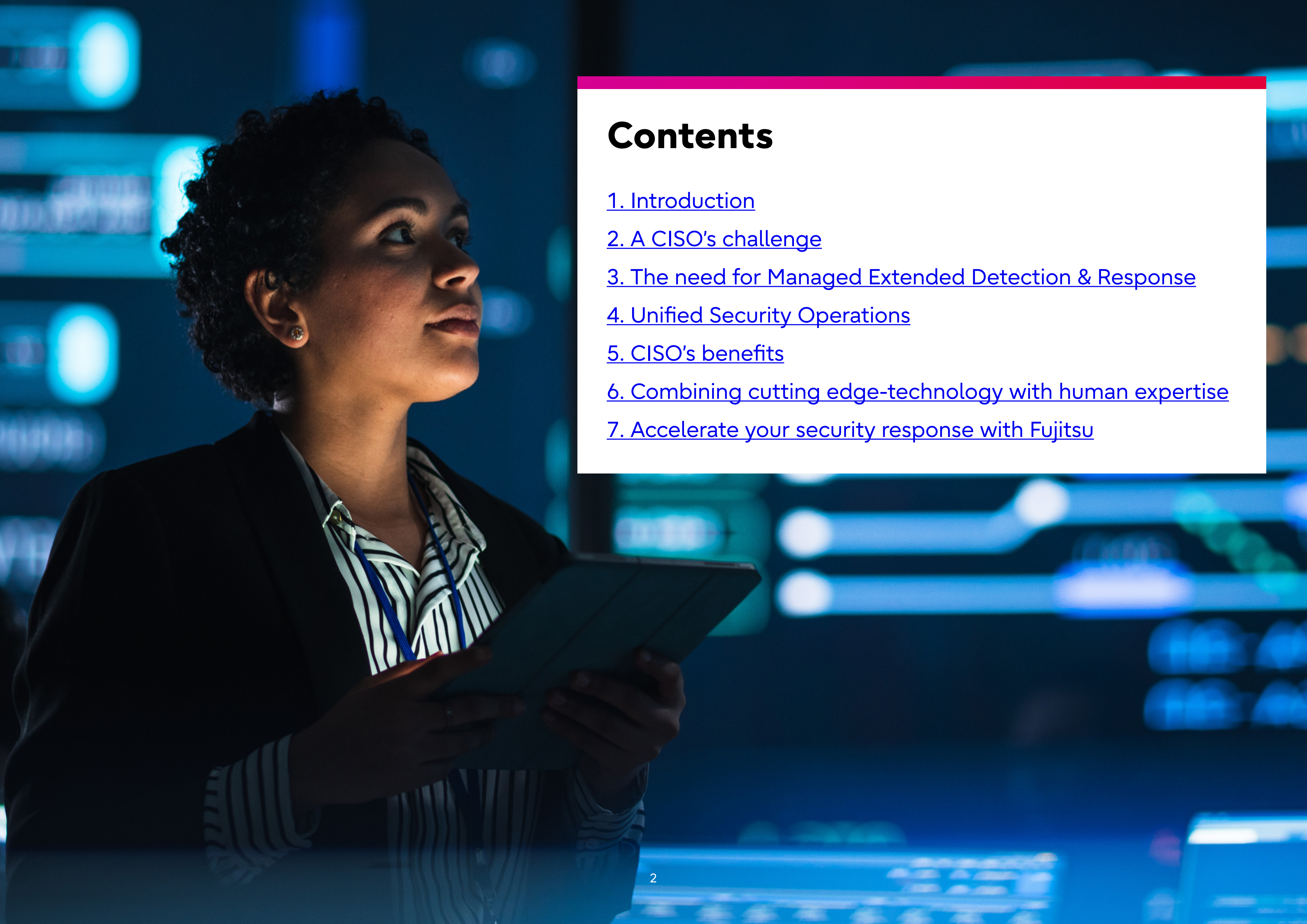
Managed Extended Detection and Response (MXDR)

Accelerating security response and mitigating business risks with Fujitsu

Solution guide



Contents

> *“Security leaders are increasingly cognizant that reducing the time to detect a threat is meaningless without a corresponding reduction in the time to respond to a threat to enable a return to a known good state.”*
>
> Gartner Research Market Guide for Managed Detection and Response Services

1. Introduction

The threat landscape continues to grow in velocity and complexity. Organizations are navigating a landscape fraught with security threats, including sophisticated phishing attempts, ransomware and frequent exploitation of application and network vulnerabilities. These threats pose significant risk to the daily operation of businesses and present formidable challenges that must be addressed to not only detect but adequately respond.

