beazley security

Public Risk Innovation, Solutions, and Management (PRISM) Service Catalog

Issue Date: July 1, 2026

Expiration Date: June 30, 2027

PROGRAM INTRODUCTION & SERVICE CATALOG

Beazley Security is a global cybersecurity firm dedicated to helping clients prevent, prepare for, respond to, and investigate security incidents. Our team brings deep expertise from private industry, government, intelligence, and law enforcement, with capabilities spanning proactive risk management, incident response, digital forensics, offensive security, cybersecurity strategy, and threat detection.

In addition to its world-class incident response capabilities, Beazley Security offers services designed to help clients strengthen preparedness, reduce risk, and limit the impact of security incidents. The services in this catalog have been specifically developed for members of PRISM to support cybersecurity resiliency efforts, assist with regulatory readiness, and strengthen defenses against malicious actors.

The service offering subsections outlined in the Table of Contents provide descriptions and pricing for the fixed-fee services available at the time this catalog was created. Pricing is subject to change and has been calculated for PRISM members using the current Beazley discounted rate.

If a PRISM Participant wishes to purchase additional credits, add services beyond their allocated credits, or procure services outside this program catalog, a discounted rate has been made available to PRISM Participants and is reflected where applicable within each service offering.

Separate statements of work will be executed between Beazley Security and the participating organization(s), outlining the services to be provided and detailing any additional fees payable by the participant.

For more information, please contact **Jen Hockenstein at Jen.Hockenstein@Beazley.Security**

NEW: Security Posture Report, A complimentary offering available to ALL members, that does not count toward your credit allocation.

The Security Posture Report (SPR) delivers a non-invasive, strategic, point-in-time assessment of your organization's external cyber risk exposure. By analyzing your internet-facing technologies, the SPR translates complex technical findings into clear business insights that inform smarter security decisions.

Request a Custom Security Posture Report. Simply scan this QR Code:

Your tailored report will highlight:

- Attack surface
- Email security
- Security certificates
- High-risk software

Following report delivery, our experts can discuss the results, highlight potential business impact, recommending prioritized actions to strengthen resilience, reduce operational risk, and align security investment with organizational objectives. This is FREE to you; no credits are needed.

Table of Contents: Service Offerings

*Denotes services suitable for multiple risk pool members

Microsoft and Cloud Security Services

Active Directory Hardening Assessment

An Active Directory Assessment is a comprehensive cybersecurity service designed to evaluate the health, security, and performance of an organization's Active Directory infrastructure. Active Directory is a critical component of an organization's network, managing user accounts, permissions, and access control. This assessment provides insights and recommendations to enhance the efficiency, security, and resilience of Active Directory, minimizing the risk of unauthorized access and data breaches.

Description	Credits
Active Directory Hardening Assessment, OnPrem, Cloud, Hybrid	3 Credits

Ransomware Readiness Assessment

A comprehensive evaluation of the organization's current cybersecurity posture, including existing policies, procedures, incident response plans and procedures, and backup processes and procedures to ensure the availability and integrity of critical data in the event of a ransomware attack.

Description	Credits
Ransomware Readiness Assessment • Active Directory Assessment • Incident Response Plan Review • BCP/DR Plan Review • Backup Architecture Review • Detection Controls Review	3 Credits

Defender for Office 365 Pilot

Description	Credits
Microsoft Defender for Office 365 is a comprehensive, cloud-based email filtering service that helps protect your organization against unknown malware and viruses. It provides robust zero-day protection and includes features to safeguard your organization from harmful links in real time. Defender for Office 365 has rich reporting and URL trace capabilities that give administrators insight into the kind of attacks happening in your organization. It's part of Microsoft's advanced threat protection services, designed to help secure emails, files, and Office 365 applications against cyber threats. The pilot engagement includes discovery, architecture, documentation and validation with a pilot group of five users. Ready to be taken forward to a full production rollout.	3-4 Credits

