ALEXSTA
CYBERSECURITY AG

SERVICES CATALOG / 2026

Bespoke security for organizations that cannot afford to be wrong.

A boutique firm of senior consultants. Eleven services, each scoped to the organization rather than fitted to a package.

AlexSta CyberSecurity AG
Sinserstrasse 67 / 6330 Cham, Zug / Switzerland

alexsta-cybersecurity.com

[CONTENTS]

What is in this catalog

Services are tailored to each organization, so the descriptions here describe the shape of an engagement rather than a fixed package. Scope, duration and detail are agreed in writing before work begins. This catalog is an overview, not a binding offer; engagements are governed by the terms of our formal agreements. For current information, or for a requirement not covered here, contact us directly.

[01 / HOW WE WORK]

More than a consulting firm.

AlexSta Cybersecurity AG is more than just a cybersecurity consulting firm; it is a boutique powerhouse of highly experienced professionals dedicated to delivering custom-tailored, high-quality cyber services. Whether the need is proactive or reactive, unmatched technical expertise and an unwavering commitment to excellence define every engagement.

Through meticulously designed engagements, clients' existing investments in security are optimized, ensuring maximum value and effectiveness. Consultants at AlexSta Cybersecurity AG invest significant time in cutting-edge research and innovation, reshaping the value delivered to meet and exceed even the most demanding client requirements.

Our clients are forward-thinking organizations with a strong understanding of their security posture and the specific risks they aim to mitigate. They seek services that go beyond generic, off-the-shelf solutions, and demand a level of precision, expertise, and attention to detail that few can offer.

If your organization has demanding security requirements and values a partner who can rise to the challenge, you've come to the right place.

Our philosophy is simple: excellence in every engagement. We are driven by a commitment to overdeliver and ensure that every project we undertake leaves a lasting impact on your security posture.

Innovation at the Core: We are relentless in staying ahead of the curve. Through constant research, innovation, and collaboration with industry leaders, we ensure our methodologies and tools are always a step ahead of emerging threats.

Unparalleled Quality: Every engagement is crafted with meticulous care, ensuring no detail is overlooked.

Unbeatable Value: Our offerings deliver a level of quality and impact that far outpaces the price you pay.

Obsessed with Overdelivering: Achieving success for clients is the core mission at AlexSta Cybersecurity AG, with every effort dedicated to not only meeting but surpassing expectations at every step.

End-to-End Support: From proactive risk assessments to incident response and recovery, our comprehensive service offering ensures that we are with you at every step of your cybersecurity journey. Whether you need to prevent, detect, or respond, we deliver seamless, end-to-end support.

We take pride in our ability to think beyond the conventional and deliver results that set us apart from the competition.

Our clients include some of the most respected names across industries such as finance, healthcare, and critical infrastructure. Time and again, we have delivered results that not only meet but exceed expectations, enabling long-term resilience and trust.

To ensure a smooth and transparent collaboration, please review the following details:

Scheduling and Availability: All services are subject to scheduling based on our consultants' availability. Early engagement to secure your preferred timeline.

Custom Requests: Every organization is unique, and so are its cybersecurity challenges. If your needs extend beyond the services listed in this catalog, we invite you to contact us. Our team is experienced in crafting bespoke solutions designed to meet your specific business objectives.

Four categories, one standard.

Our services are organized into four categories that address the range of cybersecurity needs our clients bring. Each reflects the same commitment to targeted, high-quality work.

PROACTIVE

Proactive Services

Anticipate threats and strengthen your security posture with services designed to identify and mitigate vulnerabilities before they are exploited.

- **Risk Assessments.** Comprehensive evaluations of your organization's security landscape, including vulnerability assessments, threat modeling, and attack surface analysis.
- **Penetration Testing.** Simulated attacks to uncover exploitable weaknesses in applications, networks, and systems.
- **SOC Capability Enhancement.** Elevate your Security Operations Center's effectiveness with targeted improvements in incident response processes, threat hunting methodologies, malware analysis capabilities, and automation strategies to accelerate detection and response times.
- **Cybersecurity Training.** Interactive training programs tailored for employees, IT teams, and executives, including phishing simulations and technical security workshops.

MANAGED

Managed Services

Gain peace of mind with continuous monitoring and expert management of your cybersecurity infrastructure.

- **Security Operations Center (SOC).** 24/7 monitoring, detection, and response to cyber threats through our dedicated SOC team.
- **Managed Endpoint Security.** Implementation and oversight of advanced Endpoint Detection and Response (EDR) solutions to protect against malware, ransomware, and other endpoint threats.
- **DFIR Retainer.** Secure priority access to our Digital Forensics and Incident Response (DFIR) experts. Our program service ensures rapid, on-demand assistance for incident response, forensic investigations, and mitigation strategies when time is critical.
- **Threat Hunting.** Proactive investigation and identification of hidden threats within your environment.

REACTIVE

Reactive Services

Quick, expert responses to incidents and breaches to minimize damage and support recovery.

- **Incident Response.** End-to-end incident management, including containment, forensic analysis, and root-cause investigation.
- **Digital Forensics.** Deep analysis of digital artifacts, including disk, memory, and network data, to uncover the who, what, and how of an incident.
- **Compromise Assessments.** Retrospective investigations to detect past intrusions or ongoing threats and provide actionable recommendations.

SPECIALIZED

Specialized Services

Tackle unique and advanced cybersecurity challenges with precision and expertise.

- **Red Team Operations.** Advanced adversarial simulations to test your defenses, including physical, social engineering, and technical attack vectors.
- **Cloud Security.** End-to-end support for secure cloud adoption, from architecture design to continuous monitoring and compliance.
- **IoT and OT Security.** Protecting Internet of Things (IoT) devices and Operational Technology (OT) systems from emerging threats.

[03 / SERVICES]

The services in detail.

Each service below sets out what it is for, the value it delivers, how it is run, what you receive, and what we need in order to scope it accurately.

SERVICE 3.1

Compromise Assessment

The Compromise Assessment Service offers a comprehensive evaluation of an organization's IT environment to identify any indicators of compromise or unauthorized activity that may have evaded existing security controls. This service is essential for organizations aiming to validate their current security posture and confirm that their network and systems are free from undetected breaches or malicious activity. Using advanced forensic tools and methodologies, the assessment thoroughly examines all aspects of the digital environment, including endpoints, servers, and network devices, providing actionable insights to enhance security resilience.

