Security Operations

B

h2 2023-11-23T21:15:00.083867Z app/production-app-lb/3ee0698f49fe8d39 103.236.201.88:49203 10.240.30.177:8080 0.002 0.168 0.000 200 200 135 8120 "POST https://apptastic.io:443/login HTTP/2.0" "FNetwork/1410.0.3 Darwin/22.6.0" ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 arn:aws:elasticloadbalancing:us-east-1:226692608800:targetgroup/production-target/3e4e18eadc57fcc8 "Root=1-6536e253-74cc2f2613f7ff515507343b" "apptastic.io" "arn:aws:acm:us-east-1:226692608800:certificate/76c4d867-fc78-49f1-a8dc-daa557abf852" 3 2023-11-23T21:14:59.914000Z "waf,forward" "-" "-" "10.240.30.177:8080" "200" "-" "-"

Log Review: The AWS Application Load Balancer (ALB) is used to distribute and redirect inbound network traffic across multiple targets and availability zones. Logs are typically captured in-line with the ALB and stored in a S3 bucket.

ALB access logs follow this format: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html#access-log-file-format

Security Operations

A

This Spike in user-reported spam alert is to inform you that an unusually high volume of messages from a sender have been marked as spam on 2023-11-23.

The alert details include:

Summary: 74 message(s) were reported as spam by users in your domain. There were 3 recipient(s): ciso@apptastic.io, marketing@apptastic.io, finance@apptastic.io. Sender of the message originated from @borealis.com domain.

Log Review: Many email systems generate automated messages if there is a high volume of reported spam messages. In this case, the system generated alert identified 74 messages that were marked as spam by 3 email addresses.

Security Operations

B


```
{
  “debugContext.debugData.factor”: “OKTA_VERIFY_PUSH”,
  “debugContext.debugData.factorIntent”: “AUTHENTICATION”,
  “debugContext.debugData.pushOnlyResponseType”: “OV_RESPONSE_DENY”
  “displayMessage”: “Authentication of user via MFA”,
  “actor.alternateId”: “juniper-msp@apptastic.io”,
  “client.ipAddress”: “103.236.201.88”
}
```


Log Review: Activity logs from the company’s identity system can be used to identify potentially suspicious or abnormal activity. In this case, the activity logs describe a failed authentication action with Multi-Factor Authentication (MFA). The log identifies the ID of the user or actor along with the IP address where the action originated from.

In this case, the logs identified 200+ failed (DENY) MFA requests to this user account between 03:00 and 07:00 UTC and 1 successful (SUCCESS) MFA request at 07:00 UTC on Nov 23, 2023.

GRC

A

Vendor Assessment Report: Borealis

Borealis is a managed IT and System Administration services company based in the United States. Apptastic plans to use Borealis to staff numerous support roles including IT Help Desk, Database Administration (DBA) and System Admins. A security assessment of Borealis identified 2 medium severity risks.

1. Borealis staff did not complete all assigned security training on schedule.
2. Not all laptops provided to Borealis staff had proper security software configured.

Vendor Assessments: Companies typically conduct vendor security reviews or assessments to evaluate the security risks involved in doing business with the vendor. These reviews cover documentation provided by the vendor and audit reports or certifications (if available). Risks are documented and communicated so that the company (customer) can make informed risk-based decisions.

Security Operations

B


```
{
  “debugContext.debugData.factor”: “OKTA_VERIFY_PUSH”,
  “debugContext.debugData.factorIntent”: “AUTHENTICATION”,
  “debugContext.debugData.pushOnlyResponseType”: “OV_RESPONSE_DENY”
  “displayMessage”: “Authentication of user via MFA”,
  “actor.alternateId”: “athena-msp@apptastic.io”,
  “client.ipAddress”: “103.236.201.88”
}
```


Log Review: Activity logs from the company’s identity system can be used to identify potentially suspicious or abnormal activity. In this case, the activity logs describe a failed authentication action with Multi-Factor Authentication (MFA). The log identifies the ID of the user or actor along with the IP address where the action originated from.