Defender for Endpoint Pilot

Description	Credits
Microsoft Defender for Endpoint is a robust, enterprise-level platform designed to help organizations prevent, detect, investigate, and respond to advanced threats and data breaches on their networks. It uses the power of the Microsoft Intelligent Security Graph to rapidly detect threats across endpoints, allowing security teams to swiftly respond and secure their environments. Defender for Endpoint offers automated investigation and remediation capabilities, reducing the volume of alerts in minutes at scale. It's integrated with other Microsoft services, providing seamless protection across the organization's digital estate. The pilot engagement includes discovery, architecture, documentation and validation with a pilot group of five users. Ready to be taken forward to a full production rollout.	3-4 Credits

Active Directory/Entra ID Security Assessment

Description	Credits
The Active Directory and Entra ID Security Assessment service offers a comprehensive evaluation of an organization's identity and access management systems. It includes a thorough review of Active Directory and Entra ID environments, risk assessment, and compliance check. The service aims to enhance security, improve compliance, and optimize performance.	3 Credits

Entra ID Plan 1 Deployment Services

Description	Credits
Entra ID Plan 1 Deployment includes an evaluation of current configuration and features in use. Current configurations will be optimized based on best practices. Any unused features in a business use case will be enabled. Common Plan 1 features are MFA, Conditional Access, and SSO with SaaS applications.	3-4 Credits

Entra ID Plan 2 Deployment Services

Description	Credits
Entra ID Plan 2 Deployment includes an evaluation of current configuration and features in use. Current configurations will be optimized based on best practices. Any unused features in a business use case will be enabled. Common Plan 2 features are Privileged Identity Management and Risk-based sign in detections.	3-4 Credits

Microsoft Purview Pilot

Description	Credits
Microsoft Purview is a unified data governance service that helps organizations achieve a holistic understanding of their data landscape. It allows businesses to map, catalog, understand, and manage data no matter where it resides, whether in on-premises, multi-cloud, or SaaS applications. With Purview, organizations can automate data discovery, cataloging, and end-to-end data lineage. It also helps ensure compliance with privacy regulations by identifying sensitive data and enforcing data access policies. The pilot engagement includes discovery, architecture, documentation and validation with a pilot group of five users. Ready to be taken forward to a full production rollout.	3-4 Credits

Microsoft Intune Pilot

Description	Credits
Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). It allows businesses to manage mobile devices and apps, protecting company information by controlling the way it is accessed and shared. With Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure. It's part of Microsoft's Enterprise Mobility + Security suite, offering seamless integration with other Microsoft services like Azure and Office 365. The pilot engagement includes discovery, architecture, documentation, and validation with a pilot group of five users. Ready to be taken forward to a full production rollout.	3-4 Credits

M365 or Google Workspace Email Hardening Assessment

Description	Credits
An Email Hardening Assessment is a service designed to evaluate and enhance an organization's email security infrastructure. Given that email is a common vector for cyberattacks, including phishing, malware delivery, and business email compromise (BEC), it is crucial to secure email systems effectively. This assessment helps organizations identify vulnerabilities, misconfigurations, and weaknesses in their email security to prevent malicious email-based threats.	3-4 Credits

Cloud Security Assessment (Azure, AWS, GCP)

Description	Credits
A cloud security assessment is a comprehensive evaluation of an organization's cloud infrastructure to identify potential vulnerabilities and threats. It involves a thorough examination of the cloud environment, including data storage, applications, and network configurations. The Assessment helps in understanding the effectiveness of existing security measures and compliance with industry standards. It provides actionable insights and recommendations to enhance security posture, mitigate risks, and ensure data privacy. Ultimately, a cloud security assessment is crucial for maintaining the integrity and security of an organization's cloud-based assets.	4-5 Credits

M365 Copilot Technical Readiness

Description	Credits
Copilot can transform how organizations work, but only when the underlying data and controls are ready for it. This offering delivers that readiness: assessing the environment, locking down data governance to stop oversharing, protecting derivative works, and detecting insider risk and AI misuse. The result is a fully architected, monitored Copilot rollout, plus knowledge transfer that leaves the team ready to run it, enabling fast, safe AI adoption without putting data or reputation at risk.	3-4 Credits

