ANALYTICA42

DATASHEET

Devo Use Case Development

DEVO

Are you making full use of Devo?

Devo's logging and analytics capabilities are only one piece of the security puzzle. Unless you're mapping those alerts to a framework (like the MITRE ATT&CK framework), you're just seeing noise—you don't know what's important or how to tune your security protocols.

Companies with a mature threat detection capability go way beyond automated alerts to customize CTI according to environment and goals, and cusomize bahvioral patterns, fine tuning the results to improve decision making. So, how mature is your threat detection?

only 20%

of security operations practitioners describe their organizations as having a mature security practice

Source: https://www.siemplify.co/resources/the-road-to-security-operations-maturity-a-cyentia-research-report/

Use cases raise your security maturity.

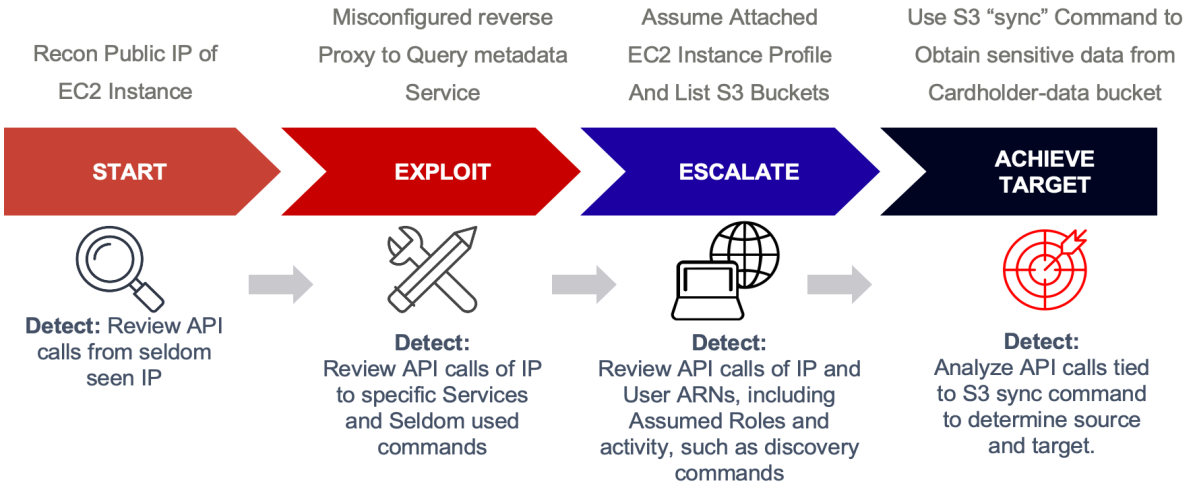
Analytica42 can develop use cases, from definition through implementation and validation, based on your environment and known top vectors of compromise. For example, AWS Use Cases mapping:

- Configuration change activity
- User investigations
- Anomalies and errors
- IAM, S3, EC2, Key pair activity

to the MITRE ATT&CK framework of:

- Initial access
- Execution
- Persistence
- Priviledge escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Collection
- C&C
- Exfiltration
- Impact

Breach Use Case



Use Case Services

Devo Content Support may include, but is not limited to:

- Use Case Workshop(s) / Kick off meeting to review and discuss Devo Detections, define Use Case Roadmap
- Use Case Prioritization and Feasibility Analysis
- Use Case Devo Content Research & Development
- Use Case Deployment, QA, and Tuning
- Use Case Documentation
- Devo Parser Development
- Use Case Workflow Management Best Practices

A Certified Services Partner

- Devo Installation/Configuration
- Data ETL Services
- Data Analytics
- Education Services
- 3rd-Party Integrations
- Devo Threat Hunt Services

Our approach

We begin with an analysis of industry best practices including common methods of exploitation and existing attacks. Then we build rules tied to a framework, adding context and tuning. Those rules feed the alert automation management capability. Finally, we build the investigative capability to provide alert triage, general situational awareness, and threat hunting, and validate the results. Contact us to find out how we can increase your organization's security maturity through Use Case development.

Example A42 Content Packages coverage:

- Cloud (AWS, GCP, Azure, O365)
- OS (Windows, Linux, Mac)
- Network (Firewall, DHCP, Flow)
- EndPoint (CrowdStrike, Sysmon)
- Application (Web, Custom)
- Auth (SSO, Okta)
- CTI Analysis and much more
- Tailored/Customized Content