In this case, the logs identified 200+ failed (DENY) MFA requests to this user account between 03:00 and 07:00 UTC on Nov 23, 2023.

Security Operations

B


```
{
  “debugContext.debugData.factor”: “OKTA_VERIFY_PUSH”,
  “debugContext.debugData.factorIntent”: “AUTHENTICATION”,
  “debugContext.debugData.pushOnlyResponseType”: “OV_RESPONSE_DENY”
  “displayMessage”: “Authentication of user via MFA”,
  “actor.alternateId”: “ares-msp@apptastic.io”,
  “client.ipAddress”: “103.236.201.88”
}
```


Log Review: Activity logs from the company’s identity system can be used to identify potentially suspicious or abnormal activity. In this case, the activity logs describe a failed authentication action with Multi-Factor Authentication (MFA). The log identifies the ID of the user or actor along with the IP address where the action originated from.

In this case, the logs identified 200+ failed (DENY) MFA requests to this user account between 03:00 and 07:00 UTC on Nov 23, 2023.

Security Operations

B


```
{
  “debugContext.debugData.factor”: “OKTA_VERIFY_PUSH”,
  “debugContext.debugData.factorIntent”: “AUTHENTICATION”,
  “debugContext.debugData.pushOnlyResponseType”: “OV_RESPONSE_DENY”
  “displayMessage”: “Authentication of user via MFA”,
  “actor.alternateId”: “artemis-msp@apptastic.io”,
  “client.ipAddress”: “103.236.201.88”
}
```


Log Review: Activity logs from the company’s identity system can be used to identify potentially suspicious or abnormal activity. In this case, the activity logs describe a failed authentication action with Multi-Factor Authentication (MFA). The log identifies the ID of the user or actor along with the IP address where the action originated from.

In this case, the logs identified 200+ failed (DENY) MFA requests to this user account between 03:00 and 07:00 UTC on Nov 23, 2023.

Security Operations

A

Dear AWS Customer,

As part of our AWS Shield Advanced offering, we noticed a significant volume of traffic against your public Elastic IPs in 226692608800. This is usually indicative of a DDOS attack. We recommend you block all IP addresses identified in the WAF logs.

109.201.133.100
109.70.100.65
185.220.100.243

Please create an AWS Support ticket if you would like to chat with an agent in real time.

AWS Shield: AWS provides varying levels of DDOS detection, protection and mitigation through its AWS Shield server. A DDOS (Distributed Denial of Service) attack is a type of attack where a server or system is flooded with a lot of web traffic to the point where the server can become unresponsive. DDOS attacks can be instigated using stolen (compromised) servers or other means.

Security Engineering

B

IP Address: 185.220.100.243
Decimal:1743571288
Hostname:ip103-236-201-88.cloudhost.web.id
ASN:136052
ISP:PT Cloud Hosting Indonesia
Services:Tor Exit Node
Assignment:Likely Static IP

Threat Intelligence: IP lookups are typically done to find out more information about an IP address. IP addresses should have a DNS (Domain Name System) record associated with it that identifies the owner, location and use of the IP address.

Think of DNS as the phone book (or directory) of the internet.

TOR exit nodes are the nodes on the TOR network that traffic exit from.

Security Engineering

B

IP Address: 109.201.133.100
Decimal:1841923428
Hostname:
ASN:43350
ISP:NForce Entertainment B.V.
Services:Tor Exit Node / Recently reported forum spam source. (307)
Assignment:Likely Static IP

Threat Intelligence: IP lookups are typically done to find out more information about an IP address. IP addresses should have a DNS (Domain Name System) record associated with it that identifies the owner, location and use of the IP address.

Think of DNS as the phone book (or directory) of the internet.

TOR exit nodes are the nodes on the TOR network that traffic exit from.

Security Engineering

B

IP Address: 103.236.201.88
Decimal:3118228723
Hostname:tor-exit-16.zbau.f3netze.de
ASN:205100
ISP:F3 Netze E.V.
Services:Tor Exit Node / Recently reported forum spam source. (4533)
Assignment:Likely Static IP

Threat Intelligence: IP lookups are typically done to find out more information about an IP address. IP addresses should have a DNS (Domain Name System) record associated with it that identifies the owner, location and use of the IP address.

