CyberProof®
A UST Company

Cyberproof use case management service

cyberproof.com

The Use Case Management service provides your organization with a means to identify, develop, and deploy use cases to achieve rapid threat detection and effective incident response automation.

To help solve these challenges, CyberProof has partnered with Microsoft to provide cloud-scalable security monitoring, threat detection, and response services across your IT estate.

Identify and fill threat detection gaps

With 84% of MITRE tactics and techniques missing in the SIEM, according to recent research (CardinalOps, 2021), how can you ensure coverage? CyberProof baselines your threat landscape and existing coverage to prioritize use cases and create relevant detection rules. In return, the quality of alerts generated by your security analytics platforms improve since only approved use case alerts are generated.

Continuous Improvement

CyberProof's team of engineers and developers identify and fill gaps in detection and response while continuously developing and deploying content aligned to threat use cases. Our unique Use Case Factory uses Agile principles for the ongoing development of kits, containing detection rules, corresponding incident response playbooks and third-party API integrations to achieve incident response automation.

Improve each stage of the SOC workflow

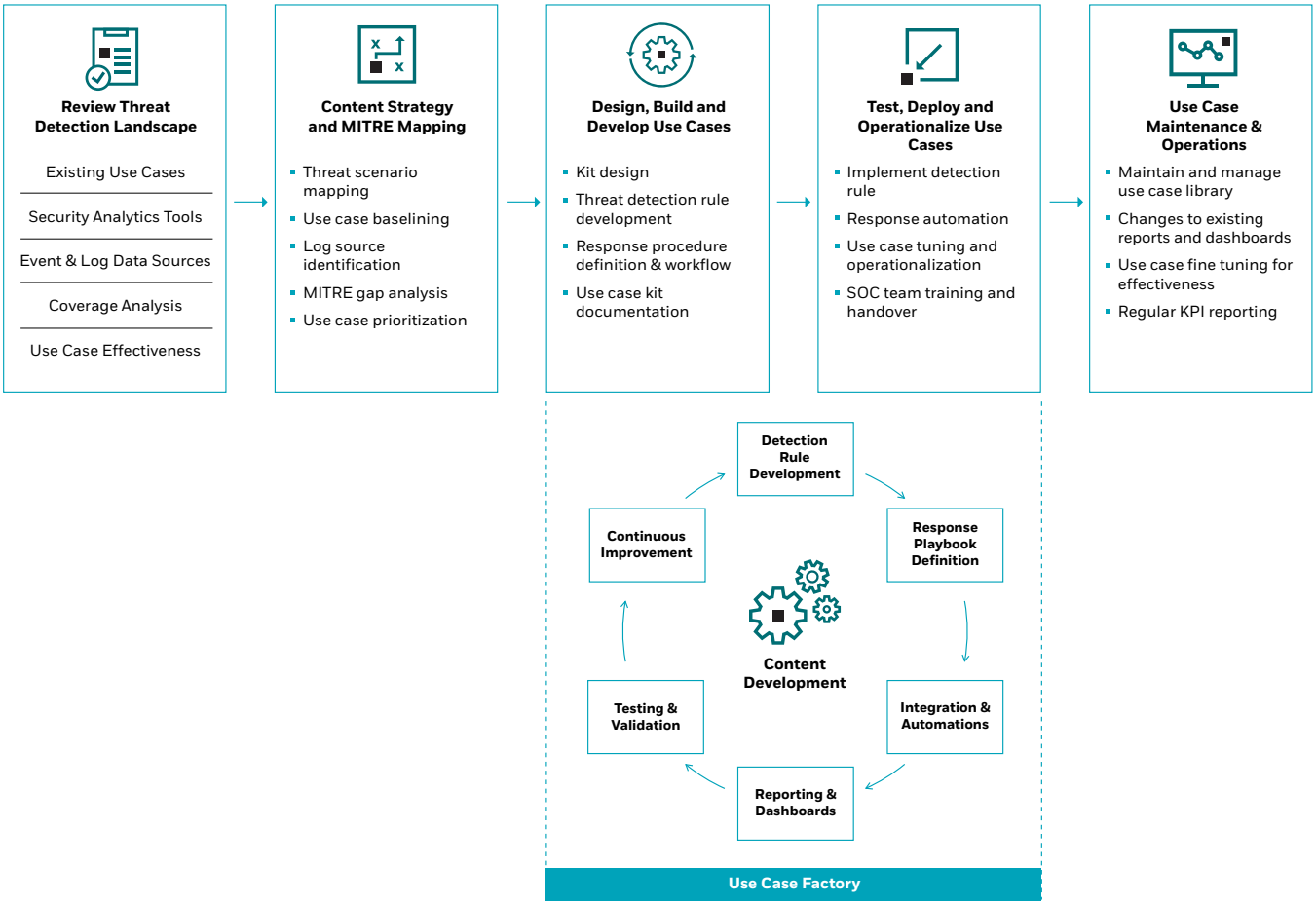
Improve the efficiency and effectiveness of each stage of the SOC workflow – from alert triage, investigation and threat hunting to incident response and remediation. CyberProof's use case kits are available in a central repository where the use cases are organized by various filters such as MITRE tactics, attack type, sector, and more.