For any business, effectively managing and responding to these threats is crucial. Without a centralized and dynamic approach to handling these security challenges, the capacity to prevent breaches across the digital enterprise is markedly diminished.

Many organizations are seeking a way to alleviate the burden on internal IT and cyber support functions, whilst ensuring a resilient and secure environment in today’s ever-evolving threat landscape.

2. A CISO's challenge

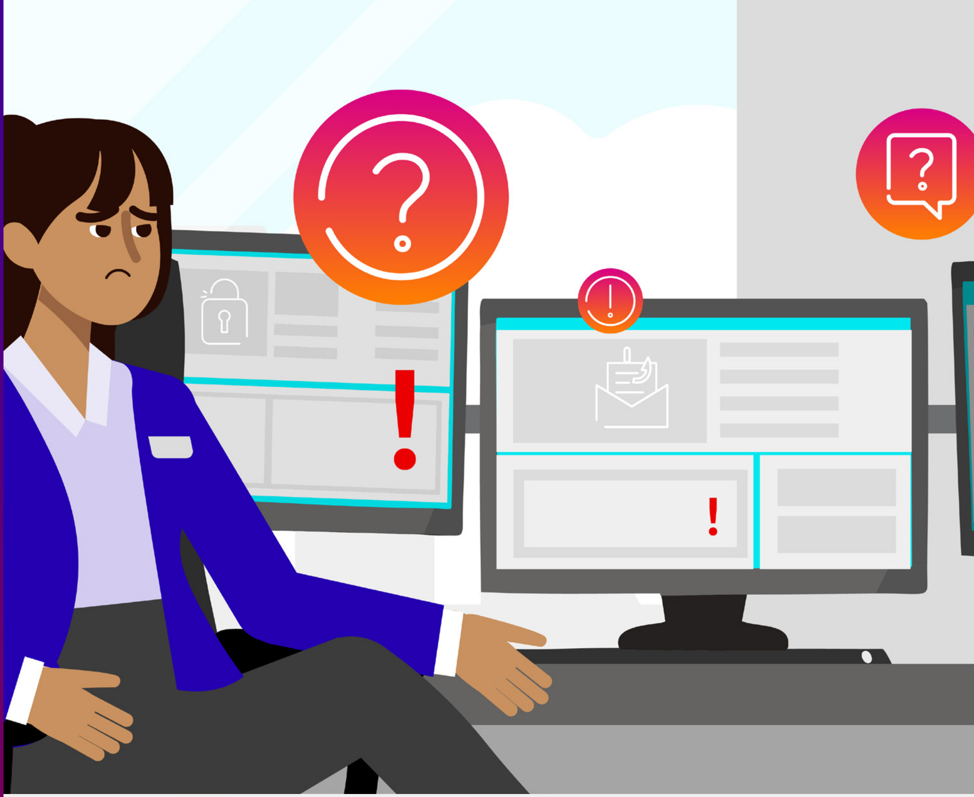
Imagine a Chief Information Security Officer (CISO) with a mission – protecting the organization from the ever-present dangers of cyber attacks.

The burden of a CISO

The job of a CISO is a fine balancing act of managing risk and resources, often with budget constraints. The CISO and Security Operations team are inundated with alerts from many separate tools making it challenging to identify and respond to true positives. There is an abundance of manual tasks, daily checks and a requirement to manage multiple and disparate security tools. As such, the stakes are high – any oversight could lead to breaches, significant regulatory fines with unwanted exposure and reputational damage.

Where the CISO stands

- Past security incidents linger as stark reminders of the potential consequences of a breach.
- Alarm fatigue is a daily reality, with an overwhelming volume of security events to handle.
- Ensuring technologies are properly configured, maintained, and patched is a continuous task, vital for security integrity and to maximize the ROI on technology spend.
- Tuning and configuring rules to counter sophisticated threats require expertise which is hard to come by.
- Monitoring security alerts 24/7 is a continual effort, but another huge challenge is how to respond effectively and in a timely manner.