Think of DNS as the phone book (or directory) of the internet.

TOR exit nodes are the nodes on the TOR network that traffic exit from.

Security Engineering

B

IP Address: 109.70.100.65
Decimal:1833329729
Hostname:tor-exit-anonymizer.appliedprivacy.net
ASN:208323
ISP:Foundation for Applied Privacy
Services:Tor Exit Node / Recently reported forum spam source. (267)
Assignment:Likely Static IP

Threat Intelligence: IP lookups are typically done to find out more information about an IP address. IP addresses should have a DNS (Domain Name System) record associated with it that identifies the owner, location and use of the IP address.

Think of DNS as the phone book (or directory) of the internet.

TOR exit nodes are the nodes on the TOR network that traffic exit from.

Security Engineering

B

IP Address: 199.249.230.180
Decimal:3355043508
Hostname:tor91.quintex.com
ASN:62744
ISP:Quintex Alliance Consulting
Services:Tor Exit Node
Assignment:Likely Static IP

Threat Intelligence: IP lookups are typically done to find out more information about an IP address. IP addresses should have a DNS (Domain Name System) record associated with it that identifies the owner, location and use of the IP address.

Think of DNS as the phone book (or directory) of the internet.

TOR exit nodes are the nodes on the TOR network that traffic exit from.

GRC

A

Risk Exception Request
Status: Approved by Jimmy Livvy (CTO)
Approved On: 9/5/2022

Risk: Borealis staff did not complete all assigned security training on schedule.

Rationale:
1. Borealis will remind its employees to complete their required training on phishing and MFA fatigue. This should not stop our ability to work with Borealis.

Risk Exceptions: Companies typically accept some level of risk for various reasons. A risk exception process allows companies to identify the risk, and with the right level of approval, accept it with proper justification. Typically, risk exceptions are revisited and re-approved every year because circumstances change.

Security Engineering

B

IP Address: 3.33.145.223
Decimal:52531679
Hostname:ae7f7cd4514c83ac6.awsglobalaccelerator.com
ASN:16509
ISP:Amazon Technologies Inc
Services:Datacenter
Assignment:Likely Static IP

Threat Intelligence: IP lookups are typically done to find out more information about an IP address. IP addresses should have a DNS (Domain Name System) record associated with it that identifies the owner, location and use of the IP address.

Think of DNS as the phone book (or directory) of the internet.

In this case, the IP address is one of many allocated to Amazon Web Services.

Security Operations

C

HTTP/1.1 200 OK
Date: Wed, 24 Nov 2023 05:09:20 GMT
Content-Type: text/html
Content-Length: 48822
Connection: keep-alive
Location: https://homeroom.apptastic.io
Cache-Control: no-cache

Application: HTTP responses like this are messages that application servers typically send back in response to a request. In normal operations, the server should respond with a HTTP 200 OK message. If there are errors, the server may then respond with a 403, 404, 500 or other related error code.

For reference, here is a list of HTTP response status codes:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

GRC

A

Asset: monitoring.apptastic.io
Type: EC2 Servers
IP Address: 10.240.30.111
Port: 443
Classification: Confidential
Owner: Jimmy Livvy (CTO)
Last Updated: March 20, 2023

Asset Inventory: Companies typically maintain an asset inventory or Configuration Management Database (CMDB) that lists all discoverable assets the company has along with certain types of metadata, such as asset type, IP address and owner. It is important to associate owners with assets so that teams know who to contact if there are issues with the asset.

GRC

A

Asset: api.apptastic.io
Type: EC2 Servers
IP Address: 10.240.30.90
Port: 443
Classification: Confidential
Owner: Jimmy Livvy (CTO)
Last Updated: March 12, 2023

Asset Inventory: Companies typically maintain an asset inventory or Configuration Management Database (CMDB) that lists all discoverable assets the company has along with certain types of metadata, such as asset type, IP address and owner. It is important to associate owners with assets so that teams know who to contact if there are issues with the asset.