Business value

- **Early Detection of Breaches.** Identify hidden breaches or ongoing malicious activities, reducing the potential damage from undetected compromises.
- **Enhanced Security Confidence.** Gain assurance in your security posture with a comprehensive evaluation of your systems and networks.
- **Risk Management.** Understand and manage the risks associated with undetected threats, enhancing your organization's overall risk management strategy.
- **Regulatory Compliance.** Ensure compliance with industry standards and regulations by proactively identifying and addressing potential security lapses.
- **Informed Security Decisions.** Use the insights gained from the assessment to make informed decisions about security strategies and investments.

Methodology

01 The methodology of a Compromise Assessment (CA) involves a systematic and comprehensive review of an organization's IT environment to identify signs of a security breach or compromise.

02 Moreover, the methodology extends beyond identifying evidence of compromise, recognizing that gaps in best practices can serve as open invitations for threat actors. Each assessment rigorously evaluates current security practices, identifying any missing elements that could be exploited.

03 By addressing both direct indicators of compromise and deficiencies in best practices, this dual-layered approach ensures a comprehensive enhancement of cybersecurity. This holistic strategy not only strengthens defenses against existing threats but also fortifies the environment against potential future exploits, setting a benchmark for robust and forward-thinking security protection.

The methodology typically encompasses the following steps

01 **Planning and Scope Definition.** Establish the objectives, scope, and scale of the assessment. This includes determining the critical assets, systems, and network segments to examine.

Data Collection: Gather relevant data from various sources within the IT environment, such as

01 Active Directory (AD) security logs

02 Network infrastructure (DNS, PROXY, Firewall) logs.

03 Business applications.

04 Endpoint data (using Velociraptor).

05 This step may also involve deploying specialized forensic tools and sensors to collect additional data.

06 **Threat Intelligence Integration.** Utilize up-to-date threat intelligence to identify known indicators of compromise (IoCs) and tactics, techniques, and procedures (TTPs) used by attackers. This information helps in pinpointing suspicious activities and patterns that may indicate a breach.

07 **Analysis & Triage.** Analyze the collected data to identify anomalies, signs of unauthorized access, or evidence of malicious activity. This involves both automated analysis through security tools and manual investigation by cybersecurity experts.

08 **Incident Confirmation.** Validate potential security incidents through further investigation and corroboration, ensuring that detected anomalies are indeed signs of compromise.

09 **Impact Assessment.** Assess the impact of any confirmed compromises on the organization's operations, data integrity, and security posture.

10 **Reporting and Recommendations.** Compile findings into a comprehensive report detailing the identified issues, their impact, and recommendations for remediation and enhancing security posture.

Deliverables

- The deliverables from a Compromise Assessment provide an organization with actionable insights and a clear understanding of its security status. Key deliverables typically include:
- **Executive Summary.** A high-level overview of the assessment's findings, aimed at senior management, summarizing the scope, methodology, key findings, and recommended actions.
- **Detailed Findings Report.** An in-depth report that includes:
- Description of the methodology and tools used.
- Detailed accounts of all identified signs of compromise, including the nature of each threat, affected systems, and evidence supporting the findings.
- Analysis of the impact of these compromises on the organization's security and operations.
- **Remediation Plan.** A prioritized list of recommended actions to address identified vulnerabilities and compromises. This plan includes both short-term fixes to immediate threats and long-term strategies to improve security posture.
- **Incident Response Recommendations.** Guidance on responding to identified compromises, including steps for containment, eradication of threats, and recovery of affected systems.
- **Enhanced Security Measures.** Recommendations for enhancing the organization's security measures, practices, and policies to prevent future breaches. This may include suggestions for security tools, training, and process improvements.
- **Presentation and Debriefing.** A formal presentation of the findings and recommendations to the organization's stakeholders, followed by a debriefing session to discuss the results and plan next steps.

WHAT WE NEED TO SCOPE IT

- Count of endpoints.
- Count of applications hosted by the client and exposed to Internet.
- Number of users.
- Does the client use Azure Entra ID and O365.

INDICATIVE DELIVERY SCHEDULE

MILESTONE	W1	W2	W3	W4	W5
Kick-Off and planning	■				
Velociraptor deployment	■				
Data Collection			■		
Triage of hits			■		
Final report				■	
Report review with customer					■

SERVICE 3.2

Threat Hunting as a Service

Threat Hunting as a Service (THaaS) is a proactive solution focused on identifying potential threats within an organization's digital environment. Leveraging existing technologies such as Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), and Network Detection Systems (NDS), this service aggregates and analyzes telemetry and log data to uncover hidden risks and suspicious activities.

All data is processed on a dedicated server using advanced data analysis and pattern recognition to uncover hidden, emerging, or advanced threats that conventional security measures might miss. In addition to the standard threat hunting deliverables, our service provides innovative real-time use-case ideas, enhancing your ongoing security monitoring and threat detection capabilities.

Business value

- **Proactive Threat Detection.** Stay ahead of potential threats by identifying and addressing them before they escalate.
- **Enhanced Security Posture.** Improve your overall security posture with advanced threat hunting capabilities, reducing the risk of significant breaches.
- **Customized Security Insights.** Gain valuable insights specific to your organization's environment, leading to more effective security strategies.
- **Strategic Improvement Suggestions.** Benefit from actionable recommendations for real-time security monitoring and threat detection enhancements.
- **Resource Optimization.** Leverage our expertise to augment your existing security team, optimizing your resource utilization and focus.

Methodology

01 **Integration with Client Technologies.** Establish connections with the client's existing EDR, SIEM, and (Network Detection Systems) NDS systems to aggregate necessary telemetry and logs.

02 **Data Aggregation and Processing.** Collect and process the aggregated data on a dedicated server using Python for advanced data analysis.

03 **Hunt Cycles.** Conduct threat hunting activities on a monthly basis, ensuring regular and systematic examination of the client's digital environment.

Threat Hunting main categories

01 **Threat Intelligence-Based Hunts.** Perform hunts using the latest Threat Intelligence Indicators of Compromise (IOCs) from current threat attack campaigns. This involves analyzing known malicious patterns and tactics to uncover similar activities in the client's environment.