M365 Security Roadmap – Identity, Collaboration & AI Security

Description	Credits
Most organizations use M365, but few have their tenant configured to best-practice security standards. This offering assesses a single M365 tenant - across Entra ID, Exchange Online, SharePoint and OneDrive, Teams, and AI security controls, against Microsoft and leading security frameworks, with no restriction on license level. The result is a clear, prioritized roadmap aligned to key risk indicators, delivered through a technical report and an executive summary, giving both practitioners and leadership a clear path to a stronger identity, collaboration, and AI security posture.	3-4 Credits

M365 Security Roadmap – Threat Protection, Data Security, Apps & Device Management

Description	Credits
Modern threats target endpoints, identities, cloud apps, data, and devices - and most organizations lack a clear view of how well M365 is protecting across all of them. This offering assesses a single M365 tenant against Microsoft and other leading security frameworks, with no restriction on license level. Spanning Defender XDR solutions, Intune, Purview, Microsoft Fabric, Power Platform and Viva Engage. It distills the findings into a prioritized roadmap aligned to key risk indicators, delivered through a technical report and executive summary, giving both technical teams and leadership a clear path to stronger threat protection, data security, and device management.	3-4 Credits

Advisory, Strategy and Risk Governance

AI Policy Development and AI Security Awareness Training

Description	Credits
Beazley Security's AI Policy Development and AI Security Awareness Training offering provides organizations the policy design guidance on AI Acceptable Use Policy and AI Cyber policy design for clients ranging from AI-risk averse to AI-heavy users. Additionally, Beazley Security will develop customized training sessions to help prepare organizations against AI Cyber threats as well as to enable appropriate AI usage internally for clients ranging from AI-averse to AI-heavy users. This is for clients looking for guidance on how to implement AI as a personal assistant as well as education their end users on the threats AI can pose to an organization.	3-5 Credits

Beazley Security Cyber Preparedness Workshop

Description	Credits
Beazley Security's Cyber Preparedness Workshops are customized, expert-led sessions designed to help organizations strengthen their readiness for today's most common and high-impact cyber incidents. Each workshop equips participants with practical tools, response strategies, and actionable guidance tailored to the organization's risk profile, operating environment, and current security maturity. Workshop topics can be tailored to client needs. Examples of previously delivered workshop focus areas include: • Developing an incident response program • Creating a business continuity plan • Preparing for and responding to ransomware incidents • Responding to business email compromise incidents • Managing crisis communications during a cyber event Workshops are designed to foster cross-functional collaboration among security, IT, legal, communications, operations, executive leadership, and other key stakeholders.	2-3 Credits

Incident Response Plan Review

Incident Response Plan Review is a service designed to review the Incident Response Plan for an organization to effectively respond to cybersecurity incidents and data breaches. The service involves the collaborative creation of a comprehensive incident response plan (IRP) tailored and customized to the organization's unique needs and risks.

Description	Credits
Incident Response plan review specifically focuses on the following domains: • Teams and Roles • Assessment, Classification, and Escalation • Analysis • Containment, Mitigation, Eradication, and Recovery • After Action Review	1-2 Credits

Incident Response Play Card Development*

Incident Response Play Card Development is a service focused on creating a structured and comprehensive set of guidelines and procedures that facilitate the effective preparation for and efficient response to cybersecurity incidents such as Ransomware, Business email compromise, etc. These play cards serve as a quick-reference guide for incident responders, ensuring that they can follow a well-defined plan when an incident occurs.

Description	Credits

• Incident Response Play Card Development
  ○ Development of up to three incident response play cards
  ○ Example play card topics include:
  • Supply chain attack
  • Data exfiltration through third-party compromise
  • AI governance incident
  • Ransomware
  • Email outage
  • Credential loss
  • Business email compromise
  • Endpoint protection incident
	3 credits for 3 play cards

Cybersecurity Gap Assessment

Beazley Security's Cybersecurity Gap Assessment helps organizations to assess and improve their cybersecurity posture against certain regulatory frameworks e.g., HIPAA, NIS, GDPR, CIS 18 etc. Our expert Advisory Services team conducts a thorough assessment of your existing security infrastructure, policies, resources, and procedures to identify vulnerabilities and areas of improvement. We customize methodologies aligned to each client's pertinent regulatory framework to evaluate your network architecture, data protection measures, access controls, incident response protocols, and more.