GRC

A

Asset: retrieval.apptastic.io
Type: EC2 Servers
IP Address: 10.240.30.177
Port: 8080
Classification: Confidential
Owner: Margaret Thatcher (Marketing Director)
Last Updated: May 5, 2019

Asset Inventory: Companies typically maintain an asset inventory or Configuration Management Database (CMDB) that lists all discoverable assets the company has along with certain types of metadata, such as asset type, IP address and owner. It is important to associate owners with assets so that teams know who to contact if there are issues with the asset.

GRC

A

Asset: finance.important.sap.com
Type: EC2 Servers
IP Address: 10.240.31.50
Port: 443
Classification: Confidential
Owner: Johnny Snowman (CFO)
Last Updated: August 9, 2023

Asset Inventory: Companies typically maintain an asset inventory or Configuration Management Database (CMDB) that lists all discoverable assets the company has along with certain types of metadata, such as asset type, IP address and owner. It is important to associate owners with assets so that teams know who to contact if there are issues with the asset.

GRC

A

Asset: turnkey.api.apptastic.io
Type: EC2 Servers
IP Address: 10.240.155.100
Port: 443
Classification: Confidential
Owner: Data Science
Last Updated: Nov 10, 2023

Asset Inventory: Companies typically maintain an asset inventory or Configuration Management Database (CMDB) that lists all discoverable assets the company has along with certain types of metadata, such as asset type, IP address and owner. It is important to associate owners with assets so that teams know who to contact if there are issues with the asset.

GRC

A

Asset: step.apptastic.io
Type: ECS Cluster
IP Address: 10.100.0.198
Port: 22
Classification: Confidential
Owner: Human Resources
Last Updated: August 1, 2022

Asset Inventory: Companies typically maintain an asset inventory or Configuration Management Database (CMDB) that lists all discoverable assets the company has along with certain types of metadata, such as asset type, IP address and owner. It is important to associate owners with assets so that teams know who to contact if there are issues with the asset.

GRC

A

Audit: Annual NIST CSF Audit
Completed: Feb 24, 2023

Sub-Category: DE.CM-4: Malicious code is detected

Finding: Only 63% of company servers have Crowdstrike installed and running. Of the remaining 37% of servers, they are used to run a number of critical systems including API, Monitoring and SAP.

Audits: Company typically conduct audits to evaluate the effectiveness of their security and other technology controls. Audits can be external (by third party auditors) or internal (internal teams). Findings from audits should be reviewed.

The NIST Cybersecurity Framework (CSF) is an international security framework published by NIST. It covers a range of security categories intended to help companies build effective security programs and controls.

GRC

A

Audit: Quarterly Access Reviews
Completed: August 19, 2023

User Lists: juniper-msp@apptastic.io, athena-msp@apptastic.io, ares-msp@apptastic.io, artemis-msp@apptastic.io, jimmy@apptastic.io, lauren@apptastic.io, thistle@apptastic.io, lagrange@apptastic.io, jennifer@apptastic.io

Audits: Company typically conduct audits to evaluate the effectiveness of their security and other technology controls. Audits can be external (by third party auditors) or internal (internal teams). Findings from audits should be reviewed.

In this case, a user access review is done to determine whether accounts to company systems are appropriate. If the access is not appropriate, companies typically have processes to deactivate those accounts.

GRC

A

Password Policy

Minimum of 12 characters
Must include:

- at least one uppercase (capital letter) character
- at least one lowercase character
- at least one numerical (0 to 9) character
- at least one non-alphabetic (special) character - #, !, *, $, %

Does not include your username or email address
Does not reuse the last 5 passwords
Enable Two-Factor Authentication (2FA) (mandatory)

Policy: Company typically have policies to define company-wide requirements for security, privacy, ethics and other compliance topics. In this case, the Password Policy should define the minimum password requirements that all company systems have to implement or use.

GRC

A

Risk Mitigation
Status: Approved by Steering Committee
Approved On: 9/1/2022

Risk: Not all laptops provided to Borealis staff had proper security software configured.