02 **Anomaly Detection and Pattern Recognition Hunts.** Utilize telemetry and logs from customer's security systems to identify anomalies and advanced attack patterns. This type of hunt focuses on uncovering unusual activities or potential sophisticated security threats that might evade traditional detection methods.

03 **Development of Real-Time Use-Cases.** Create innovative real-time use-case ideas based on the findings from both types of hunts to enhance the client's ongoing security monitoring and threat detection.

04 **Continuous Feedback and Adaptation.** Provide regular feedback and adapt hunting strategies to align with the evolving threat landscape and the client's specific environment, ensuring the hunts remain effective and relevant.

Deliverables

- **Threat Hunting Report.** Detailed report of the threat hunting activities, findings, and potential threats identified. The reports are done following the TH cycles (recommended monthly).
- **Real-Time Use-Case Ideas.** A set of innovative ideas for real-time security monitoring and threat detection use-cases.
- **Security Enhancement Recommendations.** Strategic recommendations for enhancing the client's overall security posture based on the findings.
- **Data Analysis Summary.** A summary of the data analysis and pattern recognition outcomes.
- **Continuous Improvement Plan.** A plan for ongoing threat hunting and security monitoring improvement, tailored to the client's evolving needs.

WHAT WE NEED TO SCOPE IT

- **Size of the environment.** number of endpoints, users, applications exposed to Internet.
- Desired duration of the service (minimum 1 year contract).

SERVICE 3.3

Threat Hunting Capability Assessment

The Threat Hunting Capability Review service assesses the maturity, effectiveness, and alignment of an organization's Security Operations Center (SOC) threat hunting function with its business and security objectives. This service identifies gaps in current processes, tools, and skillsets, providing actionable recommendations to transform threat hunting into a proactive and valuable service that enhances organizational security.

Our experts analyze the SOC's current threat hunting methodologies, data sources, and integration with other security functions, benchmarking them against industry best practices such as the MITRE ATT&CK framework. The result is a tailored roadmap for building a robust threat hunting capability that identifies advanced threats and aligns with the organization's strategic goals.

Business value

- The Threat Hunting Capability Review service delivers measurable value by helping organizations evolve from reactive to proactive threat detection. A mature threat hunting capability strengthens the SOC's ability to identify and mitigate sophisticated threats before they impact the organization, reducing the risk of data breaches and operational disruptions.
- By transforming threat hunting into a well-defined and valuable SOC service, organizations can:
- Gain deeper visibility into their threat landscape.
- Build resilience against advanced threats that evade traditional detection tools.
- Demonstrate a proactive security posture to stakeholders and regulators.
- Ultimately, the service enables the SOC to provide meaningful insights and risk mitigation strategies to the business, enhancing overall security operations and supporting informed decision-making.

Methodology

The Threat Hunting Capability Review service employs a structured and collaborative approach to assess and enhance the SOC's threat hunting capabilities

01 **Assessment of Current Capability.** Conduct a comprehensive review of existing threat hunting processes, tools, data sources, and integration with SOC workflows. This includes evaluating the use of frameworks (e.g., MITRE ATT&CK) and alignment with organizational security objectives.

02 **Gap Analysis.** Identify gaps in current threat hunting efforts, such as missing data sources, insufficient automation, limited scope, or inadequate expertise.

03 **Recommendations & Roadmap Development.** Provide actionable recommendations to address identified gaps, focusing on process improvements, skill development, tool optimization, and integration with other SOC functions.

04 **Implementation Support (Optional).** Assist in implementing the recommended changes, including process redesign, technology configuration, and training for threat hunters.

05 **Follow-Up Review.** After implementation, conduct a follow-up review to measure progress and refine the capability further.

Deliverables

The key deliverables from this service include:

- **Threat Hunting Capability Assessment Report.** A detailed report summarizing the current state of the SOC's threat hunting capability, identified gaps, and areas for improvement.
- **Actionable Recommendations.** A prioritized set of recommendations to build and mature the threat hunting function, including short-term and long-term actions.
- **Roadmap for Capability Development.** A structured plan for implementing the recommendations, including timelines, milestones, and resource requirements.
- **Threat Hunting Use Case Catalogue.** A tailored list of use cases for proactive threat hunting based on the organization's threat landscape and business context.
- **Training and Skill Development Plan.** A customized plan to enhance the knowledge and expertise of SOC analysts in threat hunting techniques and frameworks.
- **Post-Engagement Review (Optional).** A review conducted after the implementation of recommendations to evaluate progress and refine the capability further.

INDICATIVE DELIVERY SCHEDULE

SERVICE 3.4

Cyber Resilience Assessment & Enablement

This two-phase engagement helps organizations assess and strengthen their cyber resilience posture by aligning their security operations capabilities with both the evolving threat landscape and internationally recognized cybersecurity standards.

The engagement starts with a focused Cyber Resilience Maturity Assessment and is followed by a targeted enablement phase, during which all critical gaps are addressed through the development of tailored documentation, processes, and service definitions.

The assessment is applicable across sectors and is designed to ensure that the organization's security operations are not only fit-for-purpose but capable of continuously delivering value in real-world threat scenarios. The evaluation and resulting improvements consider the organization's business context, technology environment, and applicable regulatory obligations.

When needed, the engagement can be mapped to national or sector-specific frameworks such as the SAMA Cybersecurity Framework (Saudi Arabia), NCA ECC/CCC (KSA), DESC (Dubai), or QCB/NIA (Qatar).

Business value

- This service provides a direct path from situational awareness to capability uplift. By combining a precise diagnosis of the current maturity level with practical enablement, organizations can rapidly close gaps that impact their ability to detect, respond to, and manage cyber threats.
- The result is not only a set of new (or updated) documents and templates, but a tangible strengthening of internal capabilities: teams gain improved clarity of roles, structured procedures, and hands-on exposure to best practices that endure beyond the engagement itself.
- All these will produce a more defensible, standards-aligned, and auditable security operations capability - whether the goal is continuous improvement, regulatory readiness, or the launch of new security functions.

Methodology

01 **Our methodology is grounded in two foundational coordinates.** the applicable threat landscape and internationally recognized industry best practices. This ensures that the assessment reflects both the real-world threats an organization is likely to face and the practical capabilities required to withstand them.