Based on the assessment findings, we work closely with your team to develop tailored strategies

and roadmaps to enhance your security posture. This includes recommending technology solutions, implementing best practices, and establishing robust policies and procedures to mitigate risks effectively.

Description	Credits
Three examples of framework-based Security Assessments are provided below: 1. A CIS 18 Gap Assessment is a targeted cybersecurity service designed to evaluate an organization's current security practices against the Center for Internet Security's Critical Security Controls (CIS Controls). This assessment provides a structured analysis of how well an organization aligns with these industry-recognized best practices, identifying specific areas where security measures may be lacking or insufficiently implemented. The outcome of the assessment is a clear understanding of existing cybersecurity gaps, prioritized recommendations for remediation, and a strategic roadmap to strengthen the organization's overall security posture in alignment with the CIS Controls framework.	Contact Us
2. A NIST Cybersecurity Framework (CSF) Gap Assessment is a specialized cybersecurity service aimed at evaluating an organization's existing cybersecurity practices and determining their alignment with the National Institute of Standards and Technology's Cybersecurity Framework. This framework offers a structured and flexible approach to managing and reducing cybersecurity risks. Through the assessment, organizations gain insight into where their current practices diverge from the NIST CSF guidelines, enabling them to identify specific gaps and areas for improvement. The result is a clear, actionable understanding of how to enhance their cyber security program in accordance with the NIST CSF, ultimately supporting stronger risk management and resilience.	Contact Us
3. A HIPAA Gap Assessment is a focused compliance service designed to assist healthcare organizations and their business associates in evaluating their adherence to the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. This assessment examines the organization's current policies, procedures, and technical safeguards to determine how well they align with mandated standards for protecting patients' protected health information (PHI). By identifying areas of non-compliance or insufficient implementation, the assessment provides a clear path toward achieving and maintaining HIPAA compliance, reducing regulatory risk, and strengthening the overall privacy and security posture of the organization.	Contact Us

Security Policy Review and Development

Beazley Security Policy Review and Development service provides options for organizations with security policies and procedures at any maturity level, from those building from the ground up to others looking to bolster existing documentation. Pricing for Security Policy Review and Development depends upon the volume and granularity of the assistance needed, as well as additional consulting hours, with descriptions provided in the table below:

Option	Description	Credits
1	Review and development efforts that include the creation of a template that can be used to create or standardize additional policies and procedures. This includes 15 hours of consulting from Beazley Security experts on related topics.	Contact Us
2	Any fully customized security policy review and creation of missing policies and procedures or development of existing library of documentation necessary for the organization to function securely in its operating environment and business sector.	Contact Us

Virtual Chief Information Security Officer*

Description	Credits
A Virtual Chief Information Security Officer (vCISO) provides expert-level augmented cybersecurity expertise and strategic guidance tailored to your organization's unique needs without the overhead of a full-time executive. Leveraging years of experience across industries, our vCISOs help design and implement comprehensive security programs, ensure compliance with regulatory frameworks, conduct risk assessments, and respond to evolving threats with agility. Whether you're building security from the ground up or need support refining your existing operations, this service delivers board-level leadership, insight and tactical execution to strengthen your security posture and protect your business. • Up to 10 hours per credit	1 Credit

Security Program Review

The Security Roadmap Review is a high-level consulting engagement designed to assess an organization's
existing security roadmap or help establish one if none exists.

This scaled back review includes a lightweight gap analysis aligned with industry standards, identification of the top 5 to 7 priority risk areas, and strategic recommendations to guide future security planning. The goal is to provide a clear, actionable foundation for refining or developing a security strategy that aligns with business objectives and risk tolerance.
Deliverables include a summary report highlighting key findings, prioritized risks, and roadmap recommendations. While the engagement is scoped as a high-level review, it can be extended into a more detailed analysis if needed, with additional consulting hours and credits required.