Mitigation:

1. Add to the contract with Borealis that they are required to roll out standard security software, defined as antivirus and host-based firewalls, to all company laptops.

Risk Mitigations: For risks that the company does not accept, transfer or avoid, they should have mitigation plans in place. Mitigation plans are projects or tasks that, when complete, help reduce the likelihood or impact of a risk. Typically, risk mitigations are reviewed and/or approved by an individual or group within a Company.

GRC

A

Backup Policy

1. Full daily backups are taken of all Aurora PostgreSQL databases in RDS.
2. Backups are encrypted using AES-256 or higher
3. Backups are stored in a dedicated S3 Bucket in AWS
4. Backup failures are investigated within 24 hours by the Site Reliability Engineering team.
    a. If the cause of the failure is identified, a root cause analysis is documented in JIRA.
    b. If the cause of the failure is unknown, a P1 incident will be created

Policy: Company typically have policies to define company-wide requirements for security, privacy, ethics and other compliance topics. In this case, the Backup Policy should define the standards by which the company takes and stores system backups.

GRC

A

Risk Mitigation
Status: Approved by Steering Committee
Approved On: 9/1/2022

Risk: Not all laptops provided to Borealis staff had proper security software configured.

Mitigation:
1. Add to the contract with Borealis that they are required to roll out standard security software, defined as antivirus and host-based firewalls, to all company laptops.

Risk Mitigations: For risks that the company does not accept, transfer or avoid, they should have mitigation plans in place. Mitigation plans are projects or tasks that, when complete, help reduce the likelihood or impact of a risk. Typically, risk mitigations are reviewed and/or approved by an individual or group within a Company.

Security Operations

C

HTTP/1.1 500 Internal Server Error
Date: Wed, 24 Nov 2023 06:02:44 GMT
Content-Type: text/html
Content-Length: 102
Connection: keep-alive
Location: https://retrieval.apptastic.io
Cache-Control: no-cache

Application: HTTP responses like this are messages that application servers typically send back in response to a request. In normal operations, the server should respond with a HTTP 200 OK message. If there are errors, the server may then respond with a 403, 404, 500 or other related error code.

For reference, here is a list of HTTP response status codes:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

Security Operations

C

HTTP/1.1 500 Internal Server Error
Date: Wed, 24 Nov 2023 06:05:44 GMT
Content-Type: text/html
Content-Length: 102
Connection: keep-alive
Location: https://api.apptastic.io
Cache-Control: no-cache

Application: HTTP responses like this are messages that application servers typically send back in response to a request. In normal operations, the server should respond with a HTTP 200 OK message. If there are errors, the server may then respond with a 403, 404, 500 or other related error code.

For reference, here is a list of HTTP response status codes:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

Security Operations

C

HTTP/1.1 500 Internal Server Error
Date: Wed, 24 Nov 2023 06:30:44 GMT
Content-Type: text/html
Content-Length: 102
Connection: keep-alive
Location: https://monitoring.apptastic.io
Cache-Control: no-cache

Application: HTTP responses like this are messages that application servers typically send back in response to a request. In normal operations, the server should respond with a HTTP 200 OK message. If there are errors, the server may then respond with a 403, 404, 500 or other related error code.

For reference, here is a list of HTTP response status codes:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

Security Engineering

A

List of Backups:

rds:apptastic-postgresql-2023-11-07-21-13	Nov 7, 2023 14:41 UTC	Completed
rds:apptastic-postgresql-2023-11-08-21-13	Nov 8, 2023 14:40 UTC	Completed
rds:apptastic-postgresql-2023-11-09-21-13	Nov 9, 2023 14:37 UTC	Completed
rds:apptastic-postgresql-2023-11-10-21-13	Nov 10, 2023 14:45 UTC	Completed
rds:apptastic-postgresql-2023-11-11-21-13	Nov 11, 2023 14:41 UTC	Completed
rds:apptastic-postgresql-2023-11-12-21-13	Nov 12, 2023 14:40 UTC	Completed
rds:apptastic-postgresql-2023-11-13-21-13	Nov 13, 2023 14:30 UTC	Failure
rds:apptastic-postgresql-2023-11-14-21-13	Nov 14, 2023 14:31 UTC	Failure
rds:apptastic-postgresql-2023-11-15-21-13	Nov 15, 2023 14:28 UTC	Failure
rds:apptastic-postgresql-2023-11-16-21-13	Nov 16, 2023 14:35 UTC	Failure
rds:apptastic-postgresql-2023-11-17-21-13	Nov 17, 2023 14:32 UTC	Failure

