🧰 Post-Breach Automation Strategy with Red Hat Ansible

Company: Bank of Ontario
Title: Automation-Driven Cybersecurity Remediation Using Red Hat Ansible
Date Published: June 3, 2025
Author: Leila Farhani, Cyber Automation Lead
Reviewed By: Ravi Khurana (IR), Amira Dosanjh (VP CyberOps), Deloitte Canada

---

1. Executive Summary

Following the critical security incident **BOO-SEC-2025-0587** on May 23, 2025, **Bank of Ontario** accelerated the adoption of **Red Hat Ansible Automation Platform** to eliminate human error, reduce response time, and proactively contain similar threats in the future.

By codifying security playbooks and integrating with **Cisco SecureX**, **Cisco AMP**, and **SIEM systems**, Ansible enabled end-to-end **incident response**, **host quarantine**, and **network isolation workflows**, delivering measurable **operational efficiency and cost savings**.

---

2. Use Cases Implemented with Ansible

🔒 2.1 Automated Host Quarantine

- **Trigger**: High-severity SecureX alert (e.g., impossible travel, malware beacon)
- **Playbook Actions**:
    - Connect to Cisco Secure Endpoint (AMP)
    - Isolate host from internal VLAN
    - Notify SOC via Microsoft Teams + Email

yaml
CopyEdit

```
- name: Quarantine endpoint via Cisco AMP
  hosts: localhost
  tasks:
    - name: Trigger AMP isolation API
      uri:
        url: "https://amp.api.cisco.com/v1/computers/{{ hostname
}}/isolate"
        method: POST
        headers:
          Authorization: "Bearer {{ amp_token }}"
        status_code: 204
```

🔐 2.2 VPN Access Revocation

- **Trigger**: Detection of credential misuse or credential reuse from breached accounts
- **Playbook Actions**:
    - Disable affected user's VPN access via LDAP
    - Rotate password and revoke tokens
    - Update ServiceNow ticket with reference logs

🌐 2.3 TOR Exit Node Blackhole

- **Trigger**: IP reputation flag from Cisco Umbrella or Talos
- **Playbook Actions**:
    - Pull Tor exit node list from open-source Intel feed
    - Update firewall (Cisco FTD or Palo Alto) dynamic blocklist object
    - Log update in Splunk with change control

🧠 2.4 Threat Simulation & Drills

- Orchestrated phishing simulation every 30 days
- DR tabletop scenarios kicked off quarterly via Ansible Playbooks calling Microsoft 365 calendar APIs

---

3. Platform Integration Architecture

sql
CopyEdit

```
[ Cisco SecureX ] ---> [ Ansible Tower API Trigger ]
          |
          +--> [ Ansible Automation Hub ]
                  |
                  +--> [ Endpoint Isolation ]
                  +--> [ VPN Deactivation ]
                  +--> [ Network ACL Updates ]
                  +--> [ SIEM Ticket & Notification ]
```

- **Identity & Secrets Management**: Integrated with HashiCorp Vault
- **Approval Flows**: SOC manager must approve via Ansible Tower UI for privileged actions
- **Audit Trail**: Logged into Splunk via Ansible callback plugins

---

4. Operational Benefits

Benefit	Before Ansible	After Ansible	Improvement
Mean Time to Contain (MTTC)	4.5 hours	22 minutes	**88% faster**

Human touchpoints	~6 analysts	1 analyst + review	**85% fewer manual steps**
VPN Lockdowns	45–60 min	6 min	**~10x faster**
Firewall ACL updates	90 min	12 min	**86% faster**

---

5. Cost Savings Estimate

Category	Estimated Savings (Annualized)
Analyst time (automation of 1,500 IR tasks/year)	**CAD $110,000**
Reduced breach containment overhead	**CAD $65,000**
Fewer false positives escalated to Deloitte IR retainer (5 fewer per year)	**CAD $27,000**
Incident downtime prevention (20h saved)	**CAD $35,000**
Total Estimated Savings	**~CAD $237,000/year**

---

6. Key Lessons & Recommendations

✅ What Worked

- Red Hat Ansible Tower was easy to integrate with Cisco XDR, AMP, and ServiceNow
- Event-driven automation reduced response latency significantly
- Role-based access control helped avoid privilege abuse in automated workflows

🔄 Future Enhancements

- Add **SOAR-style ChatOps workflows** via Slack bots for real-time approvals
- Move all playbooks to **GitOps workflow with version control**
- Expand automation to patching, rollback, and postmortem publishing

---

7. Governance & Ownership

Role	Owner
Platform Admin	CyberSec Automation Team
Playbook Developers	Red Hat + Internal DevSecOps
Policy Oversight	Security Governance Committee
Integration Partners	Cisco Services & Deloitte Advisory

---

8. Conclusion

Red Hat Ansible enabled **Bank of Ontario** to move from reactive, analyst-driven remediation to **proactive, automated security response**. The investment is projected to **pay for itself in less than 8 months**, while delivering faster threat containment, reduced risk exposure, and consistent enforcement of cybersecurity policies.