Description	Credits
Security Program Review, high level advice using existing documentation and interviews	2-3 Credits

Security Awareness Training*

Beazley Security believes in making security awareness training accessible for all. Beazley Security's Security Awareness Training service has been developed to offer a cost-effective, workshop-based delivery of security awareness training suitable for all audiences.

Beazley Security combines real-world experience in Incident Response and Managed Detection and Response with experienced trainers who can bring these subjects to life.

Option	Description	Credits
1	Includes virtual training on critical security topics that empowers your personnel to identify and report suspicious activity and integrate best practices into their everyday work that can protect your organization from disaster. *On-site training is available but will incur customary T&E costs.*	2-3 Credits
2	Any fully customized Security Awareness Training program, including collaboratively developed training material delivered in-person, online, or via recorded video for ongoing use.	3-5 Credits

Incident Response, Restoration, and Recovery

Endpoint Compromise Assessment

An endpoint compromise assessment is a 21-day systematic and thorough examination of an organization's endpoint devices, such as desktops, laptops, servers, cloud, SaaS applications, and mobile devices, to identify signs of compromise or undetected security breaches. This assessment is designed to detect indicators of malicious activity, unauthorized access, malware infections, or other historical compromises that may have occurred on these devices. The engagement includes deployment of advanced endpoint detection and response (EDR) tooling, digital forensics, and threat hunting.

The primary goal of an endpoint compromise assessment is to quickly validate existing security controls and identify and mitigate potential security incidents to prevent further damage and data loss.

Description	Credits
Up to 100 Endpoints in scope	2 Credits
Up to 250 Endpoints in scope	3 Credits
Up to 500 Endpoints in scope	4 Credits
Up to 1,000 Endpoints in scope	5 Credits

Restoration and Recovery Workshop*

In the face of unforeseen disasters or disruptions, having a robust business-wide recovery and restoration plan is essential to minimize downtime, limit impact, mitigate losses, and execute an efficient return to normal business operations. Our comprehensive service is designed to help organizations proactively prepare for and respond to a wide range of potential crises, from natural disasters to cyberattacks and beyond.

Description	Credits
Restoration and Recovery Workshop	1 Credit

Offensive & Technical Security

Internal Vulnerability Assessment

An Internal Vulnerability Assessment will assess an organization's internal network, systems, and applications to identify potential vulnerabilities that could be exploited by internal threats. This is accomplished through scanning/discovery, identification of vulnerabilities, risk prioritization, reporting and remediation guidance.

Network Size	Frequency	Credits
/24	One Time Assessment	1 Credit
/24	Quarterly Assessments	2 Credits
/24	Monthly Assessments	3 Credits

External Vulnerability Assessment

An External Vulnerability Assessment will assess an organization's external-facing hosts and services to identify potential vulnerabilities that could be exploited by external threats. This is accomplished through scanning/discovery, identification of vulnerabilities, risk prioritization, reporting and remediation guidance.

Active IPs per Member	Frequency	Credits
Up to 64	Once	1 Credit
Up to 256	Once	2 Credits
Up to 512	Once	3 Credits
Up to 64	Quarterly	2 Credits
Up to 256	Quarterly	4 Credits
Up to 512	Quarterly	5 Credits
Up to 64	Monthly	3 Credits
Up to 256	Monthly	7 Credits
Up to 512	Monthly	8 Credits

External Penetration Testing

An External Penetration Test is a comprehensive service designed to evaluate an organization's external internet facing systems to uncover potential vulnerabilities and data exposure that could lead to unauthorized access. This is accomplished through system discovery, enumeration, vulnerability discovery, exploitation, reporting and remediation guidance.

Active IPs	Frequency	Credits
Up to 32	Once	2 Credits
Up to 64	Once	3 Credits
Up to 128	Once	5 Credits
Up to 256	Once	8 Credits
Up to 512	Once	12 Credits

Internal Penetration Testing

An Internal Penetration Test is a comprehensive service designed to evaluate an organization's internal network security. The primary goal is to simulate the activities of a threat actor or a compromised system and to proactively address vulnerabilities to prevent unauthorized access and data breaches. This is accomplished through system discovery, enumeration, vulnerability discovery, exploitation, privilege escalation, reporting and remediation guidance.