WHAT'S INCLUDED?

- Closed a deal that was much broader than the initial discussions with Incora had indicated
- Baselining threat detection & response capabilities
- Use case management and operational governance
- Development of new content packages following Agile development best practices
- Continuous improvement of detection rules and response playbooks
- View of the use case life cycle, and alignment to the MITRE ATT&CK framework
- Use case forums that review content strategy and the use case roadmap
- Regular KPI reporting, providing coverage analysis & a pipeline view
- Improvement of SOC workflows to ensure visibility of existing and evolving threats

How the service is delivered

The Use Case Management Service uses a unique, risk-driven methodology that leads to operational efficiency. It provides organizations with a repeatable and agile process - with clear governance to continuously improve threat detection and response in line with their unique threat landscape.Microsoft to provide cloud-scalable security monitoring, threat detection, and response services across your IT estate.



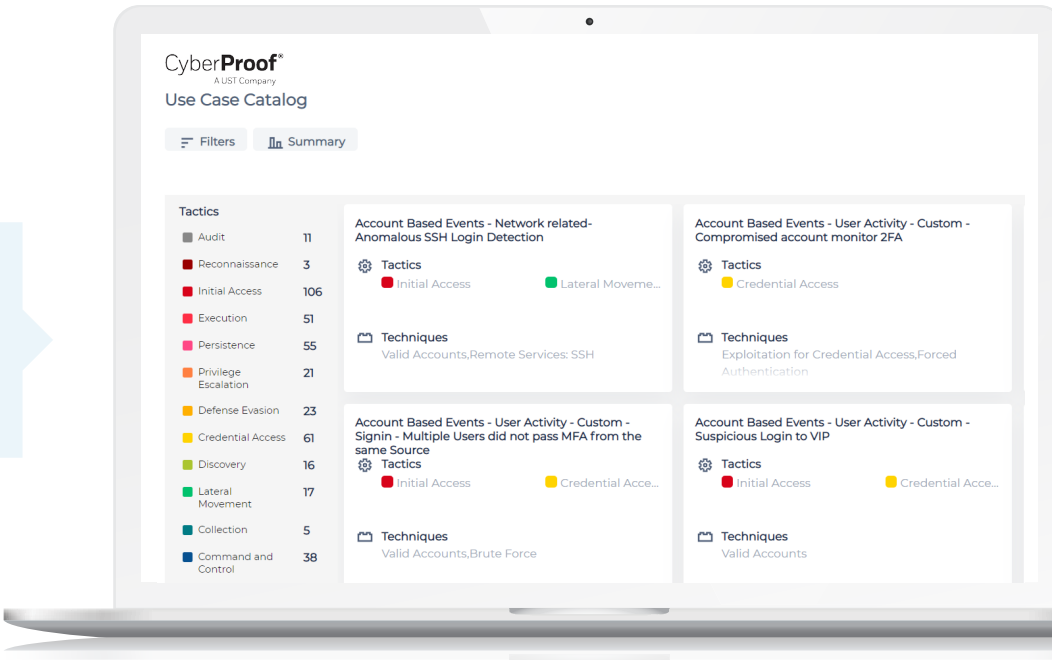
Use Case Factory

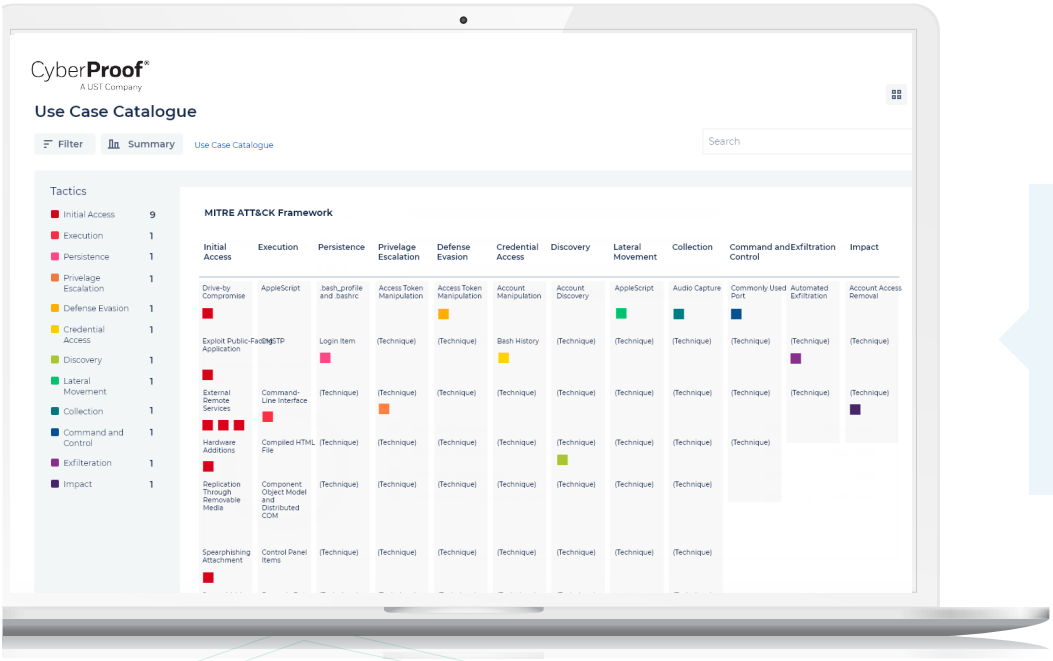
A dedicated team of engineers and developers use an award-winning model based on Agile principles, for the ongoing development, testing and deployment of kits. Each kit can contain:

- Detection Rules
- Response Playbooks
- Third-party API integrations for automation

Use Case Catalog

The catalog is a central repository with use cases grouped under MITRE tactics & techniques. New use cases are continuously added based on cyber threat trends.





You can easily select use cases based on MITRE capability gaps. Kits include detection rules & corresponding incident response playbooks. Custom use cases can be requested per your tech ecosystem & risk profile.

Why CyberProof