We draw on globally respected frameworks such as NIST CSF 2.0, CIS Controls, MITRE ATT&CK, and STIG, and, where relevant, map findings to regional regulatory frameworks such as

01 SAMA Cybersecurity and IT Governance Frameworks (Saudi Arabia)

02 NCA ECC/CCC (Saudi Arabia)

03 Dubai DESC (UAE)

04 QCB ICT Regulations and NIA (Qatar)

05 This is not a checklist-based audit nor a shallow verification of policy documents. It is a rigorous, outcome-oriented assessment led by consultants with decades of hands-on cybersecurity experience. Every recommendation is filtered through practical know-how, not just theory. We assess the design, execution, and operational reality of SOC services to determine how effectively they deliver protection and value.

Unlike conventional regulatory reviews that stop at surface-level documentation or high-level process definitions, our engagement includes

01 Full-spectrum review of security documentation used by the SOC

02 Configuration-level validation of selected key security controls (e.g., logging, EDR, SIEM, incident management tooling)

03 Evaluation of the actual execution of core SOC processes, not just whether they exist on paper

We assess security operations holistically, focusing on how services are delivered across four strategic axes

01 Strategy (vision, planning, leadership mandate)

02 Coverage (threat and asset coverage, procedural completeness)

03 Integration and Impact (cross-team alignment, responsiveness, automation)

04 Continuous Improvement (metrics, feedback loops, lessons learned)

05 Special weight is placed on Strategy and Coverage, reflecting their criticality in real-world defense outcomes.

Phase 1 , Cyber Resilience Maturity Assessment

This phase identifies the organization's current level of cyber resilience by examining how core SOC services are structured and executed in practice. It includes

01 **Threat Landscape Profiling.** Sector-relevant threat actors, attack patterns, and abuse scenarios are identified to guide the evaluation

02 **Service-Centric Assessment.** We focus on how SOC services (e.g., monitoring, detection engineering, response, threat intel, threat hunting) operate as a whole, not just isolated domains or technologies

03 **Structured Stakeholder Interviews.** Deep-dive discussions with technical and functional owners to assess how each service delivers value and interacts with the business

04 **Review of Operational Documentation.** Analysis of existing policies, procedures, and response plans used by the SOC

05 **Control Configuration Sampling.** Validation of implementation quality for critical controls (e.g., SIEM, logging, IR tools, threat intel feeds)

06 **Multi-Axis Maturity Scoring.** Each service is evaluated across Strategy, Coverage, Integration, and Continuous Improvement axes, with results compiled into both executive and technical reports

07 **Regulatory Mapping (if applicable).** Where relevant, assessment results are mapped to SAMA, NCA, DESC, or QCB frameworks

Deliverables - Phase 1

01 Threat Landscape Brief (summary of relevant actors and scenarios)

02 Executive Summary Report

03 Full Maturity Assessment Report

04 Prioritized Capability Uplift Roadmap

Phase 2 , Capability Enablement and Documentation Development

01 This phase closes identified gaps by delivering custom, high-quality operational content and engaging directly with internal teams to ensure long-term impact.

02 **Tailored Documentation Development.** Based on assessment outcomes, we produce clear, aligned, and executable materials across key SOC capabilities

03 **Feedback and Handover Sessions.** Every deliverable is explained through structured walkthroughs with the client's team to ensure understanding and ownership

04 **Knowledge Transfer.** We conduct deep-dive sessions with service owners and SOC analysts to help them apply new processes and evolve them over time

05 **Target Maturity.** Deliverables are designed to help the client reach at least Level 4 maturity (as per NIST), reflecting optimized, well-integrated operations

Deliverables , Phase 2

The list below includes some of the possible deliverables

01 Incident Response Plan, severity model, and playbooks

02 Malware Analysis Procedure

03 Log Data Quality & Completeness Assurance Procedure

04 SOC Charter and Service Catalogue

05 Threat Intelligence Governance and KPIs

06 Red Team Governance Framework

07 Defensive Security Policy

08 Threat Hunting Methodology and operational runbooks

09 Governance elements (e.g., RACI matrices, control ownership mappings)

10 All deliverables are customized to reflect the organization's environment, business context, and threat profile.

INDICATIVE DELIVERY SCHEDULE / PHASE 1

MILESTONE	W1	W2	W3	W4	W5
Kick-Off and planning	■				
Collection of documentation	■				
Interviews with SMEs	■				
Analysis of information collected	■				
Final Report					■

INDICATIVE DELIVERY SCHEDULE / PHASE 2

MILESTONE	W1	W2	W3	W4	W5
Kick-Off and prioritization	■				
Cybersecurity governance documentation	■				
Defensive and Detection documentation		■			
Response Procedures and Guides		■			
Feedback sessions with SMEs		■			
Knowledge transfer sessions				■	

SERVICE 3.5

Cyber-Perimeter Assessment

The Cyber-Perimeter Assessment service offers a comprehensive evaluation of your organization's external security posture.

This service combines in-depth vulnerability scanning of your external perimeter and assets with Open-Source Intelligence (OSINT) research to identify any exposed or leaked account credentials.

Our goal is to provide a holistic view of your organization's external vulnerabilities and potential exposure points, enabling you to better understand and mitigate risks against cyber threats.

Business value

- **Comprehensive Risk Identification.** Uncover hidden vulnerabilities and exposed credentials that could be exploited by external attackers.
- **Proactive Defense Strategy.** By identifying weaknesses, your organization can proactively strengthen its defenses before they are exploited.
- **Enhanced Security Posture.** Gain a deeper understanding of your organization's external attack surface, allowing for more targeted and effective security measures.
- **Risk Mitigation.** Reducing the likelihood of successful cyber-attacks protects not only your data but also preserves your reputation and customer trust.
- **Informed Decision Making.** The insights gained from this assessment can guide strategic security investments and policy decisions.

Methodology

01 **Initial Scoping and Planning.** Define the scope of the assessment, including target systems and assets to be evaluated.

02 **External Vulnerability Scanning.** Conduct thorough scanning of your external network and digital assets to identify potential vulnerabilities and weak points.

03 **OSINT Research.** Perform extensive open-source intelligence research to discover any exposed or compromised credentials associated with your organization.

04 **Credentials Resilience Assessment.** Analyze the data collected from both external scanning and OSINT research to identify potential risk areas and correlate findings.

05 **Web Application Testing.** Thorough external penetration testing of Internet-exposed applications to identify and mitigate potential vulnerabilities.

06 **Report Preparation and Recommendations.** Prepare a detailed report summarizing the findings, risks, and provide recommendations for remediation and improvement.