Backups: Companies typically take backups (or snapshots) of databases and other important systems so that they have a copy that they can restore if something goes wrong. It is important that these backups are taken regularly and kept in a secure location. If there are failures with the backup process, the company should investigate the failure as soon as possible.

Security Engineering

A

List of Backups:

rds:step-use1-postgresql-2023-11-07-21-13	Nov 7, 2023 12:41 UTC	Completed
rds:step-use1-postgresql-2023-11-08-21-13	Nov 8, 2023 12:40 UTC	Completed
rds:step-use1-postgresql-2023-11-09-21-13	Nov 9, 2023 12:37 UTC	Completed
rds:step-use1-postgresql-2023-11-10-21-13	Nov 10, 2023 12:45 UTC	Completed
rds:step-use1-postgresql-2023-11-11-21-13	Nov 11, 2023 12:41 UTC	Completed
rds:step-use1-postgresql-2023-11-12-21-13	Nov 12, 2023 12:40 UTC	Completed
rds:step-use1-postgresql-2023-11-13-21-13	Nov 13, 2023 12:30 UTC	Completed
rds:step-use1-postgresql-2023-11-14-21-13	Nov 14, 2023 12:31 UTC	Completed
rds:step-use1-postgresql-2023-11-15-21-13	Nov 15, 2023 12:28 UTC	Completed
rds:step-use1-postgresql-2023-11-16-21-13	Nov 16, 2023 12:35 UTC	Completed
rds:step-use1-postgresql-2023-11-17-21-13	Nov 17, 2023 12:32 UTC	Completed

Backups: Companies typically take backups (or snapshots) of databases and other important systems so that they have a copy that they can restore if something goes wrong. It is important that these backups are taken regularly and kept in a secure location. If there are failures with the backup process, the company should investigate the failure as soon as possible.

Security Engineering

A

List of Backups:

rds:kube-layer-postgresql-2023-11-07-21-13	Nov 7, 2023 14:42 UTC	Completed
rds:kube-layer-postgresql-2023-11-08-21-13	Nov 8, 2023 14:48 UTC	Completed
rds:kube-layer-postgresql-2023-11-09-21-13	Nov 9, 2023 14:55 UTC	Completed
rds:kube-layer-postgresql-2023-11-10-21-13	Nov 10, 2023 14:55 UTC	Completed
rds:kube-layer-postgresql-2023-11-11-21-13	Nov 11, 2023 14:31 UTC	Completed
rds:kube-layer-postgresql-2023-11-12-21-13	Nov 12, 2023 14:20 UTC	Completed
rds:kube-layer-postgresql-2023-11-13-21-13	Nov 13, 2023 14:40 UTC	Failure
rds:kube-layer-postgresql-2023-11-14-21-13	Nov 14, 2023 14:21 UTC	Completed
rds:kube-layer-postgresql-2023-11-15-21-13	Nov 15, 2023 14:58 UTC	Completed
rds:kube-layer-postgresql-2023-11-16-21-13	Nov 16, 2023 14:35 UTC	Failure
rds:kube-layer-postgresql-2023-11-17-21-13	Nov 17, 2023 14:22 UTC	Completed

Backups: Companies typically take backups (or snapshots) of databases and other important systems so that they have a copy that they can restore if something goes wrong. It is important that these backups are taken regularly and kept in a secure location. If there are failures with the backup process, the company should investigate the failure as soon as possible.

