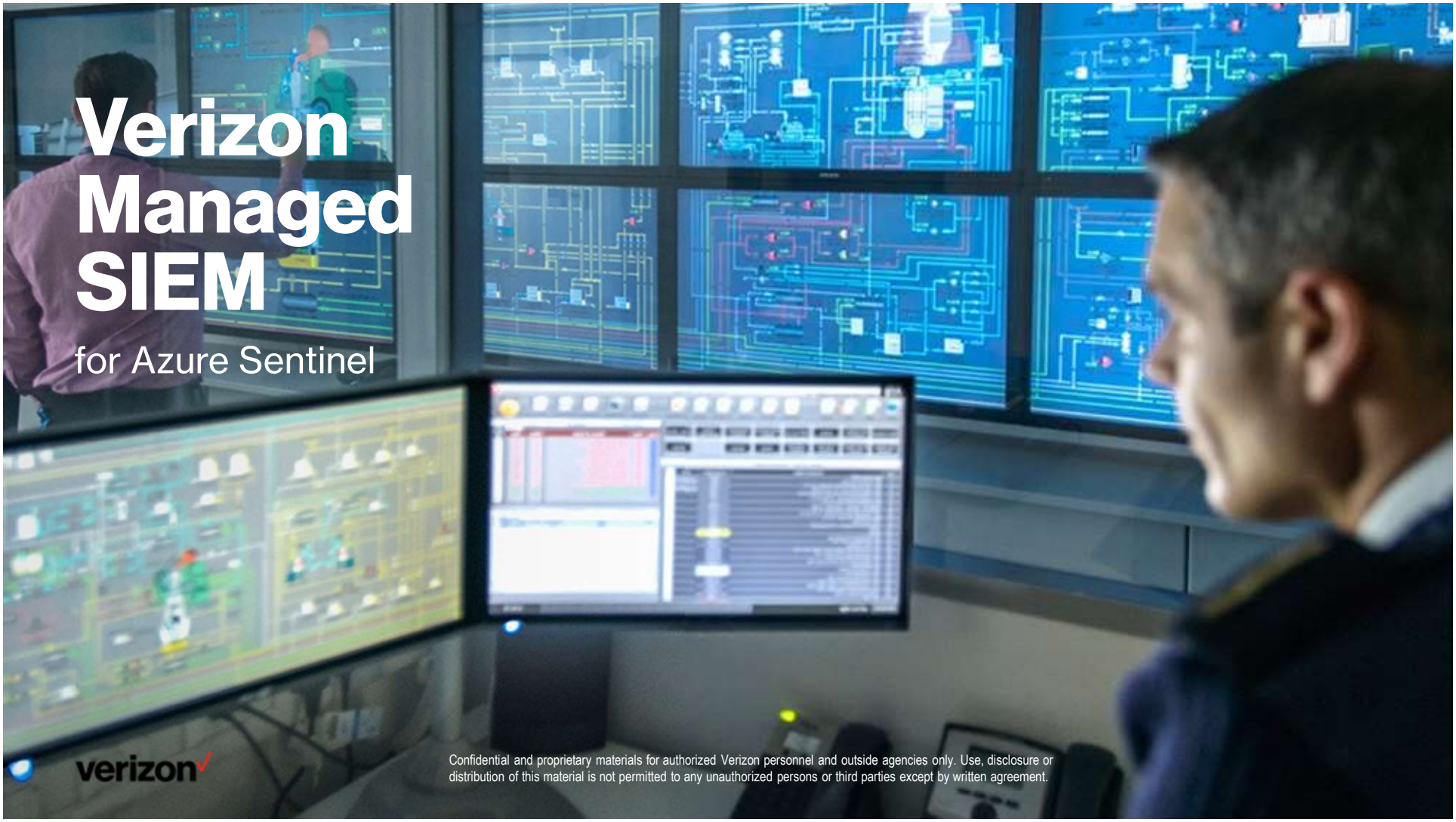

Verizon
Managed
SIEM
for Azure Sentinel
verizon
Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