07 **Client Debriefing and Feedback Session.** Present the findings to the client, discuss the implications, and integrate their feedback for any further analysis or clarification.

Deliverables

- Comprehensive Cyber-Threat Exposure report including:

- **Executive Summary.** A high-level summary of key findings and recommendations, suitable for executive leadership understanding and decision-making.
- **Vulnerability Assessment Report.** A comprehensive report detailing the vulnerabilities discovered during the external network scanning, including severity levels and potential impacts.
- **OSINT Findings.** A section on the findings from the OSINT research, highlighting any exposed or compromised credentials and their implications.
- **Risk Analysis and Recommendations.** A strategic analysis of identified risks, with tailored recommendations for remediation and security enhancement.
- **Follow-Up Action Plan.** A proposed plan for follow-up actions, including potential re-assessments or additional security measures.

WHAT WE NEED TO SCOPE IT

- Number of external IP addresses.
- How many users the client has.

INDICATIVE DELIVERY SCHEDULE

SERVICE 3.6

Incident Response Plan & Procedures

The Cybersecurity Incident Response Plan (CIRP) Service is meticulously designed to equip organizations with the tools and strategies needed to effectively manage and mitigate cybersecurity incidents. This service includes the development of a comprehensive Incident Response (IR) Plan and detailed Incident Handling Guides, each customized to address the specific needs and threat landscape of the organization.

This service encompasses the formulation of strategies, procedures, and protocols necessary to efficiently identify, respond to, and recover from cyber threats.

Our approach ensures a systematic and coordinated response to incidents, mobilizing only the required amount of business resources to minimize potential damage and help reduce recovery time and costs.

Business value

- **Enhanced Preparedness.** Equips your organization with a robust framework to effectively manage and mitigate cyber incidents, reducing potential operational and reputational damage.
- **Minimized Impact.** By having a clear response plan, your organization can swiftly and effectively address incidents, minimizing their impact on business operations.
- **Compliance Assurance.** Ensures your incident response strategy aligns with industry standards and regulatory requirements, maintaining compliance and trust.
- **Employee Empowerment.** Provides your staff with clear guidelines and confidence to handle incidents effectively, enhancing overall security culture.
- **Strategic Risk Management.** Strengthens your organization's overall risk management strategy by incorporating comprehensive incident response planning.

Methodology

01 **Initial Assessment and Requirements Analysis.** Understand the current cybersecurity landscape, policies, and specific needs of your organization.

02 **Review existing security documentation.** Thoroughly analyze all existing security documentation and policies shared by the client to understand the current state and integrate relevant aspects into the new plan.

03 **IR Plan Development (DRAFT stage).** Create a detailed Incident Response Plan including identification, containment, eradication, and recovery phases.

04 **Incident Handling Guides Creation.** Develop tailored Incident Handling Guides for different types of incidents, providing step-by-step procedures.

05 **Client Discussion and Feedback Integration (FINAL stage).** Present the draft Incident Response Plan to the client for review and discussion. Incorporate their feedback to ensure the plan aligns with their specific requirements and operational context.

06 **Review and Continuous Improvement.** Regularly review and update the IR Plan and Handling Guides to address new threats and changes in the organization.

Deliverables

- **Comprehensive Incident Response Plan.** A document outlining the overall strategy and procedures for responding to cybersecurity incidents.
- **Detailed Incident Handling Guides.** Specific guides for various types of incidents, detailing the steps for identification, containment, eradication, and recovery.

WHAT WE NEED TO SCOPE IT

- **Size of the organization.** number of employees.
- The scope of the engagement includes Playbooks? How many?

INDICATIVE DELIVERY SCHEDULE

MILESTONE	W1	W2	W3	W4	W5
Kick-Off and documentation request	■				
Review of security documentation	■				
Incident Handling Plan and Guides Creation			■		
Client feedback integration and amendments					■

SERVICE 3.7

Table-Top Exercise

Table Top Exercise (TTX) is a simulation-based activity used by organizations to test their incident response capabilities and crisis management procedures in a risk-free environment. It involves key personnel from various departments such as IT, security, communications, and management, who gather to walk through and discuss their roles and responses to hypothetical cybersecurity scenarios.

These scenarios are designed to be realistic and relevant, covering a range of threats such as cyber-attacks, data breaches, and system failures. The exercise is usually facilitated by a moderator who guides the discussion, presents the scenario details, injects new developments, and encourages participant engagement.

The primary goal of a TTX is to evaluate the effectiveness of an organization's incident response plan, identify gaps in policies and procedures, and improve interdepartmental coordination and communication.

Unlike live drills or full-scale simulations, TTXs do not involve the activation of actual resources or systems, making them a cost-effective and minimally disruptive method for testing and improving cybersecurity readiness.

Business value

- **Risk Identification and Mitigation.** Table Top Exercises help organizations identify vulnerabilities and weaknesses in their cybersecurity processes and incident response plans. By simulating cyber threat scenarios, businesses can better understand potential risks and proactively develop strategies to mitigate these risks before they manifest into actual incidents.
- **Compliance and Governance.** Conducting TTEs demonstrates an organization's commitment to cybersecurity best practices and regulatory compliance. Many cybersecurity frameworks and regulations recommend or require regular testing of incident response capabilities. TTEs can provide evidence of compliance with these mandates, reducing legal and financial risks associated with non-compliance.
- **Enhanced Incident Response.** Through the simulation of cyber incidents, participants can refine their decision-making processes, clarify roles and responsibilities, and improve the overall efficiency of the incident response. This preparation enables organizations to respond more swiftly and effectively to real cybersecurity incidents, minimizing potential damages and recovery time.
- **Improved Communication and Collaboration.** TTXs foster better communication and collaboration among different departments and teams within an organization. By bringing together various stakeholders, these exercises enhance mutual understanding and coordination, which is crucial for an effective response to cyber incidents.
- **Cost-Effectiveness.** By identifying and addressing security posture weaknesses before they are exploited, TTXs can significantly reduce the potential costs associated with cyber incidents, including data recovery, legal fees, fines, and reputational damage. The relatively low cost of conducting TTXs compared to the high financial stakes of cybersecurity incidents makes them a valuable investment for businesses.