Network Size	Frequency	Credits
/24	Once	3 Credits

Cloud Penetration Testing

A Cloud Penetration Test will examine the organization's cloud services for any attack paths or misconfigurations that would result in access to applications or potentially sensitive information. The assessment is designed to identify any risks, vulnerabilities, or gaps in the security of the organization's cloud infrastructure.

Network Size	Frequency	Credits
1 Tenant	Once	2 Credits

Open-Source Intelligence (OSINT) Exposure Assessment

An Open-Source Intelligence (OSINT) Exposure Assessment evaluates the potential risks an organization face from publicly available information. Cybercriminals frequently leverage OSINT to gather intelligence for targeted attacks, social engineering, and infrastructure exploitation. This assessment is tailored to the organization's specific needs and typically focuses on identifying security weaknesses, publicly exposed data, and potential vulnerabilities that could be exploited in further attacks.

Network Size	Frequency	Credits
1 Organization	Once	2 Credits

Phishing Campaign Assessment

A Phishing Campaign Assessment evaluates an organization's vulnerability to phishing attacks. Phishing remains a prevalent and highly effective tactic used by cybercriminals to compromise sensitive data and gain unauthorized access to systems and accounts. This assessment helps organizations test their employees' susceptibility to phishing, assess their security awareness, and identify areas for improvement in their anti-phishing measures.

Description	Credits
Phishing Campaign Assessment up to 250 Users	3 Credits
Phishing Campaign Assessment up to 500 Users	5 Credits

Web Application Penetration Testing

Web Application Penetration Testing will assess the security of web applications, websites, and APIs. It involves simulating real-world cyberattacks to identify vulnerabilities, weaknesses, and potential threats within web applications. The primary objective is to uncover security flaws that could be exploited by malicious actors, leading to data breaches, unauthorized access, and other security risks.

Due to the bespoke nature of each engagement, pricing for WAPTs is based on the number of days required to perform the testing. Contact Beazley Security for pricing details.

Description	Credits
Web Application Penetration Test	5+ Credits

VPN Assessment

With the increasing adoption of cloud services, the expansion of global business, and the rise of remote work, organizations are increasingly relying on Virtual Private Networks (VPNs) for secure, cost-effective connectivity between locations. Deployed at network perimeters, VPNs have become a primary target for threat actors. Due to the complexity of VPN software, devices, and configurations, they have been a significant point of breach in recent years.

Our VPN Security Assessment is designed to evaluate the key areas of your VPN services to ensure they do not expose your organization to unnecessary risks. This assessment will include active testing with an optional configuration or breakout assessment, offering comprehensive insights into potential vulnerabilities.

Description	Credits
VPN Assessment	2 Credits

Remote/Virtual Desktop Breakout

With the rise of remote work and the need for always-on connectivity, virtual desktop infrastructure (VDI), remote desktop services, and application streaming platforms have grown in popularity. These solutions offer organizations a flexible and cost-effective way to support legacy applications, enhance security, and streamline operations. However, as these services are often internet-accessible, leverage shared resources, and are frequently deployed alongside critical infrastructure, they can introduce significant security risks if not properly configured.

The Remote/Virtual Desktop Security Assessment is designed to evaluate the security posture of these environments. The assessment aims to ensure that virtual desktop solutions are robustly secured against threat actors attempting to breach the service, bypass security controls, escalate privileges, or pivot into the wider environment.

Description	Credits
Remote/Virtual Desktop Breakout	2 Credits

Looking for something else?

The cybersecurity professional services listed in this catalog are not an exhaustive representation of Beazley Security's full capabilities. If you do not see a service that meets your needs, please contact us. We will work with you to tailor a solution aligned to your organization's priorities, risk landscape, and desired business outcomes. Annual program benefits will continue to apply where eligible.