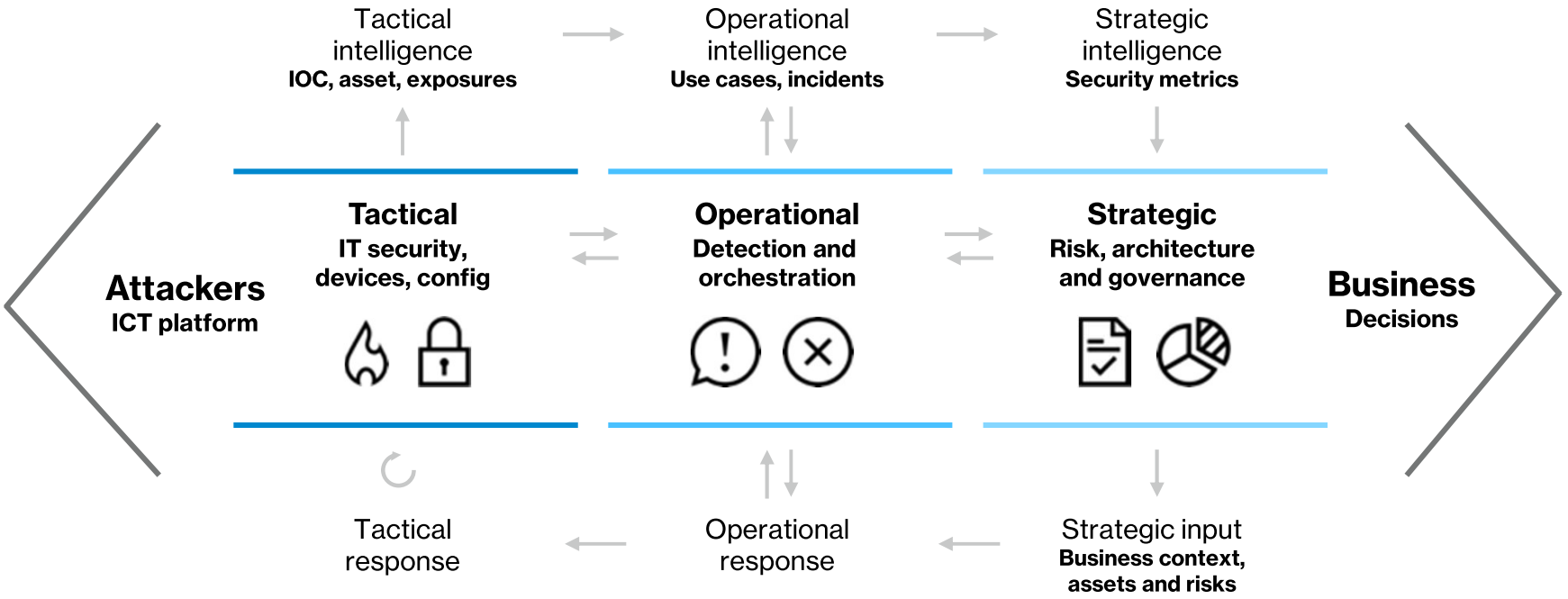
Proprietary statement.

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

How can you close the cyber-defense gap?

It takes orchestration, detection and response.



Verizon Managed SIEM: Put our cybersecurity assets to work for you.

Shared or dedicated seasoned analysts

- Exceptional people using proven tools/techniques
- 24x7x365 monitoring
- Tiered analysis before escalation to customer

Multi-platform support and expertise

- We manage the Azure Sentinel SIEM platform for you
- Analysts connect remotely, securely
- Expertise in all leading SIEM platforms

Keeping your detection up to date

- Collaborative use case alignment during onboarding phase
- Ongoing tuning to help reduce false positives for better alerts
- Adjustment of alerting thresholds as part of the process
- Actionable reports and clear SLAs

Designed to scale (flexible)

- Flexible service consumption-based pricing
- Resources can be added as customer expands data collection and logging

verizon

Verizon Managed SIEM.

