### Policies

Select a service to choose policies you want included in your scans.

<table>
<thead>
<tr>
<th>Service</th>
<th>Name</th>
<th>Service Subtype</th>
<th>Severity</th>
<th>Enabled</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2</td>
<td>AWS EC2 Instance configured with Virtual Private Gateways shouldn't be assigned to public IP addresses.</td>
<td>Virtual Private Gateways, Security Group</td>
<td>High</td>
<td>Enabled</td>
<td>AWS EC2 Instance configured with Virtual Private Gateways shouldn't be assigned to public IP addresses.</td>
</tr>
<tr>
<td>EC2</td>
<td>EC2 high privileged instance profile with IAM inline policy</td>
<td>Managed policy on role(s) applied to EC2 instance profile</td>
<td>High</td>
<td>Enabled</td>
<td>Virtual Private Gateways Security Group</td>
</tr>
<tr>
<td>EC2</td>
<td>EC2 high privileged instance profile with IAM managed policy</td>
<td>EC2 instance profile, IAM role managed policy</td>
<td>Medium</td>
<td>Enabled</td>
<td>Settings</td>
</tr>
<tr>
<td>EC2</td>
<td>EC2 instance publicly configured allows global public IP in a ingress rule on non-web ports.</td>
<td>Security Group Ingress Rule with IP Address</td>
<td>Medium</td>
<td>Enabled</td>
<td>Virtual Private Gateways and Transit Gateways should not be publicly accessible, as they are typically intended for private communications. By exposing them to the internet, you increase the risk of compromise from an external attacker, because resources that are intended to be private may be</td>
</tr>
<tr>
<td>EC2</td>
<td>EC2 instance publicly configured allows global public IP in ingress rule(s) and high risk port(s).</td>
<td>Security Group, Ingress Rule with IP Address and Ports</td>
<td>High</td>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>

- Adjust severity per policy based on your organization’s security posture.
- Enable and disable scans per policy per your security policy.
Streamlined Account Registration and Scan Schedule Settings

Flexible cloud account registration options including:

- Organization accounts
- Batch of individual accounts
- Single accounts

Single click account deregistration for both organization and individual accounts.

Set your own cloud configuration scan schedule to:

- Manage new scan frequencies
- Control the API usage

©2020 CROWDSTRIKE
Key Takeaways

Having a best-practices-based approach for securing your cloud infrastructure is not sufficient.

Develop a proactive monitoring and cloud hunting plan.

Try CrowdStrike CSPM.
We look forward to your input to help us continue to make Fal.Con better year after year.

Please fill out the survey at the link below and provide your feedback – you will be entered to win $300 on items from the CrowdStrike Swag Store!