Verizon Security Operations Service

A standardized approach to customizable security operations

Cybersecurity challenges: Increasing protect surface

As organizations are generating more data than ever and with the ever-increasing ecosystem they need to protect, organizations struggle to keep up with cyber adversaries. While important data is stored in the cloud, on network assets and across a myriad of devices, the critical ecosystem expands to valuable assets, applications and services.

This broadens the scope of what must be safeguarded. The ZeroTrust framework defines the sum of this as the 'protect surface' - which comprises critical data, assets, applications, and services. Organizations can't do this on their own. They often require ongoing support to protect their mission-critical protect surface, ensuring that their desired security posture and acceptable risk levels are addressed.

Data breach research: Attackers are as active as ever

Leading market research like Verizon's 2024 Data Breach Investigations Report suggests that attackers are not sitting still. On the contrary, the attack surface is expanding because Verizon is seeing both new and innovative attacks as well as variations on tried-and-true attacks that still remain successful. From the exploitation of well-known and far-reaching zero-day vulnerabilities, such as the one that affected MOVEit, to the much more mundane but still incredibly effective ransomware, use of stolen credentials and Denial of Service (DoS) attacks, criminals continue to do their utmost to prove the old adage "crime does not pay" wrong.

180% 180% growth (as compared against the previous year) in exploitation of vulnerabilities as the initial access step for a breach.

35% 35% of all breaches are system intrusions (most across all breach patterns).

70% 70% of system intrusion incidents involved ransomware.

Source: 2024 Verizon Data Breach Investigations Report

Both the expanding protect surface and evolving threat landscape fundamentally change the cybersecurity requirements of organizations. Monitoring the security compliance of systems and devices is no longer sufficient and enterprises require continuous 24/7 detection & response capabilities and superior intelligence to recognize and mitigate critical threats to ultimately stop developing attacks in their tracks.

Our service assists with helping identify cybersecurity risk within your organization. It can help simplify your security monitoring challenge, reduce MTTD and MTTR, and enable you to focus your efforts on the value-creating parts of your business.

Verizon is a recognized leader in developing, integrating and operating scalable security operations for enterprise and government entities across the globe. The Verizon Security Operations Service enables organizations to tap into Verizon's extensive experience in managing security

The benefits of the Verizon Security Operations Service

With the Verizon Security Operations Service, organizations will benefit from our intelligence gained from providing security services for 25 years, while still retaining the advantages that a dedicated SIEM solution offers in terms of data control. This combination can help organizations to establish an operational security service and achieve a level of monitoring and analytics that may be more advantageous than what can be provided in-house.

Why choose the Verizon Security Operations Service?

- Gain access to industry experts: Partner with highly skilled and experienced security experts, analysts, services advisors, and security engineers from Verizon; addressing any potential skills shortage concerns.
- Drive additional value from security tools investments: A solution that uses your existing tools, infrastructure and capabilities, while providing the flexibility to adapt as your requirements evolve, including adoption of security analytics platform capabilities as they're implemented.
- Boost security operations capabilities: Gain 24/7 access to proactive security incident handling that provides remediation response actions to security threats within your organization; leveraging streamlined security operations processes and integration with your technology stack.
- Broaden and deepen threat visibility: Benefit from extensive threat intelligence gathered beyond the boundaries of your organization and through Verizon's 17 years of breach investigation (DBIR) applied to your environment. Through the correlation of threat intelligence with your data sources and our global threat intelligence we can help you achieve positive results.

verizon business

The Verizon Security Operations Service is a continuous security monitoring (detection and response) solution for identifying security threats, helping organizations respond to potential compromises before they materialize into serious data breaches or cause major harm to critical business infrastructure. Our service can help an organization derive value from existing tools and assist in achieving positive business outcomes.

A standardized approach to customizable security operations

The Verizon Security Operations Service provides a proven incident management capability, access to comprehensive security intelligence and detailed reporting. The service integrates into your existing security ecosystem, and leverages your own technology including security analytics platforms and other security tools. Verizon can enrich security event data by leveraging intelligence from a wide variety of sources to help detect potential cybersecurity threats. In addition to 24/7 incident handling, Verizon also provides recommendations for remediation, next actions and mitigation of cybersecurity risks to the customer based on industry best practices.

The Verizon Security Operations Service includes security monitoring for customer's IT infrastructure and tools within your environment. Our service includes security incident detection, handling and escalation, and threat analysis as standard. Additionally, detection content development, security analytics platform management, and extended reporting capabilities can also be provided.