Methodology

The methodology of a Table Top Exercise typically involves several key steps

01 **Preparation.** Define the objectives, scope, and participants of the exercise. Develop realistic cyber threat scenarios relevant to the organization's industry and risk profile.

02 **Briefing.** Participants are briefed on the exercise's objectives, the scenario(s) to be discussed, and their expected roles and contributions.

03 **Execution.** The facilitator presents the scenario(s), and participants discuss their responses, decision-making processes, and the actions they would take. The focus is on communication, coordination, and decision-making rather than on technical aspects of incident response.

04 **Debriefing.** After the exercise, participants engage in a debriefing session to discuss what was learned, identify strengths and weaknesses in the response, and highlight areas for improvement.

05 **Reporting.** A detailed report is produced, summarizing the exercise's outcomes, including key observations, recommendations for enhancing cybersecurity posture, and an action plan for addressing identified gaps.

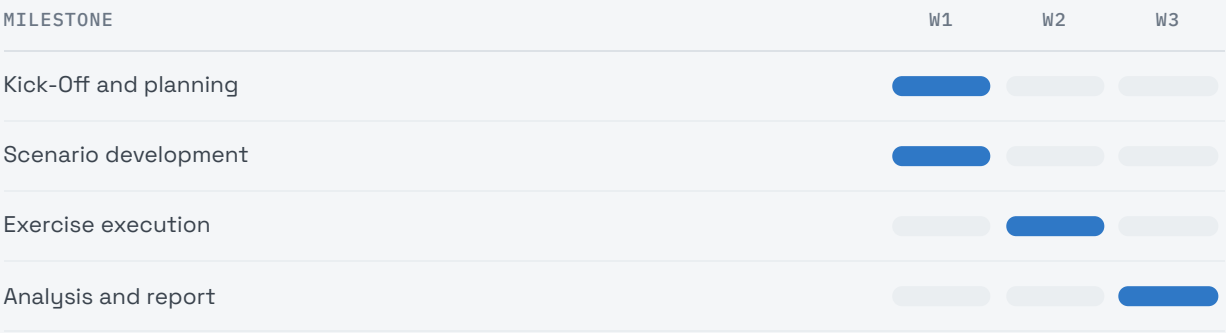
Deliverables

- The primary deliverables from a Table Top Exercise include:
- **Exercise Report.** A comprehensive document that details the exercise's objectives, scenarios, participant roles, key findings, and recommendations for improvement.
- **Action Plan.** A specific, actionable plan derived from the exercise's findings, outlining steps to address identified vulnerabilities, improve incident response protocols, and enhance overall cybersecurity measures.
- **Lessons Learned.** A summary of key insights gained during the exercise, including effective practices and areas needing improvement. This document is very important for informing future cybersecurity strategies and training programs.

WHAT WE NEED TO SCOPE IT

- Type of Table-Top Exercise, technical or for management.
- Number of participants.
- Top three most important objectives; this is used to estimate the level of complexity of the scenario used in the TTX.

INDICATIVE DELIVERY SCHEDULE



SERVICE 3.8

DFIR Functional Exercise

Our DFIR Functional Exercise Service is an advanced simulation designed to rigorously test and enhance the capabilities of your Incident Response (IR) team. This service goes beyond traditional table-top exercises (TTX) by incorporating real-life, technical challenges that simulate various stages of a cyber incident.

From the initial alert triage and evidence assessment to the advanced stages of an attack, your team will encounter scenarios involving endpoint and log-based evidence analysis.

These challenges are crafted to vary in difficulty, providing a comprehensive evaluation of your team's investigative skills, decision-making processes, and overall readiness to manage real-world cyber threats.

Business value

- **Realistic Incident Handling Experience.** Provides the IR team with hands-on experience in managing complex and nuanced cyber incidents.
- **Skill Enhancement.** Helps in identifying and strengthening the technical and strategic skills of your IR team.
- **Process Evaluation.** Offers valuable insights into the effectiveness of your current incident response processes and protocols.
- **Team Readiness Assessment.** Assesses the preparedness of your IR team to handle actual cyber incidents, highlighting areas of proficiency and those needing improvement.
- **Confidence Building.** Enhances the confidence and competence of your team in dealing with real-life cyber threats, thereby improving overall organizational resilience.

Methodology

01 **Pre-Exercise Planning and Customization.** Collaborate with the client to understand their specific needs and customize the exercise scenarios accordingly.

02 **Scenario Development.** Create detailed, realistic incident scenarios that cover various stages of a cyber-attack, including both technical and decision-making challenges. The scenario is created to fit your organization's profile.

03 **Exercise Execution.** Conduct the functional exercise, presenting the IR team with a series of technical challenges ranging from initial alert triage to complex evidence analysis.

04 **Debriefing and Feedback.** Conduct a comprehensive debriefing session post-exercise to discuss the team's performance, decision-making, and areas for improvement.

05 **Comprehensive Analysis and Report.** Analyze the exercise outcomes and provide a detailed report on the team's response effectiveness, skill levels, and recommended areas for development.

Deliverables

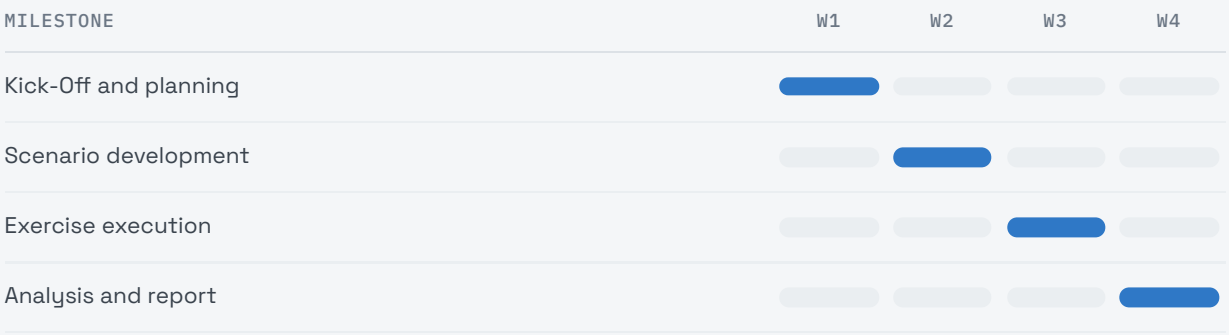
- **Customized Exercise Scenarios.** Tailored scenarios that replicate real-life cyber incident stages, specifically designed for the client's environment.