Dedicated team of use case engineers and developers, who help identify and fill threat detection and response gaps

Exhaustive list of pre-defined kits designed, built, tested and operationalized across our client base, which can be leveraged by new clients to rapidly onboard Use Cases

Our award-winning Use Case Management service won in the subcategory of "Top 10 Baby Black Unicorns"

Rated a Leader by Forrester and ISG in Managed Security Services market in 2018, 2020 and 2021

Client Case Study

Company profile

- Food and consumer goods industry
- Large company with multiple subsidiaries
- Operates worldwide

The challenge

The security team was monitoring multiple security analytics technologies, with numerous use cases deployed, that weren't demonstrating their value. They also sought to improve their threat detection coverage, and were unable to map use cases against the MITRE ATT&CK framework to ensure the right tools and enrichments were implemented for their business.

The Solution

Our Use Case Management service provided the client with a risk-driven, agile and standardized methodology for defining use cases and prioritizing the development and optimization of relevant detection and response content.

The service included:

- Assessment of existing threat detection landscape
- Content strategy & MITRE mapping
- Design, build and development of use cases
- Testing and deployment of use case kits
- Use case maintenance and operations

Benefits

- Ability to continuously tune their use cases in a sustainable way across multiple SIEMs
- Ability to prioritize and develop new use cases in an agile manner based on risk and their unique threat landscape
- Significantly reduced security team alert fatigue

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations.

For more information, visit www.cyberproof.com

Locations
Barcelona | California | London | Singapore | Tel Aviv | Trivandrum