Standard and Extended analytics models offer flexibility

The Verizon Security Operations Service provides flexibility in security operations services by offering two analytics models with the ability to customize to the customer's requirements. The service is available with either Standard or Extended levels of incident triage, and these form the basis of the service.

With both service models, Verizon provides global 24x7 security operations service options, support for multiple security maturity scenarios, threat hunting, and ticketing system support. With the Verizon Security Operations Service, Verizon can provide additional customized services in the areas of threat hunting, detection content development, governance, and security analytics platform management.

People: Seasoned and long-tenured experts

The Verizon Security Operations Service delivery team is comprised of security experts and can be grouped as follows:

- **Security Operations Analysts** is a 24x7 team performing security monitoring of incoming incidents, handling those incidents and providing security incident response guidance.
- The **Security Services Advisor** oversees the entire security service and provides a single point of contact within Verizon for you to interact with.
- The **Security analytics platform and SOAR Engineer** is responsible for the ongoing tuning of the customers security detection content and reporting.
- **Other experts** supporting the Verizon Security Operations Service include the following roles:
  - Tier 3 Security Analyst
  - Client Security Engineer
  - Designated Security analyst

Verizon Security Operations Services Standard

- 24x7 monitoring
- Security incident investigation and analysis in Verizon's SOAR platform and the customer's security analytics platform
- Threat hunting at HMM (Hunting Maturity Model) Level 1
- Specified response times, metrics and reporting
- Use case tuning
  - "Out of the box" analytics content delivered with the customer's security analytics platform
  - Customer specific analytics content
- A one-time initial review and tuning of customer's security analytics platform content
- A monthly service report

Verizon Security Operations Services Extended

provides all of the features of Standard with additional enhancements:

- Enhanced security incident investigation SLAs
- Extended analysis of security incidents
- Additional security incident investigation and analysis in the customer's security analytics platform
- Integrate with customer's security tools to perform containment activities
- A weekly service report

Figure 1: Features of the two service models of the Verizon Security Operations Service.

Note: A detailed list of features, tasks, responsibilities, and additional service options can be found in the Verizon Security Operations Service - Service Description.

Process: Proven operational procedures and workflows

The Verizon Security Operations Service is delivered from our regional SOCs that leverage tried and tested operational processes. For example, our high-level incident workflow can be described as follows:

verizon business

Incoming incident...

- Incident created within customer analytics platform
- Ingested into Verizon's incident handling platform

Standard analytics

Provide an analysis of the incident that allows the customer to continue further investigation with their own security team. Verizon will:

- Retrieve content
- Extract incident triggers
- Collect IoCs
- Depending on situation: Run drill-down search and verify similar historic incidents

If no additional information is required, go directly to Incident analysis summary.

Extend analytics

Provide more in-depth background information around an incident and suggested actions with, e.g.:

- Performing additional queries
- Sandboxing
- Including additional context data like domain registar information
- Syncing with threat hunting activities

Incident analysis summary

- Analysis of gathered data
- Triage decision based on available information
- Creation of summary showing information available
- Next steps for the customer

...two possible outcomes:

1. Escalation	2. Closing
of the incident to the customer CSIRT or response team via email and for critical severity via phone.	of the incident with the appropriate comments allowing a potential later review by the customer.

Figure 2: Incident workflow of Verizon Security Operations Service

20T	20+ trillion signals (raw logs) analyzed annually (on average)
35M	3.5+ million alerts annually (on average)
75k	75,000+ escalated tickets annually (on average)

Source: 2024 Verizon

Technology: Help enhance protection and tool integration

In order to derive value from your existing investments in security tools and from our ability to help detect potential threats to your business, the Verizon Security Operations Service will integrate both your and Verizon's own tools. More specifically, our analysts leverage:

- **Customer-provided toolsets**: The Verizon service will consume data from your security analytics platform and other existing tool sets.
- **Customer ticketing system**: Verizon will use the ticketing system provided by you to ensure integration with your teams and facilitate incident escalation and case management.
- **Verizon SOAR**: Verizon leverages a Security orchestration, automation and response (SOAR)-driven incident handling methodology that enables faster detection, response and mitigation.

We understand that you expect a predictable, measurable, quality service. The Verizon Security Operations Service will include metrics in an SLA that will clearly specify what you can expect from the service, and by when. We also publish quality metrics, fully document escalation procedures, and define the responsibilities of each party in the form of a RACI matrix.

Learn more

To find out how the Verizon Security Operations Service can help protect your business, contact your Verizon Business Account Manager and visit Verizon.com/business/security

verizon business