- **Performance Analysis Report.** A detailed report assessing the IR team's performance during the exercise, highlighting strengths and areas for improvement.
- **Recommendations for Skill and Process Enhancement.** Strategic recommendations based on the exercise outcomes to enhance the team's technical skills and incident response processes.
- **Debriefing and Feedback Documentation.** Comprehensive documentation of the post-exercise debriefing, including feedback and insights for future training and development.

WHAT WE NEED TO SCOPE IT

- How many participants.
- Description of the roles and responsibilities of the participants.

INDICATIVE DELIVERY SCHEDULE



SERVICE 3.9

Training

The Cybersecurity Training program equips employees with essential knowledge and skills to defend against cyber threats. This comprehensive training covers key topics relevant to each security role from a modern Security Operations Center. Designed to be engaging and accessible, it ensures all staff, regardless of their technical background, understand their role in maintaining cybersecurity.

Business value

- Investing in Cybersecurity Training offers significant business benefits. Firstly, it significantly reduces the risk of security breaches, a primary concern in the digital age. Educated employees become the first line of defense, capable of spotting and mitigating threats before they escalate. Secondly, it fosters a culture of security awareness, ensuring cybersecurity is a shared responsibility among all staff. This proactive stance enhances overall security posture and demonstrates compliance with industry standards, boosting client trust and confidence.
- Ultimately, the training programs go beyond teaching basic tasks, focusing on empowering and equipping teams with the critical skills needed to navigate and resolve complex incidents effectively. By fostering confidence and expertise, the goal is to prepare teams to respond proactively and efficiently to challenging cybersecurity situations, ensuring the organization's integrity and resilience remain safeguarded.Top of Form

Methodology

01 The Cybersecurity Trainings are strategically segmented into two distinct modules, catering to different levels of expertise and operational roles within your organization. This tiered approach ensures that each team member receives tailored training that aligns with their responsibilities and skill sets, maximizing the effectiveness of the program.

02 **First Responders (SOC L1 & L2) Training.** This module is designed for personnel who are likely to be the first point of contact in a cybersecurity incident. The training focuses on equipping them with the skills to identify potential threats, understand immediate response protocols, and effectively communicate the situation to the relevant advanced teams.

03 It covers basic security principles, incident identification, initial containment strategies, and communication channels, ensuring a swift and coordinated response to any threat.

04 Advanced Digital Forensics and Incident Response (DFIR) Team Training: Targeted at your specialized DFIR team, this advanced module delves into the complexities of forensic analysis and detailed incident response. It encompasses in-depth training on the latest forensic tools, sophisticated threat hunting techniques, and advanced incident analysis.

05 The aim is to empower your DFIR team to thoroughly investigate incidents, uncover the root causes, and implement strategic countermeasures to prevent recurrence.

WHAT WE NEED TO SCOPE IT

- How many participants.
- Roles and responsibilities of the participants.
- Depth of the content (e.g., SOC L1 , L3, DFIR consultant).
- Any specific topics that should be included in the training.

INDICATIVE DELIVERY SCHEDULE

MILESTONE	W1	W2	W3
Kick-Off and planning			
Curriculum Review			
Training Delivery			
Final Report			

SERVICE 3.10

Emergency Incident Response

The Emergency Incident Response service provides organizations with immediate, expert assistance in the event of a critical cybersecurity incident. This service ensures rapid deployment of our experienced Incident Response (IR) professionals to mitigate threats, minimize damage, and restore normal operations swiftly. Our team specializes in handling high-impact incidents such as ransomware attacks, insider threats, data breaches, and advanced persistent threats.

The service includes rapid containment, detailed forensic analysis, and guided recovery, leveraging cutting-edge tools and proven methodologies tailored to your organization's specific needs. This ensures that incidents are addressed efficiently and comprehensively, limiting both operational and reputational damage.

Business value

- The Emergency Incident Response service delivers significant business value by enabling organizations to respond effectively to cyber crises. The rapid response minimizes downtime, reduces financial losses, and preserves critical business operations. By addressing incidents promptly, organizations can also safeguard their reputation and maintain customer trust.
- Additionally, having a structured and expert-led approach to incident handling helps organizations meet regulatory and compliance requirements while demonstrating a commitment to cybersecurity resilience. This service is not just a reactionary measure; it forms part of a robust security strategy that empowers organizations to recover quickly and strengthen their defenses against future incidents.

Methodology

The Emergency Incident Response service employs a structured approach to ensure quick and effective resolution of incidents. This includes

01 **Activation & Triage.** Upon notification, the IR team activates the response process, performing a rapid triage to prioritize and assess the incident's scope and severity.

02 **Containment.** Immediate actions are taken to contain the incident and prevent further damage. This may involve isolating affected systems, disabling compromised accounts, or applying emergency patches.

03 **Incident Analysis.** The team conducts a thorough investigation to identify the root cause, attack vectors, and the extent of the compromise. Digital evidence is collected and analyzed to support remediation and potential legal actions.

04 **Remediation & Recovery.** Based on the analysis, the team implements a remediation plan to eradicate the threat, restore affected systems, and return operations to a secure state.

05 **Post-Incident Review.** After resolving the incident, the team conducts a review to identify lessons learned and provide actionable recommendations to enhance the organization's security posture.

Deliverables

- Key deliverables from the Emergency Incident Response service include:
- **Incident Report.** A detailed document outlining the nature of the incident, the response actions taken, and the impact on the organization. Includes a timeline of events and supporting evidence.
- **Containment & Remediation Plan.** Specific recommendations for addressing vulnerabilities, recovering systems, and improving security measures.
- **Forensic Analysis Report (if applicable).** A comprehensive forensic report detailing the evidence, analysis methodologies, and conclusions.
- **Post-Incident Debrief.** A session with stakeholders to review the incident findings, response efforts, and lessons learned.
- **Regulatory Support Documentation.** Assistance in preparing incident documentation for regulatory or legal purposes.
- **Lessons Learned Summary.** A document identifying strengths and weaknesses in the incident response process, aimed at improving future resilience.

WHAT WE NEED TO SCOPE IT

- **Live Incident.** between 40 , 80 hours (not including final report).
- **NOTE.** the client will receive daily technical updates with description of the case progress.
- **The final report.** 16 hours. The report is customized to answer to all questions the client wants to be addressed.
- **Post mortem investigations.** minimum 32 hours (including final report).