A new dawn

Resources drained by ineffective incident triage and false positives should be a thing of the past. A CISO needs a real-time and unified view of all their alerts and incidents across the organization's entire security landscape. One platform that gives visibility across your entire network, endpoints, and cloud environments increases detection efficiency and response coordination. Threat enrichment ensures they can zoom in, respond and mitigate genuine threats. A CISO needs confidence their approach will maintain pace with the evolving threat landscape. This ensures the organization can operate safely and securely with a threat response strategy that adapts and responds just as quickly as the threats it's designed to counter.

Meet Jane, a CISO mastering cyber security challenges

Watch this video to discover how Fujitsu MXDR service transforms her team's efficiency with automated, cutting-edge technology.

Click the link below to watch the video.
youtube.com/watch?v=x2Nlp-96GYY

3. The need for Managed Extended Detection and Response

Managed Detection and Response (MDR) extends beyond traditional and disparate security services such as Security Information and Events Management (SIEM). Managed Extended Detection and Response (MDXR) builds on SIEM and offers comprehensive platform management and incident analysis across Microsoft Sentinel and all Microsoft Defender XDR applications. This enables CISO's to have a unified view of their security posture, supporting compliance with requirements like NIS2, and ensuring rapid response to threats.

Sending logs to a SIEM platform and waiting for alarms to fire is simply no longer fit for purpose. There is a need for proactive threat management. Rules must be created dynamically with high fidelity to detect the latest threats. Data must be enriched and tagged with up-to-date threat intelligence and where possible responses must be handled as efficiently as possible with elements of automation frameworks like MITRE ATT&CK are also increasingly important to assist in identifying the type of attack and technique being used. Correlating this across other security events allows for a holistic and enriched analytical view. MXDR will help you accomplish this challenging task.

By leveraging the right technology alongside the expertise of our Global Security Operations Centers (SOCs) - staffed by 600 skilled security practitioners worldwide - we actively monitor and respond to security incidents. User and Entity Behavior Analytics (UEBA) and proactive Threat Hunting are key service components which empower our SOC analysts to investigate anomalous events and investigate threats. Security Orchestration, Automation and Response (SOAR) and Automated Investigation and Response (AIR) can be used to reduce the number of incidents handled by our analysts, focusing on critical issues before they can impact your organization.

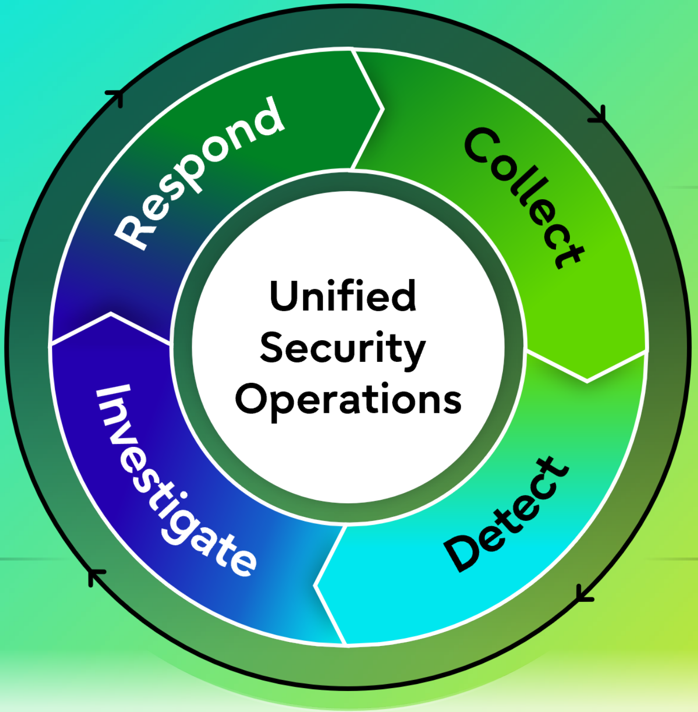
A CISO should adopt a comprehensive approach to security by integrating various detection tools and technologies, effectively minimizing the risk of security breaches and ensuring robust, optimal protection.