Security Engineering

A

List of Backups:

rds:homeroom-postgresql-2023-11-07-21-13	Nov 7, 2023 12:41 UTC	Completed
rds:homeroom-postgresql-2023-11-08-21-13	Nov 8, 2023 12:40 UTC	Completed
rds:homeroom-postgresql-2023-11-09-21-13	Nov 9, 2023 12:37 UTC	Completed
rds:homeroom-postgresql-2023-11-10-21-13	Nov 10, 2023 12:45 UTC	Completed
rds:homeroom-postgresql-2023-11-11-21-13	Nov 11, 2023 12:41 UTC	Completed
rds:homeroom-postgresql-2023-11-16-21-13	Nov 16, 2023 12:35 UTC	Completed
rds:homeroom-postgresql-2023-11-17-21-13	Nov 17, 2023 12:32 UTC	Completed

Backups: Companies typically take backups (or snapshots) of databases and other important systems so that they have a copy that they can restore if something goes wrong. It is important that these backups are taken regularly and kept in a secure location. If there are failures with the backup process, the company should investigate the failure as soon as possible.

GRC

A

Vendor Assessment Report: Homeroom

Homeroom is a SaaS based work management tool typically used by Human Resource teams to manage employee engagement and feedback. Teams upload employee files via CSV or integrate Homeroom with the company Payroll system. Employee engagement is then tracked via a variety of means ranging from surveys to user analytics across the duration of the individual's employment.

1. There is a lot of data stored. Consider auto deleting data every 12 months.

Vendor Assessments: Companies typically conduct vendor security reviews or assessments to evaluate the security risks involved in doing business with the vendor. These reviews cover documentation provided by the vendor and audit reports or certifications (if available). Risks are documented and communicated so that the company (customer) can make informed risk-based decisions.

GRC

A

Vendor Assessment Report: AWS

AWS is an Infrastructure-as-a-Service (IaaS) provider that offers a range of services that companies can use to manage their cloud infrastructure. AWS' data centers span multiple countries (regions) and availability zones (physical buildings). Access to the AWS Console is controlled using Single Sign On (SSO) and other means. There are no additional recommendations in this report.

Vendor Assessments: Companies typically conduct vendor security reviews or assessments to evaluate the security risks involved in doing business with the vendor. These reviews cover documentation provided by the vendor and audit reports or certifications (if available). Risks are documented and communicated so that the company (customer) can make informed risk-based decisions.

GRC

A

Vendor Assessment Report: Okta

Okta is a SaaS based identity management platform used by companies to manage access to various applications. Okta uses Single Sign On (SSO) via the SAML 2.0 protocol, OIDC and other protocols to centralize access. Access to Okta is further protected with 2FA. Okta's services may be hosted in data centers across the world.

1. Every 12 months, audit the company's Okta configuration against security best practices and periodically review audit logs in Okta for suspicious activity.

Vendor Assessments: Companies typically conduct vendor security reviews or assessments to evaluate the security risks involved in doing business with the vendor. These reviews cover documentation provided by the vendor and audit reports or certifications (if available). Risks are documented and communicated so that the company (customer) can make informed risk-based decisions.

Security Engineering

A

Vulnerability Scan Report
monitoring.apptastic.io

Findings:
HIGH (2)

- Security groups to the servers permit full access on all ports (0.0.0.0/0)
- Server is listening on certain ports (ie., 21 and 23) that permit unencrypted traffic

Vulnerability Scans: Companies typically run security scans against applications, servers and other systems to identify potential vulnerabilities. These vulnerabilities are classified based on certain metrics (ie., CVSS). It is important to categorize these vulnerabilities (findings) and assign them to the right teams to triage.

Security Engineering

A

Vulnerability Scan Report
api.apptastic.io

Findings:
HIGH (2)

- Security groups to the servers permit full access on all ports (0.0.0.0/0)
- Server listens on port 443 to traffic from the ALB, but does not authenticate all requests.

Vulnerability Scans: Companies typically run security scans against applications, servers and other systems to identify potential vulnerabilities. These vulnerabilities are classified based on certain metrics (ie., CVSS). It is important to categorize these vulnerabilities (findings) and assign them to the right teams to triage.