SERVICE 3.11

DFIR Program

The Digital Forensics and Incident Response (DFIR) Program service provides your organization with immediate, expert assistance in the event of a cybersecurity incident. This program ensures priority access to our team of seasoned DFIR professionals who specialize in quickly identifying, containing, and analyzing cyber threats.

Our experts are adept in handling a wide range of incidents, from data breaches and ransomware attacks to complex, targeted intrusions.

The service includes proactive threat hunting, detailed forensic analysis, and comprehensive incident response planning, tailored to your organization's specific needs and environment.

Business value

- The DFIR Program service offers significant business advantages. Firstly, it ensures rapid response in critical situations, drastically reducing the potential impact and downtime caused by cyber incidents. Quick and efficient response not only mitigates immediate risks but also helps in preserving company reputation and customer trust.
- Secondly, having a dedicated DFIR team means your organization benefits from continuous threat intelligence and evolving best practices in cybersecurity, keeping you a step ahead of potential threats.
- This service also demonstrates to stakeholders and regulators your commitment to robust cybersecurity, which can be crucial for compliance with industry standards and legal requirements. Ultimately, the DFIR Program is not just an emergency measure; it's a strategic investment in your organization's resilience, providing peace of mind and enabling you to focus on your core business operations, knowing that your cyber defenses are fortified by experts.

Methodology

The methodology under a DFIR Program typically follows a structured approach to ensure rapid and effective response to incidents. This approach includes

01 **Preparation and Planning.** This initial phase involves understanding the client's IT infrastructure, identifying key assets, and establishing communication protocols. Preparation may also include conducting initial assessments to understand the security posture and potential vulnerabilities.

02 **Incident Detection and Analysis.** On Program activation, the DFIR team uses a combination of automated tools and expert analysis to detect and assess the nature, scope, and impact of the incident. This phase relies heavily on the collection and examination of digital evidence.

03 **Containment, Eradication, and Recovery.** Once the incident is understood, the team works to contain the threat, remove the attackers' presence from the system, and restore affected operations. This might involve deploying patches, changing passwords, and cleaning infected systems.

04 **Post-Incident Analysis.** After the immediate threat is addressed, a thorough analysis is conducted to understand how the breach occurred, the extent of the data or systems affected, and the effectiveness of the response.

05 **Continuous Communication.** Throughout the incident response process, the DFIR team maintains open lines of communication with the client, providing updates, receiving input, and adjusting strategies as necessary.

06 **Consulting Hours for Additional Services.** If Program hours allocated for incidents and investigations are not fully consumed, these hours are not lost. Instead, they can be utilized for other consulting services, such as vulnerability assessments, penetration testing, security policy review, or additional training sessions.

07 This flexibility ensures that organizations derive maximum value from their Program, enhancing their overall security posture.

Deliverables

- Deliverables from a DFIR Program agreement are designed to provide the client with detailed insights into the incident, recommendations for recovery, and strategies for preventing future incidents. Key deliverables include:
- **Incident Report.** A comprehensive document detailing the nature of the incident, the methods used by the attackers, the impact on the organization, and the steps taken to respond. This report should include a timeline of events and any relevant evidence.
- **Remediation Plan.** A set of recommendations for remedying the vulnerabilities exploited during the incident and improving the overall security posture to prevent similar attacks. This may include technical fixes, policy changes, and recommendations for employee training.
- **Post-Incident Debrief.** A meeting or presentation to discuss the findings of the incident report, explain the remediation plan, and answer any questions. This is an opportunity for the client to understand the incident and the steps taken to resolve it fully.
- **Lessons Learned Document.** An analysis of the incident response process to identify strengths and weaknesses in the response effort. This document aims to improve future responses and overall security practices.
- **Forensic Analysis Report (if applicable).** In cases where a detailed forensic investigation is conducted, a separate report detailing the forensic findings, methodologies used for analysis, and evidence supporting the conclusions may be provided.
- **Regulatory and Legal Support Documentation.** Assistance in preparing reports or documentation required for compliance with regulatory requirements or for legal proceedings related to the incident.
- A DFIR Program ensures that organizations have rapid access to expert assistance in the event of a cyber incident, minimizing the impact and aiding in the swift recovery of operations.

WHAT WE NEED TO SCOPE IT

- Size of the environment, how many endpoints and users.
- Use of O365 (how many users).
- Count of Web Applications exposed to Internet.

Combining services.

Cybersecurity needs are interconnected, and addressing them together is often the most effective route. Add-on services complement a primary engagement; bundles combine services that work well in sequence.

Add-On Services

Enhance your primary engagements with targeted add-ons to achieve deeper insights and more comprehensive outcomes.

- **Advanced Threat Hunting.** Add proactive threat-hunting activities to any monitoring or assessment service for deeper detection of stealthy threats.
- **Custom Reporting and Executive Briefings.** Tailored reports with detailed findings, risk assessments, and actionable recommendations, including executive-level summaries for leadership teams.
- **Cloud Security Posture Review.** Add a targeted review of cloud configurations and security settings to broader risk assessments or penetration tests.

Bundled Service Packages

Optimize your cybersecurity efforts with pre-designed service bundles that address multiple needs efficiently.

- **SOC Modernization Bundle.** Combines Threat Handling Review (of documentation) with Threat Hunting Assessment and advanced training for your SOC team to improve overall efficiency and response times.
- **Proactive Security Suite.** A combination of penetration testing, compromise assessments, and security awareness training to strengthen your defenses from multiple angles.
- **Cyber-resilience Bundle.** Includes DFIR Functional Exercise, Table-Top Exercise and Security Posture Assessment.

Custom Bundles

Every organization has distinct needs and objectives. If the predefined bundles do not fully align with your requirements, a custom bundle can be designed to address specific challenges and goals, ensuring tailored, cost-effective solutions that meet your unique circumstances.

Request an engagement

Scoping starts with a conversation rather than a questionnaire. Tell us what you need to establish and we will tell you which service answers it, or that none of them does.

If your requirement is not covered in this catalog, that is worth a call too. Bespoke work is the normal case here, not the exception.

---

contact@alexsta-cybersecurity.com

+41 76 76 44884

alexsta-cybersecurity.com

AlexSta CyberSecurity AG / CHE-349.360.783 / Registered in the Canton of Zug