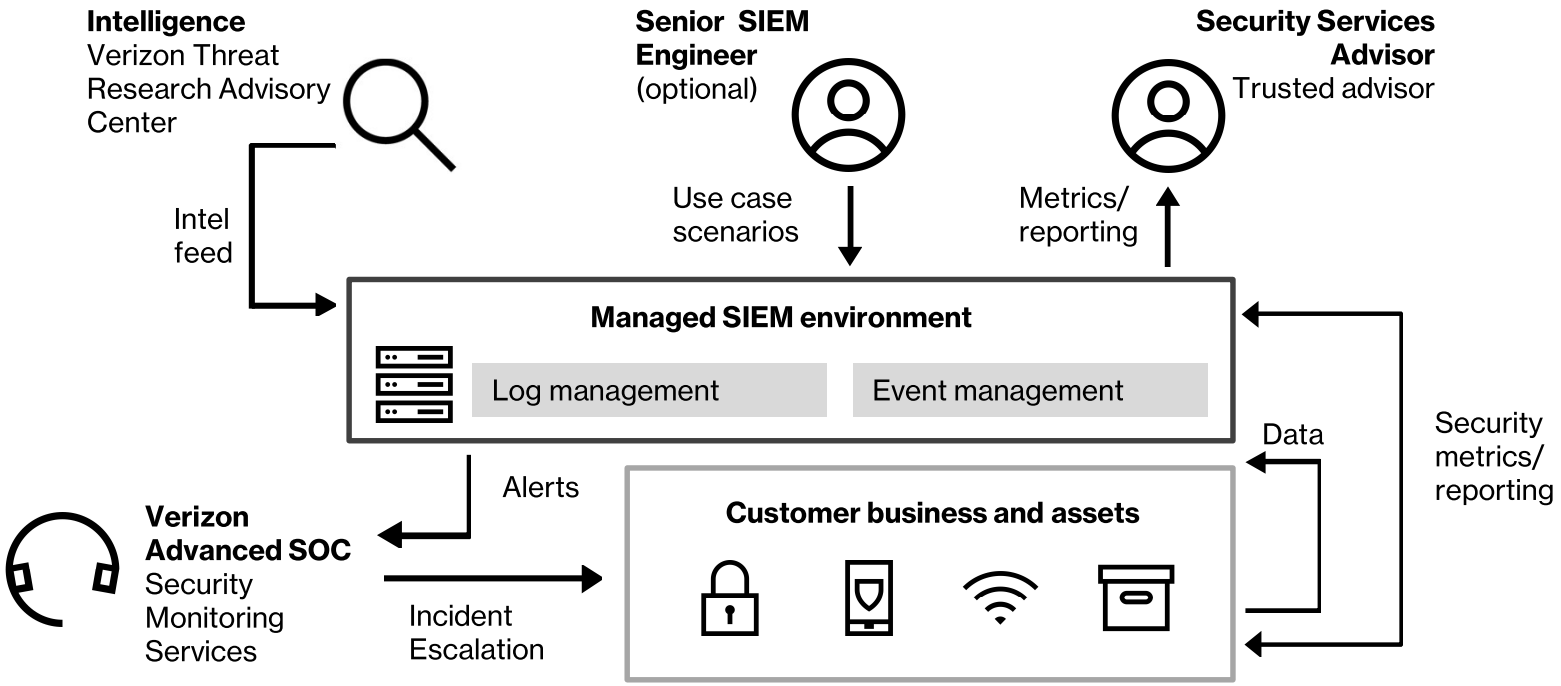
Our comprehensive Managed Security Service for customers that:

- Have purchased Azure Sentinel or selected it as a SIEM technology partner
- Need a partner to support them in implementing and monitoring Azure Sentinel
- Require a dedicated solution for log collection, correlation and security event escalation

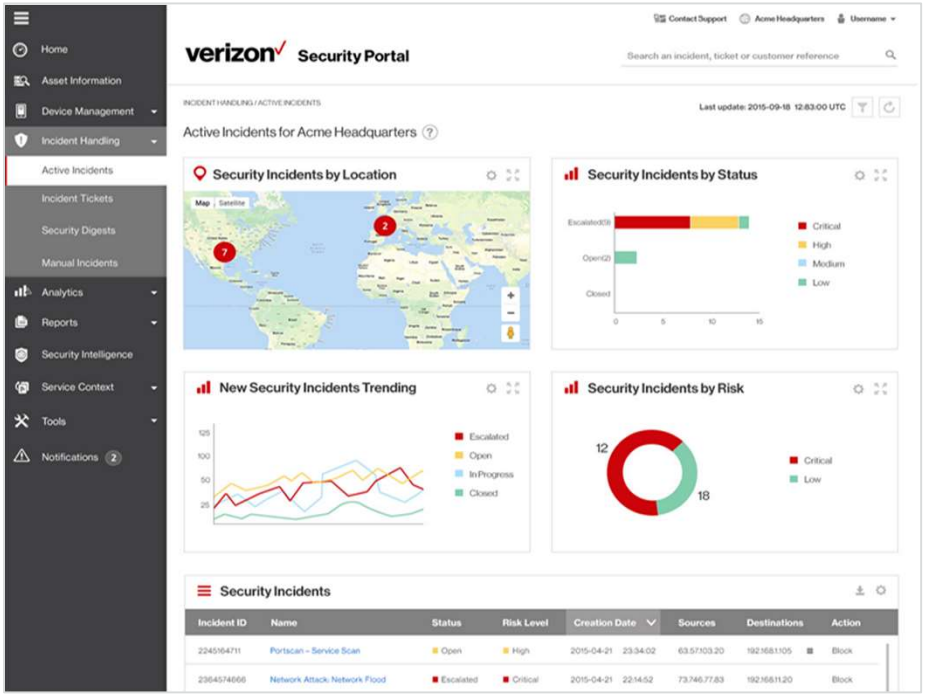
Features include:

- Upfront implementation and/or tuning services for Azure Sentinel based on standard Verizon rule sets
- In region located 24x7 security operations centers for continuous security monitoring
- Regular rule-set maintenance in line with emerging threats and changing threat landscapes
- Access to specialist service and engineering resources throughout the lifecycle of the service

Verizon Managed SIEM: Process flow.