Security Engineering

A

Vulnerability Scan Report
homeroom.apptastic.io

Findings:
LOW (2)

- Content Security Policy is partially implemented and includes unsafe scripts.
- Information in HTTP responses contains information about the proxy server.

Vulnerability Scans: Companies typically run security scans against applications, servers and other systems to identify potential vulnerabilities. These vulnerabilities are classified based on certain metrics (ie., CVSS). It is important to categorize these vulnerabilities (findings) and assign them to the right teams to triage.

Security Engineering

A

Vulnerability Scan Report
kube.manage.apptastic.io

Findings:
HIGH (1)

- Security groups to the servers permit full access on all ports (0.0.0.0/0)

Vulnerability Scans: Companies typically run security scans against applications, servers and other systems to identify potential vulnerabilities. These vulnerabilities are classified based on certain metrics (ie., CVSS). It is important to categorize these vulnerabilities (findings) and assign them to the right teams to triage.

Security Engineering

A

The Security Engineering team has read/write access to the AWS Backup service and has permissions to capture or restore from backups of RDS clusters, or archive backups to a dedicated S3 bucket.

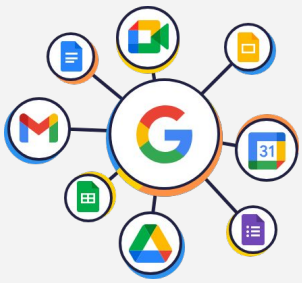
ACTIONS:

1. Restore a database from a backup.
2. Take a new backup from an existing database.

AWS Backup: AWS Backup services are used to automatically capture backups or snapshots of various resources such as RDS clusters and to restore backups to create a new cluster. Access to the AWS Backup service is controlled using the AWS Console.

Security Engineering

A



The Security Engineering team has full administrative access to the Google Workspace Admin console and services.

ACTIONS:

1. Add email addresses or domains to the SPAM list.
2. Disable user access.

Google Workspace: Google Workspace is a popular online collaboration and productivity suite that includes Google Email, Docs, Sheets, etc. Admin access to the Google Workspace services allows authorized users to manage users, application configurations, email routing and other privileged functions.

Security Engineering

A

The Security Engineering team has read/write access to the AWS WAF service and has permissions to edit all WAF Rules.

ACTIONS:

1. Add IP addresses to the WAF block list.

AWS WAF: A Web Application Firewall (WAF) is software that sits in front of web applications and can be configured, using rules, to detect and block certain traffic. A WAF is typically used for Layer 7 web traffic and can be used to block common web exploits, such as Cross-Site Scripting (XSS) or SQL Injection.

Security Engineering

A

The Security Engineering team has full administrative access to the Crowdstrike console.

ACTIONS:

1. Isolate infected systems.
2. Run on-demand anti-malware scan.

Crowdstrike: Crowdstrike is a popular antivirus software used by companies to protect devices against viruses, such as ransomware, spyware, etc. Crowdstrike works using agents (software) that are installed on a person's laptop. It can be configured to block certain types of attacks using signatures.

Security Operations

B

From: dc909e7dae4f47ecb7a0161adf7225e3
Private IP: 10.240.30.177
Port: 8081

To: 103.236.201.88
Port: 40931

DateTime: 2023-11-23T22:10:00

Log Review: Activity logs from the company's identity system can be used to identify potentially suspicious or abnormal activity. In this case, the activity logs describe traffic captured by AWS that shows data transfer between an EC2 instance with the designated private IP address to an external IP address.

GRC

A

Risk Exception Request
Status: Approved by Jimmy Livvy (CTO)
Approved On: 9/7/2022

Risk: Step service used by Human Resources does not support 2FA currently. If a user's password is compromised, the attacker could gain access to employee data.

Rationale:
1. Layered controls (ie., VPN) in place.

Risk Exceptions: Companies typically accept some level of risk for various reasons. A risk exception process allows companies to identify the risk, and with the right level of approval, accept it with proper justification. Typically, risk exceptions are revisited and re-approved every year because circumstances change.

Security Operations

Security Engineering

Governance
Risk
Compliance

CISO