Key capabilities

- Threat intelligence for real-time insights
- Threat hunting to proactively uncover hidden risks
- Detection engineering for dynamic, precise and actionable alerts
- Automated responses to neutralize threats at speed

4. Unified Security Operations

Our MXDR service provides a unified approach to Security Operations through a single interface, offering a comprehensive view of alerts and incidents across Microsoft XDR, Sentinel, and all Defender applications (Defender for Endpoint, Defender for Identity, Defender for Office 365 and Defender for Cloud Apps). By consolidating Microsoft security technologies into one platform, we simplify deployment, streamline threat detection, and strengthen response capabilities. This improves key performance metrics like Mean Time to Respond (MTTR) and Mean Time to Close (MTTC). Your organization can gain the advantages of vendor consolidation while reducing complexity and continuously refining monitoring and outcomes.



Improved Incident Response for Computer Security Incident Response Team (CSIRT) and ability to Automate Investigation and Response (AIR).

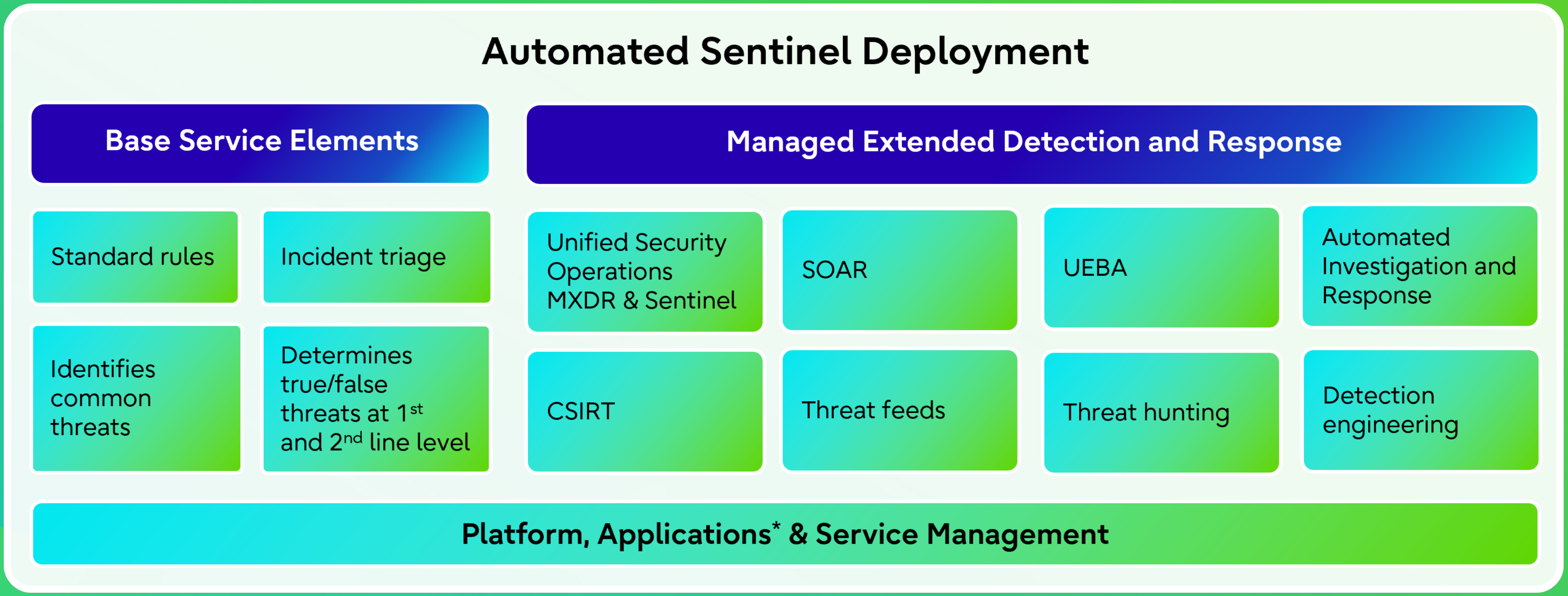
Collection of all security telemetry into a single platform.

Single interface for enrichment and context enables deep analysis for incidents and proactively hunt threats.

Dynamic environment for detection engineering for precise and actionable alerts.

A consolidated view of all incidents and alerts across Microsoft XDR, Sentinel and all Defender applications.