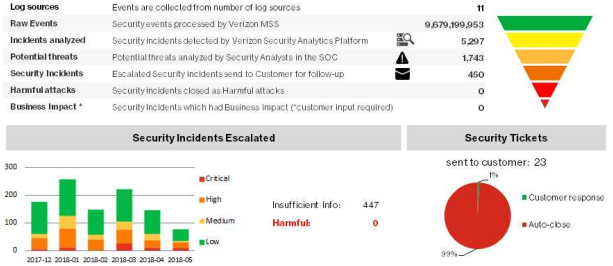


Verizon Managed SIEM: Monitoring and reporting.



Quarterly Service Review (QSR)

Cyber Threat Dashboard



Verizon Managed SIEM: Summary.

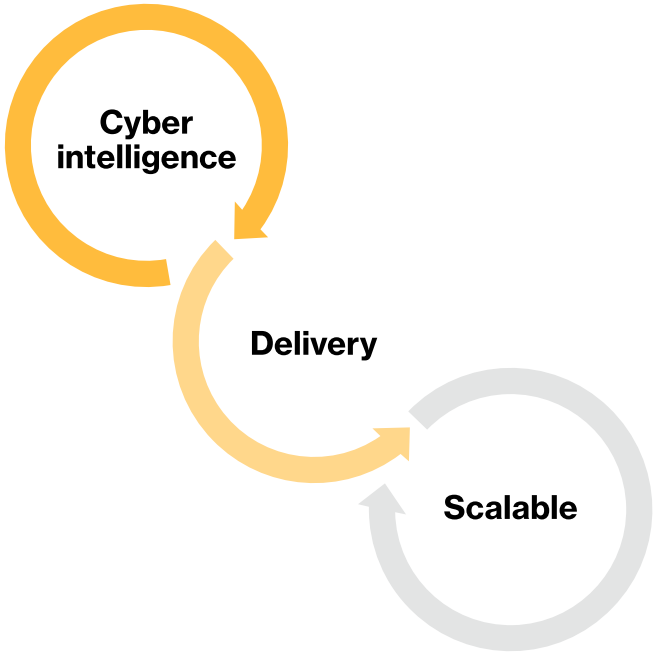
Integrated operational model that leverages both customer and Verizon security and intelligence capabilities.

Tailored solution that grows with the customer, including a ramp up process to align with capabilities as each is implemented and integrated.

Shared Verizon SOC (24x7) in region leveraging existing facilities and mature operational experience.

verizon

Why partner with Verizon?



1. Intelligence: Verizon's tactical and applied intelligence
2. Solution: Tailored solution and consumption-based resourcing model
3. People and processes: Designated and dedicated in region security professional service expertise and resources
4. Reputation/execution: Strong record in all aspects of designing, building and operating SOCs
5. Innovate: Continuous improvement to ensure the delivery of best-in-class cybersecurity services
6. Integrated operational model: Combines customer's IT landscape and business goals with Verizon's intelligence and expertise
7. Partnership: Verizon Managed SIEM is a natural extension of customers' security organization

Thank you.

Managed SIEM: Customer Success Stories.

verizon

Credit union banks on Verizon's network monitoring.

Challenges

- Customer lacked SIEM content development expertise
- Lack of trained SOC and Incident Response Team

Solutions

- Managed SIEM and advanced behavioral analysis platform
- Critical SOC expertise and analyst support

Benefits

- Customized phishing detection use case provided last line of defense for threats reaching the end user
- Behavior Analysis analytics enriched existing use cases
- Leveraged decades of VZ experience

230GB	20B	2,500
Daily Log Volume	Monthly Events	Annual Incidents

verizon

Home security company trusts Verizon with their security.

Challenges

- Required ability to detect and respond to insider threats
- Lack of SIEM engineering capability
- No incident response or SOC teams

Solutions

- Developed Managed SIEM log analysis and SOC monitoring capability
- Implemented Cyber Security Incident Response Team (CSIRT) in order to effectively respond to detected incidents

Benefits

- Provided visibility into cloud-related security incidents
- Enabled behavioral analysis capabilities
- Incident response capability realized

270GB	16B	3,500
Daily Log Volume	Monthly Events	Annual Incidents

verizon