

Defensury Inc. & Subsidiaries

Über die Cyber Security Gruppe

Defensury Inc. | RedGov | Invensics





Ausrichtung der Gruppenunternehmen

- Defensury Inc. ist ausschließlich im privaten Sektor tätig.
- RedGov ist ausschließlich im öffentlichen Sektor tätig.
- Defensury & RedGov entwickelt 360 Grad Sicherheitslösungen im Rahmen eines 3 Phasen Modells
- Invensics ist sowohl für öffentliche, als auch privatwirtschaftliche Organisationen tätig
- Invensics untersucht ein breites Spektrum krimineller Aktivitäten



Aufstellung der Gruppenunternehmen

- 300 Mitarbeiter weltweit erlauben 24/7 Operationen
- 80% unserer Cyber-Experten haben einen militärischen bzw. nachrichtendienstlichen Hintergrund
- 20% unserer Cyber-Experten sind „white hats“ , renommierte Mitglieder unterschiedlicher Communities: DefCon, Black Hat, PHDays etc.
- Zu unseren Teams zählen auch Experten aus den Bereichen HUMINT, OSINT, SIGINT und FININT mit umfassender Berufserfahrungen in „Special Operations“ und Intelligence.
- Alle unsere Mitarbeiter verfügen über weltweite Sicherheitsfreigaben unterschiedlicher Regierungen. RedGov verfügt zusätzlich über Sondergenehmigungen der USA und der Regierung der Russischen Föderation.

Das 3-Phasen-Modell

Phase I



- Defensury und RedGov Mitarbeiter organisieren sich für jedes Projekt in 2 Teams: Cyber und On-site Operatoren.
- On-site versuchen die Organisation (ohne das Wissen der Mitarbeiter zu infiltrieren. Dabei finden ebenso Techniken des Social Engineering durch das Heben von HUMINT Anwendung, wie OSINT. Ziel ist es soviel Informationen wie möglich über die Kundenorganisation zu gewinnen und ggf. einen Ansatz für den Cyber-Ansatz zu identifizieren. Ist die Kundenorganisation international aufgestellt, reisen unsere Teams zu verschiedenen Standorten um sich vor Ort ein Bild über die Infrastruktur zu verschaffen.
- Unsere „Electronic Warfare“ Spezialisten attackieren die Kundenorganisation rund um die Uhr. Unsere Spezialisten suchen nach vulnerablen Ansatzpunkten durch den Einsatz freizugänglicher Werkzeuge, als auch durch die Verwendung exklusiver nachrichtendienstlicher Technologien.
- Phase 1 für die Phase 1 planen wir regelmäßig mindestens 3 Monate Operationszeit ein. Ziel der Phase I ist es vulnerable Ansatzpunkte zu identifizieren. Die veranschlagte Operationszeit basiert auf Erfahrungswerten aus der Vorgehensweise feindlicher Akteure, die regelmäßig mindestens 3 Monate vor den ersten Zugriffen in die Analyse ihrer Zielorganisation investieren.

Das 3-Phasen-Modell

Phase II



- Auf den Befunden der Phase I basierend entwickeln unsere Spezialisten einen individuellen Trainings-/Fortbildungsplan für die Mitarbeiter der Kundenorganisation, sowie ein angepasstes Handbuch zur Informationssicherheit zur Minimierung künftiger HUMINT Angriffe.
- Das Cyber-Team verfasst einen detaillierten Report zu den Befunden der Operation inklusive einer sicherheitsfokussierten Analyse der Netzwerkinfrastruktur der Kundenorganisation.
- Nach der gemeinsamen Analyse der Projektergebnisse mit dem IT-Team der Kundenorganisation, fixieren die Defensury's/Redgov Spezialisten die identifizierten Schwachstellen **gemeinsam mit dem IT-Team der Kundenorganisation** (learning by doing effect!).
- Ziel ist es eine sichere 360 Grad Sicherheitsarchitektur für die Kundenorganisation zu entwickeln. Defensury / RedGov Experten-Teams können Soft- und Hardwarelösungen entwickeln, wenn keine ausreichend geeigneten kommerziellen Lösungen verfügbar sind.

Das 3-Phasen-Modell

Phase III



- Periodische Reassessments um den fortgesetzten Erfolg der implementierten Lösung sicherzustellen. Die Reassessments umfassen den Test der Reaktionszeit des Kunden-IT-Teams ect.
- Aufbau eines externen SOC Zentrums um die Kundennetzwerke kontinuierlich zu begleiten ...
- Updates der Kunden-IT zu aktuellen Bedrohungen und technologischen Entwicklungen

Invensics



- Invensics ist der investigative Arm der Gruppe und ist weltweit für Regierungsorganisationen und Wirtschaftsunternehmen tätig.
- Invensics ist auf Cyber Forensic und Counterintelligence spezialisiert.
- 24/7 Reaktionsfähig.
- Invensics ist in der Lage innerhalb von 6h weltweit ein Ermittlungsteam vor Ort zu bringen.
- Unsere digitalen Forensikspezialisten können innerhalb von 15 Minuten nach Aktivierung ein Forensik-Setup online zu bringen.