Fujitsu Uvance MXDR service



Automated Sentinel Deployment

Base Service Elements

- Standard rules
- Incident triage
- Identifies common threats
- Determines true/false threats at 1st and 2nd line level

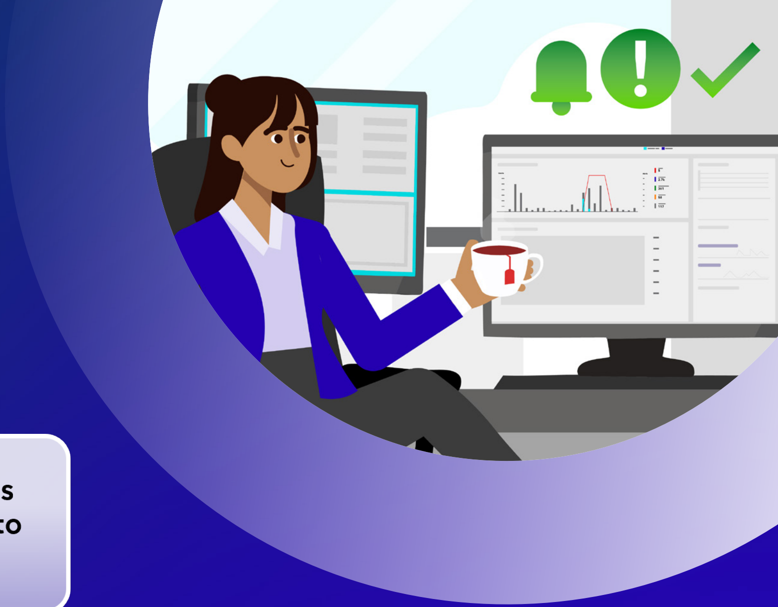
Managed Extended Detection and Response

- Unified Security Operations MXDR & Sentinel
- SOAR
- UEBA
- Automated Investigation and Response
- CSIRT
- Threat feeds
- Threat hunting
- Detection engineering

Platform, Applications* & Service Management

*Applications include Microsoft XDR, Sentinel, Defender for Endpoint, Defender for Identity, Defender for Cloud Apps and Defender for O365.

5. CISO's benefits



Key customer benefits of Fujitsu MXDR service:

Increased visibility	Comprehensive and unified view of all security alerts and incidents across your entire network, endpoints, and cloud environments into one platform.
Proactive threat management	Continuous protection and improvement by embedding Threat Hunting and User and Entity Behavior Analytics (UEBA) into our service to proactively look for the latest threats and evaluate anomalous events.
Faster detection	Combining Fujitsu's global cyber security experts monitoring the service 24/7 with advanced rules and policies, you are quickly informed of critical issues which need attention before they cause significant impact.
Enhanced response	Automated investigation response and containment activities allow for quick actions to be taken against identified threats, minimizing potential impact and restoring normal operations as quickly as possible.

Our MXDR service combines end to end platform management for Microsoft XDR, Sentinel and all Defender applications with alert triage and response. Your organization benefits from less time spent in the trenches of cyber defense and more time driving business value, growth, and innovation.

6. Combing cutting-edge technology with human expertise

This is why organizations before you have chosen for Fujitsu:

Fujitsu stands out by offering global expertise across security services. Our strategic partnerships across academia, public and private sectors ensure we stay at the forefront of industry demands.

Global reach with a local touch

Our extensive network of Global Security Operations Centers (SOCs) is complimented by local expertise. Ensuring that expert assistance is readily available no matter your location, we deliver standardized services with predictable costs. We provide you with the expertise you need, exactly when and where you need it.

Seamless technological integration

Fujitsu has a long-standing partnership with world-class security technology partners including Microsoft and others.

Sustainability at the forefront

Our commitment to sustainability is woven into the fabric of our services. We prioritize eco-friendly practices in our service delivery, reflecting our dedication to not just securing digital assets but also preserving our planet.

7. Accelerate your security response with Fujitsu

Are you facing cyber security challenges that seem insurmountable? Whether you're grappling with the complexities of threat detection, streamlining your incident response or if you want to consolidate security technologies to maximize your investment, Fujitsu is here to elevate your security strategy while helping you mitigate business risks.

Connect with Fujitsu today to discover how our global expertise, cutting-edge solutions and dedicated teams can contribute to your cyber security success.

Visit us at fujitsu.com/global/mxdr