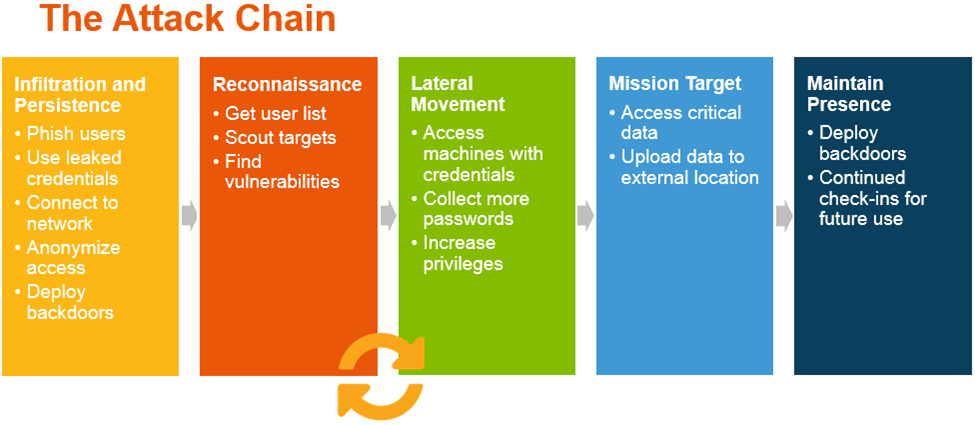
|  |
| --- |
| Zorg Industries |
|  |

# Memorandum

To: Hari Seldon CEO

From: Chad Ballay

Subject: Breach Lifecycle and Disruption Mechanism.



(Hayes, n.d.)

This is the quarterly update with regard to the recent efforts to harden our security posture as to disrupt future cybersecurity attacks. To help clarify the facets of the initiative, I’ll use the Attack Chain to frame the conversation.

### Infiltration and Persistence

During our last penetration test we discovered that our single biggest risk for attackers getting a foothold into our systems was our own users vulnerability to phishing attempts. For this phase we are attacking it by a broad push for end user education through post to our internal training site as well as policy update and mandatory online training video. We are still in the scoping phase of implementing an internally hosted phishing toolkit. The steering committee has been pleased with the selection of GoPhish. (Rivera, n.d.) (<https://github.com/gophish/gophish>)

### Reconnaissance

Limiting the information gathering ability has run into some blockers. We are in a reactionary mode for closing mechanisms that can be used to harvest information, but it still will require a sustained effort. The request for bids for a third party vulnerability scanning solution has failed to generate sufficient headway. (Edwards, n.d.) We will need to rebaseline our project plan during the next quarter. Vendors reviewed thus far are McAfee, Rapid7, and Nessus.

### Lateral Movement

Identifying suspicious behavior within our network once the attacker has breached our perimeter will be easier due to the restructuring and staff increase of our NOC. We are seeing a reduction in alert queues and an overall decrease in SLA times for research. We’ve also implemented HashiCorp’s Vault for credential/secret storage. (Manoske, n.d.) This effort has been our most visible thus far and our focus on clear branding and communication has helped tremendously on enterprise adoption.

### Mission Target

This stage of accessing data, denying our company the use of resources, or any of the other success criteria for attackers will not be quickly resolved. The various attack surfaces will require an iterative approach of continual review/refinement. We have reduced our attack surfaces by implementing several policies such as disabling of USB devices, outbound email scanning, and blocking of several external file hosting services. This still leaves much room for improvement.

### Maintaining Presence

Due to the static nature of our legacy applications we are allocating continued budget investment in automation tools for scanning and monitoring. For our green field, modern applications we’ve implemented several Cloud Native Architectural standards that help mitigate this. (Shivpuriya, n.d.) We believe our strong adoption of Infrastructure as Code, Containerization, and Chaos Testing will have the dual focus of creating resiliency and a regular clean sweeping. We are identifying several DevSecOps practices to include in our enterprise training goals. (Avner, n.d.)

# Works Cited

Avner, G. (n.d.). *DevSecOps: From Theory to Practice*. Retrieved from WhiteSource: https://resources.whitesourcesoftware.com/blog-whitesource/devsecops

Edwards, E. (n.d.). *Vulnerability scanning – in house or third party?* Retrieved from AT&T - Cybersecurity: https://cybersecurity.att.com/blogs/security-essentials/vulnerability-scanning-in-house-or-third-party

Hayes, K. A. (n.d.). *What is Incident Detection and Response?* Retrieved from Rapid7 Blog: https://blog.rapid7.com/2016/03/29/what-is-incident-detection-and-response/

Manoske, A. (n.d.). *Addressing Top Security Threats with Vault*. Retrieved from HashiCorp: https://www.hashicorp.com/blog/addressing-top-security-threats-with-vault/

Rivera, A. (n.d.). *Phish Your Own Business to Expose Vulnerabilities*. Retrieved from Business News Daily: https://www.businessnewsdaily.com/10940-phish-your-own-business.html

Shivpuriya, V. (n.d.). *Cloud Native*. Retrieved from InfoWorld: https://www.infoworld.com/article/3203265/security-in-a-cloud-native-environment.html

# Bibliography

**Much of the references here are for background context of goals and not reference of actual designs.**

Avner, G. (n.d.). *DevSecOps: From Theory to Practice*. Retrieved from WhiteSource: https://resources.whitesourcesoftware.com/blog-whitesource/devsecops

Edwards, E. (n.d.). *Vulnerability scanning – in house or third party?* Retrieved from AT&T - Cybersecurity: https://cybersecurity.att.com/blogs/security-essentials/vulnerability-scanning-in-house-or-third-party

Hayes, K. A. (n.d.). *What is Incident Detection and Response?* Retrieved from Rapid7 Blog: https://blog.rapid7.com/2016/03/29/what-is-incident-detection-and-response/

Manoske, A. (n.d.). *Addressing Top Security Threats with Vault*. Retrieved from HashiCorp: https://www.hashicorp.com/blog/addressing-top-security-threats-with-vault/

Rivera, A. (n.d.). *Phish Your Own Business to Expose Vulnerabilities*. Retrieved from Business News Daily: https://www.businessnewsdaily.com/10940-phish-your-own-business.html

Shivpuriya, V. (n.d.). *Cloud Native*. Retrieved from InfoWorld: https://www.infoworld.com/article/3203265/security-in-a-cloud-native-environment.html